THE UNIVERSITY OF
BUCKINGHAM

Robust Steganographic Techniques for Secure Biometric-based Remote Authentication

By

RASBER DHAHIR RASHID

Department of Applied Computing
University of Buckingham
United Kingdom

A thesis
Submitted for the Degree of Doctor of Philosophy in Computer Science to the School of Science and Postgraduate Medicine in The University of Buckingham

November 2015

ABSTRACT

Biometrics are widely accepted as the most reliable proof of identity, entitlement to services, and for crime-related forensics. Using biometrics for remote authentication is becoming an essential requirement for the development of knowledge-based economy in the digital age. Ensuring security and integrity of the biometric data or templates is critical to the success of deployment especially because once the data compromised the whole authentication system is compromised with serious consequences for identity theft, fraud as well as loss of privacy. Protecting biometric data whether stored in databases or transmitted over an open network channel is a serious challenge and cryptography may not be the answer. The main premise of this thesis is that Digital Steganography can provide an alternative security solutions that can be exploited to deal with the biometric transmission problem.

The main objective of the thesis is to design, develop and test steganographic tools to support remote biometric authentication. We focus on investigating the selection of biometrics feature representations suitable for hiding in natural cover images and designing steganography systems that are specific for hiding such biometric data rather than being suitable for general purpose. The embedding schemes are expected to have high security characteristics resistant to several types of steganalysis tools and maintain accuracy of recognition post embedding. We shall limit our investigations to embedding face biometrics, but the same challenges and approaches should help in developing similar embedding schemes for other biometrics. To achieve this our investigations and proposals are done in different directions which explain in the rest of this section.

Reviewing the literature on the state-of-art in steganography has revealed a rich source of theoretical work and creative approaches that have helped generate a variety of embedding schemes as well as steganalysis tools but almost all focused on embedding random looking secrets. The review greatly helped in identifying the main challenges in the field and the main criteria for success in terms of difficult to reconcile requirements on embedding capacity, efficiency of embedding, robustness against steganalysis attacks, and stego image quality. On the biometrics front the review revealed another rich source of different face biometric feature vectors. The review helped shaping our primary objectives as (1) identifying a binarised face feature factor with high discriminating power that is susceptible to embedding in images, (2) develop a special purpose content-based steganography schemes that can benefit from the well-defined structure of the face biometric data in the embedding procedure while preserving accuracy without leaking information about the source biometric data, and (3) conduct sufficient sets of experiments to test the performance of the developed schemes, highlight the advantages as well as limitations, if any, of the developed system with regards to the above mentioned criteria.

We argue that the well-known LBP histogram face biometric scheme satisfies the desired properties and we demonstrate that our new more efficient wavelet based versions called LBPH patterns is much more compact and has improved accuracy. In fact the wavelet version schemes reduce the number of features by 22% to 72% of the original version of LBP scheme guaranteeing better invisibility post embedding.

We shall then develop 2 steganographic schemes. The first is the LSB-witness is a general purpose scheme that avoids changing the LSB-plane guaranteeing robustness against targeted steganalysis tools, but establish the viability of using steganography for remote biometric-based recognition. However, it may modify the 2nd LSB of cover pixels as a witness for the presence of the secret bits in the 1st LSB and thereby has some disadvantages with regards to the stego image quality.

Our search for a new scheme that exploits the structure of the secret face LBPH patterns for improved stego image quality has led to the development of the first *content-based* steganography scheme. Embedding is guided by searching for similarities between the LBPH patterns and the structure of the cover image LSB bit-planes partitioned into 8-bit or 4-bit patterns. We shall demonstrate the excellent benefits of using content-based embedding scheme in terms of improved stego image quality, greatly reduced payload, reduced lower bound on optimal embedding efficiency, robustness against all targeted steganalysis tools. Unfortunately our scheme was not robust against the blind or universal SRM steganalysis tool. However we demonstrated robustness against SRM at low payload when our scheme was modified by restricting embedding to edge and textured pixels. The low payload in this case is sufficient to embed a secret full face LBPH patterns.

Our work opens new exciting opportunities to build successful real applications of content-based steganography and presents plenty of research challenges.

I dedicate my thesis to my Father's soul

And

To my family

ACKNOWLEDGMENT

Many thanks go to my supervisor Professor Sabah Jassim for his creative guidance during supervision. I appreciate his advices on both researches as well as on my career which have been priceless. I would like sincerely to thank Dr. Harin Sellahewa for his valuable comments and useful discussions during my study.

My warm thanks to my family, and special thanks go to my wife and love “Taban”, for her continuous support and being with me in every step in my life. I want to say thank you my two beautiful angels, Shanya and Lanya, for your patience and understanding throughout the duration of my study.

Finally, I would like to thank Ministry of Higher Education and Scientific Research in Kurdistan Region and Koya University for sponsoring part of my PhD program.

ABBREVIATIONS

AES	Advanced Encryption Standard
ANN	Artificial Neural Networks
BER	Bit Error Rate
BP	Bit Plane
bpp	Bits Per Pixel
COM	Centre of Mass
dB	Decibels
DCT	Discrete Cosine Transform
DFT	Discrete Fourier Transform
DIH	Different Image Histogram
DWT	Discrete Wavelet Transform
ECC	Error Correction Code
EOOB	Out-Of-Bag Error
FLDA	Fisher Linear Discriminant Analysis
GEFR	Gradient Energy Flipping Rate
HCF	Histogram Characteristic Function
HUGO	Highly Undetectable SteGo
HUGO BD	HUGO With Bounding Distortion
ID	Identification Cards
JPEG	Joint Photographic Experts Group
LBP	Local Binary Pattern
LBPH	Local Binary Pattern Histogram
LDA	Linear Discriminate Analysis
LSB	Least Significant Bit
LSBM	Least Significant Bit Matching
LSBMR	Least Significant Bit Matching Revisited
MSB	Most Significant Bit
MSE	Mean Squared Error
NC	Normalized Correlation
NN	Nearest Neighbour
OC-SVM	One-Class Support Vector Machine
OTP	One Time Password

PCA	Principal Components Analysis
PIN	Personal Identification Number
PoV	Pairs of Value
PRNG	Pseudo Random Number Generator
PSNR	Peak Signal to Noise Ratio
PVD	Pixel Value Differencing
RLE	Run Length Encoding
RLSB	Random Least Significant Bit
ROI	Region of Interest
RQP	Raw Quick Pair
RS	Regular and Singular
RWS	Revisited Weighted Stego
SLSB	Sequential Least Significant Bit
SRM	Spatial Rich Models
S-UNIWARD	Spatial-Universal Wavelet Relative Distortion
SVM	Support Vector Machines
SIFT	Scale Invariant Feature Transform
TLSB	Traditional Least Significant Bit
UNIWARD	Universal Wavelet Relative Distortion
WOW	Wavelet Obtained Weights
WS	Weighted Stego
WT	Wavelet Transform

CONTENTS

LIST OF FIGURES

LIST OF TABLES

DECLARATION

I, hereby declare that presented work has not previously been submitted towards any qualification degree or diploma in the University of Buckingham or any other university.

I also declare that to the best of my knowledge and belief the thesis contains no material previously published or written by another person except where due reference is made in the thesis itself.

Rasber Dhahir Rashid

Chapter 1
Introduction

Ever since the emergence of global online transmission as a tool for commercial, banking, and crime-fighting activities that involve exchange of financial transactions or sensitive and private information the question of authentication of authorised users or authorised actions have become a major challenging problem. Various remote authentication solutions have been developed but due to frequent changes in the nature of threats to the exchanged data and to the vulnerability of the authentication process this problem remains an active research area. In this thesis we shall focus on securing the exchange of biometric data as a proof of identification for mobile remote authentication for commercial purposes or for use by law enforcing agencies in crime fighting and Forensics.

Two main data protection mechanisms have been developed over the years that are designed to prevent unauthorised access and misuse of sensitive data: Cryptography and Steganography. Each of these two mechanisms has its own requirements, challenges, strengths and weaknesses. In this thesis we will be investigating the use of Digital Steganography to deal with the biometric transmission problem. In section 1.1 we shall give an overview of the research problem.

1.1 Overview of the Research Problem

Biometric-based verification has long been used to secure physical access to sensitive sites and assets. Indeed biometrics has been used for decades to limit access to certain sensitive areas in nuclear power stations and safes. In these applications the list of authorised persons was relatively small and their biometric data were stored in physically secured databases. Whenever a person arrives at the entry point of the sensitive site a fresh biometric recording is made and extracted for matching with the stored biometric templates of the registered authorised persons. Biometrics-based techniques utilize certain physiological or behavioural characteristics of persons such as fingerprints, facial features, iris, hand geometry, voice, signature, etc (Jain, et al., 2005). The popularity gained by this biometrics technology is mainly attributed to its ability to distinguish between an authorized person and a pretender who deceptively acquires the access privilege of an authorized person (Agrawal & Savvides, 2009; Jain & Uludag, 2003).

In recent years, advances in communication technology and the emergence of the Internet as the most popular mean of communication anytime and anywhere together with the availability of inexpensive biometric recording devices have led to the emergence of increasing interest in biometrics-based personal identification or authentication techniques due to their proven substantial superiority over token-based or knowledge based techniques such as identification cards (ID), passwords, etc.

While biometric authentications have inherent advantages over traditional personal identification techniques the problem of ensuring the security and integrity of the biometric data or templates is critical because once the biometric data are compromised, the whole authentication system is compromised. Given the uniqueness of a person's biometric data it is vital to ensure the security and integrity of these data against a variety of attacks or misuses. For example if a person's biometric data (e.g. a fingerprint image) is stolen and then attackers may be able to impersonate him or her and gain access to his financial as well as other personal information assets. Moreover, in this case it is not possible to replace the person's biometric data, while replacing a stolen credit card, ID, or password is an easy though inconvenient task. Moreover, the security of biometric data transmitted on open network communication channels is a major obstacle for remote biometric-based authentication needed for m-commerce and m-banking.

Protecting biometric data stored in databases and secure biometric transmission over open network channels have attracted huge interest from the biometric research community especially in relation to facilitating remote biometric-based authentication to enable secure e-commerce, m-banking and cloud transactions. Possible biometric protection mechanisms include encryption, watermarking, and steganography (Agrawal & Savvides, 2009). The emergence of cancellable or revocable biometrics over the last decade provides another alternative protection mechanism (Al-Assam, 2013).

Encryption works by converting the biometric information into data that are meaningless to attackers. The security effect of encryption fades away once the data are decrypted. Both Steganography and watermarking are related to data hiding, i.e.

protecting private information through hiding vital information in seemingly ordinary carrier signal. Steganography involves embedding secret biometric data into host signal in a way that does not raise any suspicion while transmitting the information. This way, the biometric data are being protected. Watermarking helps to identify biometric data that have been tampered with for integrity verification (Na, et al., 2010).

Steganographic techniques, on the other hand, diminish the likelihood of biometric data being intercepted by intruders and thus the chances of unauthorized alteration of the biometric data are reduced (Jain & Uludag, 2003). To increase the security profile when transferring biometric data in unsecure media, the biometric data can be encrypted first then embedded inside a cover, it means combining the principles of cryptography with steganography (Sonsare & Sapkal, 2011; Umamaheswari, et al., 2010).

Cancelable biometrics is the mechanism used for biometric template protection purpose. The concept of cancellable biometrics was introduced to denote biometric templates that can be cancelled and replaced as well as being unique for every application. Cancellable biometrics requires storage of the transformed (not actual) version of the biometric template and hence provides higher privacy levels by allowing multiple templates to be associated with the same biometric data. (Ratha, et al., 2001)

The use of homomorphic ciphers (Gentry, 2009) have been promoted for privacy preserving solution in case that users encrypt the data and then send it to the cloud, the cloud can still perform computations on the data even though it is encrypted. In recent years number of such scheme (Stehlé & Steinfeld, 2010; Gentry & Halevi, 2011; Gentry & Halevi, 2011; Smart & Vercauteren, 2014) are proposed, but efficiency to be practical seem that require more research.

The main premise of this thesis is that Digital Steganography is a security mechanism solution that has been used as an alternative or complementary to encryption can be exploited to deal with the biometric transmission problem. Steganography is derived from the Greek language and meaning secret communication involves hiding critical information in unsuspected carrier data in such a way that is imperceptible to attackers. A common application scenario that highlights the importance of steganography in sensitive governmental communication setting and law enforcing agencies in particular is at border control points. For example if the identity of a person who may be a suspect is to be checked against a law enforcing agency or immigration agency database that is located on a remote server, then face or fingerprint biometric information can be embedded within another medium (cover) to ensure secure and un-tampered arrival at the final destination. This way, the transmission of the biometric information is protected from being attacked or tampered with if the appropriate steganography procedure is implemented.

The aim of this introductory chapter is to explain the challenges in biometric systems and steganography in general. Regarding biometric systems we focus more especially on those biometric systems challenges that related to remote authentication and on biometric protection solutions via steganography while for steganography challenges we focus on the main requirements that need satisfied in any embedding system. Explaining these challenges is the key to understanding the motivation of the thesis. This chapter is ended with given the outline overall structure of the thesis.

1.2 Challenges in Biometrics based Remote authentication

Biometrics are digital representations of physiological or behavioral characteristics of human used for automatic proof of identity in a growing list of applications including crime fighting, forensics, border control, for securing electronic transactions, and checking service entitlements. Biometrics have emerged initially as a results of the need for identification or authentication of employee and vetted person who are granted access to restricted areas of sensitive sites such as military sites, nuclear power plants or Banks safes. At that stage, the main challenge is the accuracy of matching a fresh biometric data to one of the ***locally*** stored biometric templates of the approved set of persons. However, the emergence of the Internet has provided new opportunities for deployments of biometric-based authentications and changed or widened the goal post to include other than accuracy of matching.

Recently, biometrics-based person identification systems are increasingly used for access to applications or devices over non-secure channels of the Internet. These changes in use of biometrics together with mobility of users as well as the globalised commerce have led to the need for developing secure remote authentication protocols. The privacy and security issues during the collection, processing, storage and transmission of biometric data are of great concern for most biometric systems. Ratha et al. (Ratha, et al., 2001), categorise attacks on any biometric system to eight basic categories, listed below. Figure 1.1 illustrates the typical block diagram of an authentication system together with indicators of the weak points that could be exploited by each of the eight types of attacks:

- First attack, a fake biometric is presented to the sensor.
- Second attack, by passing sensors and resubmit digitally stored biometric data.
- Third attack, the feature detector is fed attacker prepared features instead of the actual features which are extracted from the original data obtained from the sensor.
- Fourth attack, features extracted from the data obtained in the sensor is replaced with a fake feature set during transmission.
- Fifth attack, matcher component could be attacked to produce attacker's preferred matching score.
- Sixth attack, templates stored in databases could be attacked by replacing with attackers template.
- Seventh attack, the channel between the database and matcher could be attacked to alter transferred template information.
- Eighth attack, altering the matching result itself by overriding the final decision by attacker.

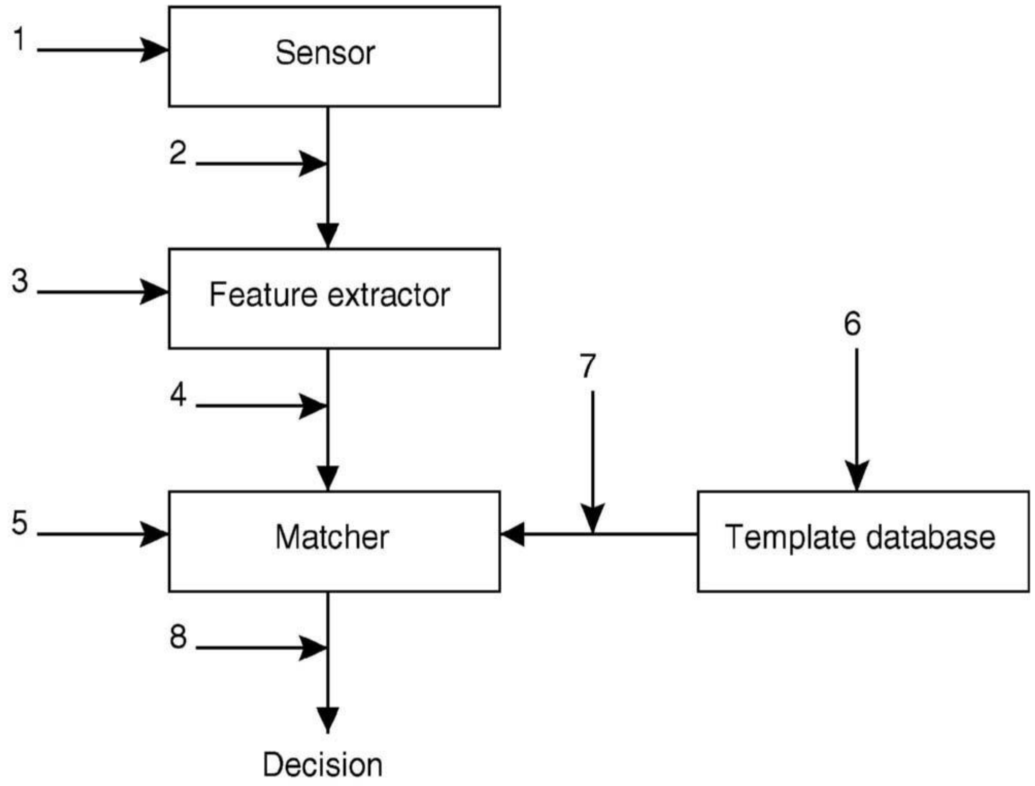


Figure 1.1: Possible attack points in a generic biometrics-based system

Some attacks occur during transmission from one step to another such as attacks number 2, 4, 7, and 8. These four attacks type in biometric system can be named as replay or man-in-the-middle attacks. Solutions such as encryption are not preventing this kind of attacks. All of these attacks lead to reduced credibility of a biometric system. Therefore, there is a need for other kind of solutions to prevent the above attacks. Watermarking and steganography are possible techniques to achieve this. Here in this thesis we focused on steganography techniques and more especially we focus on preventing or reducing chance of attacks that happen between feature extractor and matcher (i.e. attack number four). This kind of attacks mostly happen in remote authentication biometric systems, in another word this kind of attacks happen when the feature extractor is located in the location while the matcher is located in another location (remote matcher) and the result of matcher used to access the application or devices remotely.

The use of steganography to protect biometric data in storage or in transit poses a number of challenges due to the fact that there are two implicit requirements that both to need to be met. To start with the security of the biometric data needs to be maintained to the highest standard while accuracy level should not be impaired by the embedding or extraction of the biometric data in the carrier. Moreover, it is very important to realise that it is not enough to guarantee that the biometric data could not recovered by attackers, but it is more important that any third party cannot even guess the presence of a secret in the communication. Otherwise a denial of service undermines the overall authentication process.

In general, embedding a secret message in a cover image creates what is called a stego-cover which is expected to be free from any detectable artefacts that resulted from message embedding. Otherwise, the presence of artefacts may become a hint to a third party (Attacker) that a secret message is present; an event that would bring the whole steganographic tool into failure (Shaozhang, et al., 2009; Fridrich, et al., 2000; Fridrich, et al., 2001). Hence the choice of biometric traits or features becomes a challenging task. Note that for some biometric traits there are many different choices for biometric features as well as classifier used for matching. In this thesis we shall be mainly investigating the secure transmission of face biometrics as the mean of remote authentication. This choice is influenced by the nature of our intended use of remote exchanges of biometrics by law enforcing forces in fighting crimes and forensics.

However, the same issues and approaches need to be investigated for remote authentication by any other biometric trait.

1.3 Challenges in Steganography

Modern steganography and steganalysis can be defined as a communication strategy between two steganographers, Alice and Bob to exchange secret information without being raising suspicion of a warden, Wendy, who observes all communication between the two and would put them to solitary confinement if she finds or suspects them communicating secrets. Thus, Alice and Bob must communicate in such a manner that Wendy does not get to perceive their secret communication. So they need to hide secret messages inside innocuous objects so that Wendy cannot perceive its very existence. In this context, steganalysis is a set of techniques, visual or statistical, by which it is possible to detect the existence of steganographic content in a cover object. In this scenario the steganographic system is broken when Wendy finds out that Alice and Bob are communicating a secret message. In particular, the warden does not have to decode the message which makes steganalysis fundamentally different from cryptanalysis.

Recently, digital images have become a very popular choice to be used as a cover medium primarily because of its capacity as well as redundancy in representation and pervasiveness in applications in daily life. Known challenges in image steganography techniques relate to dealing with a variety of competing requirements. The following is the most commonly relevant researched steganography techniques to deal with the overall challenge of protecting the secrecy of the transactions:

1- **Security vs. Capacity:** trade-off between Security and Capacity is an important issue in steganography. It has been observed that increase in the payload capacity leads to sacrificing the security to some extent. Developing algorithms which provide both high security and capacity is one of the main important remaining challenges in image steganography.

2- **Secret message & Cover content:** looking for relation between secret message and cover content is an issue in steganography. The security of embedding techniques can be improved by finding similarity between secret message and cover contents in order to cause less change to cover pixel values in order to cause least alteration to the statistical properties of the cover images.

3- **Best positions for embedding:** developing adaptive embedding algorithm is another open problem area. The main concept of this kind of embedding is to select areas in the cover image where the embedding will cause minimum distortion of the cover such as embedding in noisy and high frequency areas.

4- **Cover structure:** the texture and statistical structure of the cover images highly affect the security of embedding techniques. Therefore selecting suitable images for specific embedding techniques and specific secret messages is an open challenge in image steganography field.

Over the years many approaches have been developed to deal with one or more of these challenging issues. For example, embedding in more than the first Least Significant Bit (LSB) or even using extended binary representation of greyscale pixel values by Fibonacci and similar sequences may have been used to increase embedding capacity. However, these approaches are of limited effect and may result in reduced cover image quality in terms of visibility of artefacts as well as increased chance of detectability. On the other hand, attempts to reduce artefact visibility have focused on selecting edge-related pixel areas for hiding secrets. However this results in reduced embedding capacity. Selecting images that include richer texture may help in this case but in a rather marginal way and may raise undesired suspicions. These approaches will be reviewed in the next chapter which highlights benefits and shortcomings. One clear observation is that most existing steganography solutions deal with a general purpose information hiding problem with little or no consideration for the specific characteristics of the secret message. In this thesis, we shall develop a holistic approach to deal with the above problems. Moreover, we shall always keep in mind that we are her interested in hiding biometric data that usually have specific structure and format that could influence the various parameters of concern raised above. In other words, we are investigating a context-aware secret hiding system where knowledge of the secret content may require an optimal special representation of the secret and developing appropriate embedding schemes that meet the main purpose of communicating it. In our case where the secret is a biometric representation of a person, there are often many different feature vector representations of the same biometric trait and the fact that matching is meant to tolerate an acceptable level of variation from stored template reduces the stringent requirement of exact recovery of the secret by the legitimate recipient that could help improved chances for meeting the other requirements. In general, context-aware steganography need to process and analyse the secret representation as well as the cover image characteristics and representation.

The success of any information hiding techniques have been evaluated against a number of steganalysis tools that have been developed over the years for these purposes. Unlike crypto-analysis tools these tools do not reveal the embedded secrets but rather report an estimate of the probability of the cover image being embedded with a secret and often these values are dependent on the percentage of the size of the secret to that of the cover. In chapter 2, we should also review these tools and in subsequent chapters we shall discuss the strength of robustness of our proposed context-aware schemes against these tools.

1.4 Motivations and Objectives

The main focus of this thesis is to develop secure and reliable steganographic tools suitable for biometric feature exchange system between two nodes using steganography. The developed context-aware system should withstand some of the biometric transmission attacks as well as meet some or all challenges in steganography field; mentioned attacks and challenges regarding biometric system and steganography as explained in previous sections. Objectives of this thesis can be summarised as follows:

- Investigate biometric-based systems to determine challenges and limitation of such systems and looking for possible and efficient steganography solutions for exchanging sensitive biometric data used for remote authentication.
- Develop a biometric recognition system that involves the smallest number of features that achieves recognition accuracy at the same level compared with original features or even higher.
- Showing and discussing how reducing the number of biometric features affects the security of steganography embedding systems.
- Based on the work of existing steganalysis tools the aim is to developing steganography that are robust and avoid detection while providing practical and secure solutions for the remote biometric authentication problem.
- Develop an optimal embedding system that guarantee less change rates of image pixel values during embedding process which make the embedding system more invisible and robust against steganalysis techniques.

- Prove and analysis how structure of the cover images affect security of embedding system and develop embedding techniques that exploit similarity between secret message (biometric feature) and cover object (image).

1.5 Main Contributions

This study investigates the possibility of the above objectives by conducting many experiments on two different publicly available face databases (Yale and ORL) used as a secret message and images from BOSSbase database used as a cover images. Moreover, experiments are testes against different statistical targeted and universal steganalysis tools. These investigations have revealed promising results in terms of steganography requirements as well as face biometric recognition requirements when compared with the well-known schemes in the corresponding fields.

The main contributions of this thesis can be stated as follows:

- Instead of traditional methods using cryptography concept, steganography concepts based schemes need to develop for transferring biometric features securely for the purpose of remote authentication.
- Develop higher invisible embedding schemes based on developing different face feature extraction schemes that aims to reduce number of features represent a secret face image without affecting the recognition accuracy.
- Analyse the work of target steganalysis tools to develop new embedding schemes that more robust against such kind of steganalysis tools.
- Develop novel embedding schemes that differentiate between embedding face biometric data and any other secret messages (text, image… etc.) based on finding similar patterns between face secret message patterns and cover cover image patterns.
- Develop robust embedding scheme based on fusing the idea of matching patterns and selection the best locations for embedding.
- Move the steganography aspect from being used in laboratories to the real world applications such as using as secure solutions for the remote biometric authentication problems in real applications such as law enforcement, forensics, and counter terrorism.

1.6 Thesis Outline

The rest of the thesis is organised as follows;

- **Chapter Two:** this chapter provides theoretical background about the main focused two branches (biometric recognition system and steganography); given in detail the requirements and components to design secure biometric embedding system. Also in this chapter literature survey about the biometric feature extraction, biometric embedding techniques, embedding based on positions selection as well as different types of steganalysis tools are given.
- **Chapter Three:** in this chapter used feature extraction methods are described in details, the structure of the statistical steganalysis tools are analyzed to propose new robust face biometric data embedding scheme. The proposed embedding scheme tested and evaluated based on the requirements of the steganography and the recognition system.
- **Chapter Four** is aimed to discuss biometric feature extraction methods; different schemes to reduce number of features that represent any face images are proposed. Moreover this chapter aimed to discuss the relation between number of face feature and the invisibility of the steganography system as well as the relation between number of face feature and the face recognition accuracy.
- **Chapter Five** is aimed at studying the optimality concept of steganographic schemes which is linked to minimizing distortion of the cover image. This chapter also aimed to differentiate between embedding biometric features and embedding any other data, explore the concept of content-based steganographic scheme. A very powerful and novel face biometric embedding technique proposed based on reducing the change rate while maintain the required payload.
- **Chapter Six:** the performance of the proposed schemes in previous chapter is tested. The test is primarily concerned with robustness against steganalysis tools by targeted as well as universal tools. Moreover modified version of the content-based scheme is proposed.
- **Chapter Seven:** include the general conclusions and potential directions for future research work.

Chapter 2
Background and Literature Survey

This chapter is primarily designed to explain and discuss the problem of biometric data hiding and highlight the state of the art works in the field. Since our aim is to embed biometric data in a cover object, then this problem differs from general steganography tasks in that it is concerned with embedding domain-dependent secret messages and requires context-aware steganography solutions. Consequently, the sought after solutions depend on the structure of the chosen biometric feature extraction scheme. Section 2.1 includes brief background description of biometric systems to include a review of the literature on biometric feature extraction methods and more specifically on face feature vectors. In section 2.2, we discuss background materials of Steganography and Steganalysis and we review the literature on most commonly used image steganography as well as steganalysis techniques based on Least Significant Bit (LSB). In section 2.3, we review the literature on recent works on hiding biometric data inside cover objects highlighting related applications.

2.1 Biometric Recognition Systems

Biometric recognition is the science of identification of individuals based on their biological or behavioural traits, such kinds of biometrics shown in figure 2.1 (Chan, 2008). It involves verification of certain body characteristics of an individual and thus is inherently more reliable secure authentication technology than existing traditional authentications that are either knowledge based (e.g. remembering password or Personal Identification Number (PIN)) or token based such as Identification Cards (ID card). Unlike the input to traditional authentication schemes, Biometrics cannot be stolen, lost or forgotten (Jain, et al., 2008). At the same time biometric systems free the user from the inconvenience of carrying sensitive tokens or remembering complex and multiple passwords.

Generally there are two main stages in any biometric recognition system: (i) Enrolment and (ii) Recognition. In the enrolment stage sample(s) of the specific biometric trait data are captured from a user and a set of discriminating digital values are extracted from the captured samples to be used as attributes of feature vector representation of the person. These feature vectors are then stored in a database to be used later as labelled templates for comparison at the recognition stage. In the recognition stage, a fresh biometric sample is presented to the system and feature vector extracted using the same scheme used at the enrolment stage. The new feature vector is then compared with those templates in the database that was constructed during the enrolment stage using a specified similarity or distance function to identify or verify the identity of a person.

In the next sub-section details of the physiological face biometric trait is discussed to cover the various steps of the process of face recognition system.

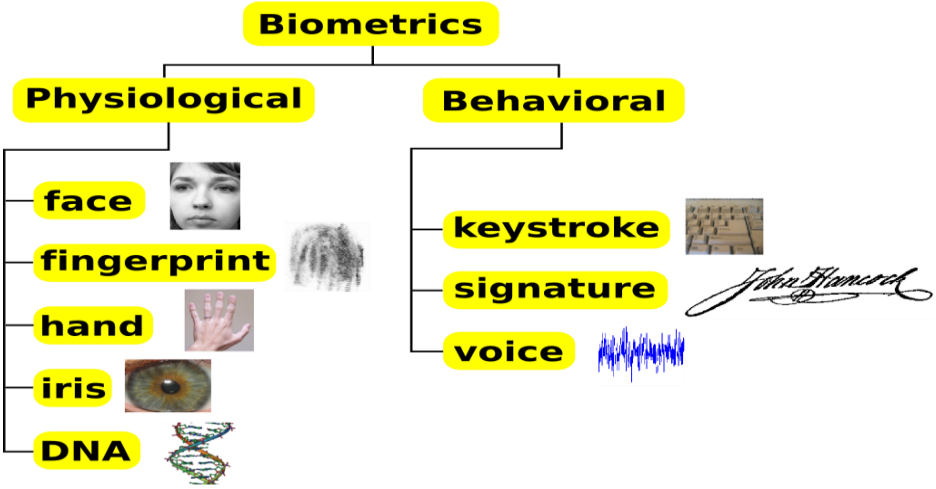


Figure 2.1: Biometric Types

2.1.1 Face Recognition System

The human face is one of the most common examples of biometric traits which represent the public identity of the person. Automatic face image analysis has received much attention by the research community for years and has wide-ranging applications in information security, law enforcement, surveillance, and access control systems. Several face biometric recognition systems together with a variety of feature extraction and matching schemes have been investigated over the past decades. Face recognition has the advantage of ubiquity and of being universal in comparison to other major biometrics, in that everyone has a face, everyone readily displays the face, and humans use it to recognize each other. Face recognition usually involves multi-step processes that include face detection, face normalization, face feature extraction, and finally classification, which could be a one-to-one matching or a one-to-many matching scenario.

In the first step, a face is automatically located and segmented from a freshly captured image. In the second stage, a normalization procedure is applied to the captured image which includes normalising face size, face pose, and illumination. Third stage is extracting features from normalized images to represent the final face image in digital form. Finally the classification process is done to determine the final outcome of a tested face image. In the literature number of different techniques are available that cover each one of the above stages and the accuracy of the final outcome (classification accuracy) depends on the robustness of each individual different stages.

The main focus of this thesis regarding face recognition system is on the feature extraction process due to the fact that this process has an impact of the structure of the output feature vector representation which in turn influences the structure and format of the secret message that we are interested in hiding it in the cover object. Here, we assume that the images presented to our proposed feature extraction processes contain only a segmented face image, but the faces are not necessarily normalized (in terms of illumination or pose). More about feature extraction process can be found in the next sub-section and briefly describe state of the art on the most commonly used face recognition schemes with focus on the schemes that are used throughout this thesis such as wavelet-based schemes and the Local Binary Patterns (LBP) based schemes in the spatial and wavelet domains.

2.1.2 Face Feature Extraction

The strategy of extracting discriminating features of a face image that are robust to varying conditions is crucial to the reliability of face recognition technologies. Feature extraction may include the acquirement of a variety of feature attributes from the image such as visual features, statistical pixel features; transform coefficient features, and algebraic features. In the remaining part of this sub-section we briefly describe the most commonly used face feature extraction methods with focus on the methods suitable for use in this thesis such as the spatial domain LBP and the wavelet-based multi-scale LBP methods.

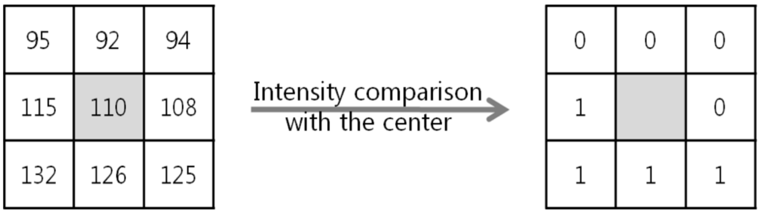
The most common approaches to extract features from face images consider the whole face image are Principal Components Analysis (PCA) proposed by Turk and Pentland

(Turk & Pentland, 1991) and the Linear Discriminate Analysis (LDA) proposed by Belhumeur et al (Belhumeur, et al., 1997). These are based on dimension reduction projections which are obtained from a sufficiently large representative training set of face images using a sufficiently small set of the eigenvectors of the covariance matrix of the training images after subtracting their average image that correspond to the most significant eigenvalues. Although these representations of face images are very compact, they are not suitable for our application because the eigenvectors need to be available on every device used which is not practical. Moreover, the recognition accuracy of these approaches is affected in uncontrolled conditions such as variable lighting conditions (Abboud, 2011; Al-Assam, 2013).

While the above approaches are based on spatial domain, there are a number of direct feature extraction schemes proposed and developed in frequency domain such as using Discrete Wavelet Transform (DWT) (Mallat, 1989; Chien & Wu, 2002; Sellahewa, 2006). Wavelet transforms is one of the example of frequency domain that have been used successfully in image processing and image analysis tasks including face recognition. These kinds of transforms have ability to reduce the original feature dimension size with small or no loss of information. Further feature size reductions can be achieved by applying the principles of PCA over Wavelet subbands such as in (Sellahewa, 2006), in the proposed not only feature vector size are reduced but also in some cases proposed significantly outperformed the traditional approach (without applying PCA) in terms of both verification accuracy and efficiency. In this thesis, discrete wavelet transform (DWT) is our chosen domain for feature extraction from the face images after the coefficient values are binaries. In the next chapter we shall give a brief description of DWTs as a multi resolution feature extractor. But at this stage we only point out that DWTs decomposes any image into a multiple of frequency subbands each representing the image at different scales and frequency ranges, and unlike Fourier transforms it also provide spatial information on the location of these frequencies. This means that we can consider each subbands as an image like data.

Local feature based approaches (Penev & Atick, 1996) aim to extract discriminative features from regions or patches surrounding facial features such as eyes, nose and mouth. These approaches are known to be robust to global changes and lead to better recognition accuracy under varying conditions compared to features extracted from entire face image approaches. These methods rely on the accurate localization of the specified facial feature. Moreover, recently more attention has been given to local window based approaches to extract features (Abboud, 2011; Al-Assam, 2013). In such an approaches the face image is first partitioned into a set of overlapping or non-overlapping regions, second features are extracted from each local region, and finally features are combined into a single feature representation (Ahonen, et al., 2006). Regarding local feature detection, Scale Invariant Feature Transform (SIFT) is a general computer vision scheme to detect local features (Geng & Jiang, 2009). The detection process in this algorithm may affect by illumination conditions and may remove some important facial features (Križaj, et al., 2010). Again these are not suitable for our applications due to the need for storage of large sets of features as well as computational cost.

Interesting types of features in face recognition field are texture features that are usually specified by the statistical distribution of spatial dependencies of grey level information. A more suitable for our purpose and efficient texture feature was introduced by Ojala et al. (Ojala, et al., 1996) named Local binary pattern (LBP) operator that helps to extract texture pattern in an image. LBP operators replace each pixel value by a binary pattern that is dependent on the order relation between the pixel value and that of certain neighbouring pixels. As shown in figure 2.2, if the neighbour value is greater than or equal to the centre pixel value, value 1 assigned to the neighbour position, otherwise 0 assigned for that position.



95	92	94
115	110	108
132	126	125

0	0	0
1		0
1	1	1

Figure 2.2: LBP Operator Example

It has shown in the literature that LBP operator to be a powerful texture descriptor yielding excellent results in terms of accuracy in a number of applications such as texture analysis, motion detection, image retrieval, remote sensing, biomedical image analysis, and face recognition. Among these applications, LBP method has shown its potential in recognizing faces (Guo, et al., 2010) under different illumination conditions and it is one of the most popular local feature-based methods. The application of LBP in face recognition was proposed by Ahonen et al. (Ahonen, et al., 2004). For face recognition an equivalence relation is defined on these binary patterns and the equivalence class histogram is used as a texture feature vector representation of the face image. These feature vectors are easy to compute, and are suitable for real time applications.

LBPs of different resolutions can be obtained through changing the sampling radius R (Ojala, et al., 2002) or by down-sampling the original image prior to adopting the LBP operator with a fixed radius (Wang, et al., 2011). Wang et al. (Wang, et al., 2011), proposed a pyramid-based multi-scale LBP approach. To begin with, multi-scale analysis is used to construct the face image pyramid using Gaussian filter into several levels then the LBP operator is applied to each level of the image pyramid to extract facial features under various scales. As a final step, all the extracted features are concatenated into an enhanced feature vector which is used as the face descriptor. A similar face feature extraction method was proposed by Liu et al. (Liu, et al., 2010) using a wavelet multi-resolution analysis. Here, low-frequency wavelet subbands (i.e. LL subbands) of several different scales are extracted as several sub-images of a subject. Then each sub-image is divided into nine non-overlapping blocks from which LBP operator extract the characteristic spectrum and statistic histogram. The methods proposed in (Wang, et al., 2011) and (Liu, et al., 2010) are both use multi-scale approach of only the approximations subband(s) coefficients of the face image and ignore high-frequency wavelet subband(s) coefficients that are known to encapsulate useful information that represent significant face features (e.g. edges and boundaries of mouth, eyes), see (Sellahewa & Jassim, 2010).

To include high frequency subbands to the process of feature extraction, face Recognition based on Haar LBP Histogram was proposed by Hengliang et al. (Tang, et al., 2010), the approach is based on decomposing the face image into four-channel subbands in frequency domain using Haar wavelet transform and applying the LBP operator on each subband to extract the face features. Related to the multi-scale LBP based, Wang et al. (Wang, et al., 2011) proposed a hand vein recognition scheme. First, a hand vein image decomposed into two levels to obtain 8 coefficient matrices: A_1, H_1, V_1, D_1, A_2, H_2, V_2 and D_2. Proposed excluded the two diagonal high-frequency components D_1 and D_2 from the feature extraction process. Meanwhile, A_1, H_1, V_1, A_2, H_2, V_2 and the original image are chosen as multi-scale components from which LBP features are extracted. Finally, LBPH features of all components are concatenated to obtain a final single feature vector representation.

In the two approaches proposed in (Wang, et al., 2011) and (Tang, et al., 2010), the LBP operator was applied on LL subbands and non LL subbands with no consideration for the differences in the frequency or feature ranges in these subbands for image features and texture. For example, applying a 2D wavelet transform (WT) on an image produces high-frequency subbands that include horizontal, vertical and diagonal features of the decomposed image respectively. Therefore, using the traditional LBP with radius 1 and 8 neighbours samples on non-LL subbands may capture useful as well as redundant information, while increasing the size of the overall face feature vector when compared to using LBP on the original image. This could be a problem for real-time identification and limit their usefulness for applications that require small feature representations. Our intended use of steganographic techniques by law enforcement agencies to communicate face biometric data hidden in innocuous cover images, is one such example. Note that increased size of secret feature vector has adverse impact on security and on the stego-image quality. However, based on the above mentioned discussions we shall investigate various versions of LBP features extracted in the wavelet domain for secure communication of face biometrics using steganography. In fact, our proposed scheme in (Rashid, et al., 2013) is a first version scheme to extract face features based on wavelets and local binary patterns (LBPs). The proposed method first decomposes a face image into multiple subbands of frequencies using Haar wavelet transform. Each subband in the wavelet domain is divided into non-overlapping sub-regions. LBP codes based on the 4-neighbour sampling points are extracted then LBPH features are extracted from each sub-blocks inside selected wavelet subband(s). Finally, all LBPHs are concatenated into a single face feature vector to effectively represent the face image. Using proposed we reduce number of features that represent face image with some degradation of the face recognition accuracy especially in cases of using wavelet LL subbands. The modified version of scheme proposed in (Rashid, et al., 2013) is shown in (Rashid, et al., 2013), in the proposed, in case of using multiple subbands to represent face image, instead of calculating LBP codes from all wavelet subbands using 4-neighbours, LBP codes based on the traditional 8-neighbour sampling points are calculated from the approximation (LL) subband(s) then uniform LBPH features are extracted, whilst 4-neighbour sampling points are used to find LBP codes from other wavelet subband(s) then LBPH features are extracted. By doing so we not just reduce number of features that represent face images compared with using original 8 neighbour methods, but also we guarantee higher recognition accuracy in most cases. More details will give in chapter 4.

2.1.3 Classification

As a final step of any face recognition systems or any biometric recognition systems in general is classification which is the process of differentiating two or more classes by labelling each similar set of data with one class. The level of randomness of biometric features is an important factor in determining the uniqueness of sample's biometric identity. In general, biometric systems deal with two types of randomness: random variations among individuals' (inter-class) and random variations within biometric samples of an individual (intra-class). Typical biometric systems obtain a set of biometric features from biometric data through features extraction techniques. A good features extraction techniques seeks to capture a maximum random variation of the first type and a minimum of the other. For this step there are number of classifiers such as nearest neighbour (NN), Support Vector Machines (SVM), and Artificial Neural Networks (ANN) classifiers. There are two phases in the construction of the classifier. The training phase, where the training set is used to decide how the features should be weighted and combined, in order to separate the different classes, and the testing phase, where the weights determined in the training stage are applied to a set of data that does not have known classes, in order to determine the class. In this thesis we shall use the simplest method to classify images which is the nearest-neighbour approach (Gonzales & Woods, 2002; Guo, et al., 2003). The NN classification measures are normally based on a similarity or distance function defined on pairs (u,v) of feature vectors. Below we present a number of measures that are commonly used for NN classifier.

- **CityBlock :**

$$D_{CityBlock}(u,v) = \sum_i |u_i - v_i| \tag{2.1}$$

- **Euclidean :**

$$D_{Euclidean}(u,v) = \sqrt{\sum_i (u_i - v_i)^2} \tag{2.2}$$

- **Correlation:**

$$S_{Correlation}(u,v) = \frac{\sum_i (u_i - \bar{u})(v_i - \bar{v})}{(N-1)\sqrt{\frac{\sum_i (u - \bar{u})^2}{N-1}}\sqrt{\frac{\sum_i (v - \bar{v})^2}{N-1}}} \tag{2.3}$$

$$D_{Correlation}(u,v) = 1 - S_{Correlation}(u,v) \tag{2.4}$$

- **Normalized Correlation (NC):**

$$S_{NormalizedCorrelation}(\mathrm{u},\mathrm{v}) = \frac{\sum_i u_i v_i}{\sqrt{{u_i}^2}\sqrt{{v_i}^2}} \tag{2.5}$$

$$\mathrm{D}_{\mathrm{NormalizedCorrelation}}(u,v) = 1 - \mathrm{S}_{\mathrm{NormalizedCorrelation}}(u,v) \tag{2.6}$$

In this thesis we will only use the Euclidean distance with the NN classifier.

2.1.4 Face Biometric databases

To test the performance of any face recognition scheme we need to use a database of multiple face images for a reasonable size population. These tests are conducted according to certain protocols for which a gallery of identity-labelled feature vectors representing all members are used as templates against which the rest of the feature vectors are matched and identification is decided according to the one of the mentioned classifiers in previous sub-section. There are number of benchmark face databases that have been recorded for the purpose of experiments, each meet certain criteria reflecting the application objectives that the database is recorded for. In this thesis we use the two most commonly used face databases that are publicly available for research purposes. The choice of these databases is based on the fact that in our application face images may not be captured under controlled conditions and these databases include sufficient variation in terms of expression, pose and lighting condition.

The Yale Database, (Georghiades, et al., 2001), consists of 15 individuals, and for each individual there are 11 face images that originally with size of 320x240 pixels of greyscale images, incorporating variations in illumination (centre-light, left-light and right-light), facial expression (normal, happy, sad, sleepy, surprised and wink), and face details (with glasses and without glasses) all images cropped to 96×80 pixel resolution and then used in the next chapters. Figure 2.3 shows some random selected samples from Yale face database.

The ORL Database, (Samaria & Harter, 1994), contains 40 distinct subjects, each with 10 different images captured in up-right frontal position with tolerance for some tilting and rotation of up to 20 degrees with 112×92 pixel resolution. Figure 2.4 shows different samples from ORL face database.

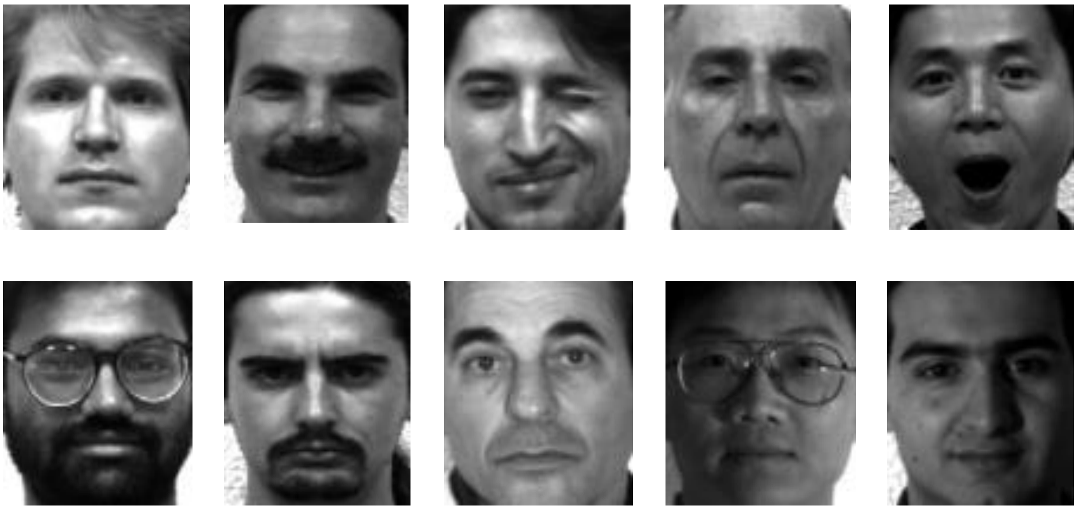


Figure 2.3: Samples of Yale Database images

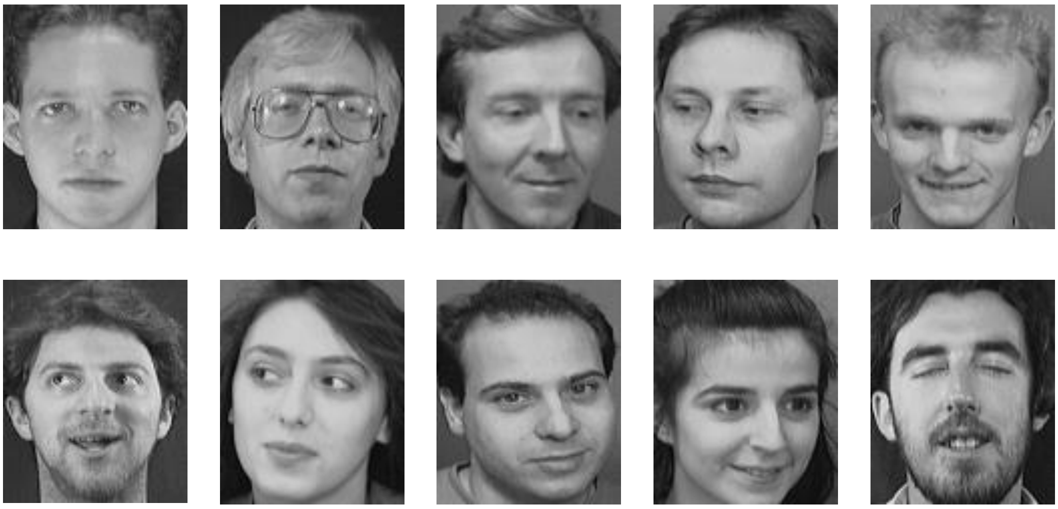


Figure 2.4: Samples of ORL Database images

2.2 Steganography and Steganalysis

The term steganography comes from Greek words Steganos meaning roof or covered and graphia which means writing (Shiva Kumar, et al., 2011). It is the art and science of hiding the fact that communication is taking place. Using steganography, you can hide a secret message inside a piece of unsuspicious information and send it without anyone knowing of the existence of the secret message. On the other hand, Steganalysis is the art of identifying stegogrammes that contain a secret message. Steganalysis does not however consider the successful extraction of the message but rather report an estimate of the probability of the cover object being embedded. In this section we shall discuss and review the Steganography and steganalysis concept in details with giving a review of the state of the art techniques in the related fields.

2.2.1 Steganography Terminology

Secret communication between two entities can be achieved through steganography. In general, in the steganography world including our works in this thesis some terminologies are required to be introduced:

- ***Cover-object or cover-medium:*** Is the carrier of the message. This could be an image, video, audio, text, or some other digital media. In this thesis, images are used as a cover-object. Therefore steganography techniques when images used as cove can be named as 'Image steganography'.
- ***Secret message or embedded message:*** This is the message need to be hidden in the cover-medium. The message could be text, image, or biometric data. In this thesis, the focus is placed on hiding the face biometric data.
- ***Stego-key:*** To make the hiding scheme more robust, a secret key can be used during embedding and extraction process. The key need to be share between sender and receiver before communication begin. Using this key is optional; therefore in some of our proposed hiding techniques we used the key while in some other keys not used.
- ***Stego-object or stego-medium:*** The object which is obtained after the secret message is hidden in the cover-medium successfully (Lin & Delp, 2001) and it is ready to send named as stego-object.
- ***Embedding process:*** Refers to the process (algorithm) of hiding secret messages in a cover object.
- ***Extraction process:*** Refers to the process of retrieving a secret message from a stego-object by the recipient (authorized person).

2.2.2 Basic Steganography Schemes

In general, any secret communication system that uses steganography concept is consists of an embedding scheme, an extraction scheme, and decision criteria. Figure 2.5 shows the general scheme of any steganography system (Fridrich & Goljan, 2002).

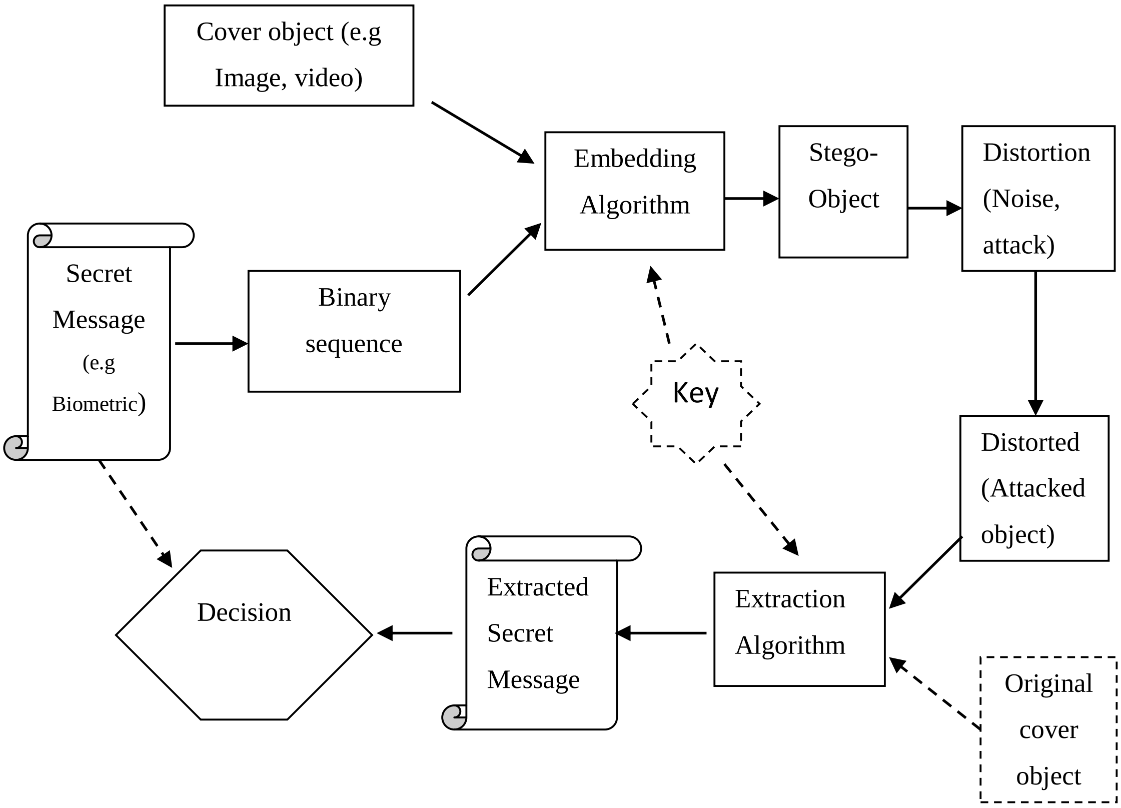


Figure 2.5: General Steganography Scheme

2.2.2.1 Embedding Schemes

As we mention before the steganography concept require the secret communication between two entities that located in different sides (sender and receiver) of the communication. In the sender side of the communication system, the secret message is converted to the bit stream and this bit stream is embedded in cover object using specific embedding algorithm. The secret message embedding technique is strongly based on the structure of the cover-object that used for embedding, in this thesis digital image used as a cover-object. The output of this scheme is the stego-object with secretly embedded message. In addition, stego-key may use during embedding process which ensures that only recipients who know the corresponding extraction key will be able to extract the secret message from a stego-object successfully (Lin & Delp, 2001).

2.2.2.2 Extraction Scheme

When the receiver side receives the stego-object that was sent by sender, recovering the message from a stego-object needs to be done. Receiver side requires the stego-image itself and a corresponding stego-key if a stego-key was used during the embedding process. The original cover image may or may not require (Lin & Delp, 2001) during extraction process (see section 2.2.4). In all our works and proposed schemes in this thesis, original cover image not used during extraction process (i.e. our work is blind steganographic techniques), this based on the fact that in real communication scenarios, the original cover-image may not available for the receiver side.

2.2.2.3 Decision Criteria

Stego-object when transmitted via unsecure channel may be subjected to attacks by third party (unauthorized person) which often includes some image processing operations such as adding noise, filtering, geometric distortion, JPEG compression. In this case some of the embedded secret message bits may destroy or missed when extracted in the receiver side. We can decide if the message extracted completely or with some distortions using BER (Bit Error Rate) which measures ratio of error bits extracted in the extraction progress. In the ideal secure hiding schemes the value of BER equal to 0 (i.e. none of the secret bits are missed)

$$BER = \frac{Error\ extracted\ bit}{Total\ Embedded\ Bits} \tag{2.7}$$

2.2.3 Fundamental Requirements of Steganographic Systems

In general, there are three main requirements for effective steganographic systems: invisibility, capacity, and robustness but we can add another one which is the number of pixels that change during the embedding process. The most important challenge in steganography is that designing a steganographic system that satisfies all these mentioned requirements together. Therefore, the balance among these requirements must be dictated by the application (Rashid, et al., 2013; Xu, et al., 2004). For example some applications may need more emphasis on high degree of invisibility, while others may require the higher capacity to hide a larger secret message (Unnikrishnan, 2011). In our proposed hiding face biometric data schemes we aim to gain high invisibility of the system with as much as possible high capacity for secret message embedding rate. We also aim to achieve robustness against steganalysis techniques. In this respect, ideally if steganalysis attacks succeed in detecting the presences of a secret message, it may or may not be possible to extract the secret message itself or even may not possible to extract the correct percentage of embedded payloads. Note that extracting hidden LBPH face feature that represent a person cannot reveal the identity of the person unless the attacker has access to the biometric database which we exclude for obvious reasons.

2.2.3.1 Invisibility or Perceptual Transparency (Security)

It is important that the embedding occurs without significant degradation or loss of perceptual quality of the cover-object. In a secret communications application, if an attacker detects some distortion then raises suspicion of the presence of hidden data in a stego-cover, the steganographic encoding has failed even if the attacker is unable to extract the message exactly (Lin & Delp, 2001).

One of the measurements used widely to calculate the visibility of the image steganography is Peak Signal to Noise Ratio (PSNR) and is computed using the following formula: (Kathuria, 2010; Chen, et al., 2010)

$$PSNRindb = 10 \times \log(\frac{\max(P'(i,j))^2}{MSE}) \tag{2.8}$$

and

$$MSE = \frac{1}{M \times N} \sum_{i=1}^{N} \sum_{j=1}^{M} [P(i,j) - P'(i,j)]^2 \tag{2.9}$$

Where M, N is the width and length of the image, $P(i,j)$ and $P'(i,j)$ represents the pixel with row number i and column number j in the original and stego-image respectively. PSNR is measured in decibels (db) therefore higher PSNR value means higher invisibility of the steganographic system obtained.

2.2.3.2 Capacity or Data Payload

It is the amount of the secret message that can be embedded in a cover-object securely without deteriorating the integrity of the cover-object. In image steganography schemes the capacity is represented by bits per pixel (bpp) (Shiva Kumar, et al., 2011).

Obviously, when less information in the cover-object embeds, the probability of introducing detectable artefacts by the embedding process is smaller than embedding higher amount (Fridrich, et al., 2001). Each steganographic system seems to have an upper bound on the maximal safe secret message length (or the bit-rate expressed in bits per pixel or sample) that tells us how many bits can be safely embedded in a given cover without introducing any statistically detectable artefacts (Fridrich & Goljan, 2002; Fridrich, et al., 2003).

2.2.3.3 Robustness (Detectability)

Here in this section we need clearly define the word robustness and differentiate between image steganography robustness and image watermarking robustness. Therefore, robustness in image watermarking schemes means that watermarking method should resist any kind of distortion introduced by standard or malicious data processing operations. Examples of common operations on images include spatial filtering, lossy compression, printing and scanning, and geometric distortions (rotation, translation, scaling, and so on). While in steganography schemes, robustness refers to how much effort is required by a steganalyst to decide (detect) whether the stego-object contains a hidden message or not. A perfect implementation of a robust steganographic scheme withstands all known attacks in the sense such attacks on the stego-object would prove to be inconclusive every time. In another word it makes no sense to perform steganography if someone can figure out how or where the secret is hidden. If someone can easily detect where you hide your secret, it defeats the purpose of using steganography. The way that steganography is usually performed to make it hard to find the hidden data is to do it in such a way that there is little change to the properties of host file. Therefore, the algorithm that is used must be robust enough that, even if someone knows how the technique works, he or she cannot easily find out that you have hidden data in a given file. In some applications steganography robustness also refers to the ability of secret embedded data to remain the same if the stego-cover undergoes transformations such as linear and non-linear filtering, addition of random noise, sharpening or blurring, scaling and rotations, cropping or lossy compression (Lin & Delp, 2001).

2.2.3.4 Number of Changed Cover Data

In image steganography, a small upper bound on the number of pixels that need to be change during embedding process is a very desirable property. Fewer changes will produce higher invisible embedding system because it is less likely to disrupt statistic properties of the cover-object (Fridrich & Soukal, 2006; Sur, et al., 2008; Wang, et al., 2010).

Reducing the amount of change may be possible to achieve by careful selecting the embedding technique positions for embedding or type of the secret message. For example in the case of traditional LSB embedding, the LSB bit of the cover image is be replaced with that of the secret message and the probability of changing the pixel values in this case is estimated to be 50%. In chapter 5, we shall investigate or propose strategies to select embedding schemes that result in much smaller number of changes in the cover image pixel values with remaining steganographic scheme at the same level of payload capacity. The proposed should also differentiate embedding biometric data with embedding any other types of secret message.

2.2.3.5 Trade-off between Conflicting Requirements

Trade-off among all above mentioned requirements are necessary, and the main challenge is to achieve a robust embedding scheme that has increased steganographic capacity while enhancing the imperceptibility or un-detectability of the secret communication. However, in general image steganographic systems capacity and imperceptibility are at odds with each other (i.e. hiding more data in cover images introduces more artefacts into cover images and then increases the perceptibility of hidden data) (Rashid, et al., 2013). Our solution regarding this challenge will be based on the investigations referred to the end of last section, i.e. controlling the number of the cover pixel value changes during embedding process with remaining the hiding system at the same level of embedding capacity compared with the traditional embedding systems (See chapter 5).

On the other hand there is odds relation between invisibility and the robustness of the hiding system; we need to find a trade-off between them. In (Rashid, et al., 2013) we proposed an embedding scheme that achieves high robustness at the expense of small amount of degraded invisibility but with optimal capacity payload. It is based on manipulating the 2nd LSB as a witness for the similarity between the secret and the LSB. More details will be given in the next chapter (chapter 3). Moreover our solution based on differentiating embedding biometric data and other kinds of secret messages proposed in chapter 5, shows that by changing less number of pixels values during embedding process we can guarantee very high invisible hiding system as well as high robustness against steganalysis schemes with remain the hiding system in the full percentage level of payload capacity.

2.2.4 Steganographic Techniques

Generally, the large number of existing steganographic techniques (Katzenbeisser & Petitcolas, 2000) can be classified in different categories. In this section, we attempt to explain and show different steganographic techniques classifications.

- ***Based on Cover Type***

Based on the type of the cover-object that used for embedding, the steganography techniques can be classified as text, audio, image, and video steganography (see figure 2.6). Most of the recent embedding techniques including our works presented in this thesis used image as a cover object, images are used as cover because it have a very common use in computer environment and shared easily on Internet. There are several reasons for using images in steganography:

- Images contain data may be not significant, changing value of those data has no effects on images functionality, while in other types of data may have effect like in text in which changing any bit will change a letter to another.
- Human visual system and its inability to distinguish minor changes in images colour.
- Images normally contain some noise, hiding information acts like adding noise; therefore it's normal when attacker (steganalyzer) notice that an image contain noise.

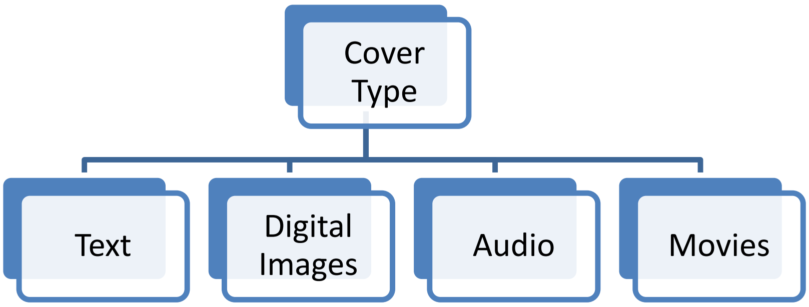


Figure 2.6: Categorized steganography based on cover type

- ***Based on Domain Used***

Steganographic techniques can be classified based on the domain that embedding technique used in. In general there are two main domains; spatial or image domain and frequency or transform domain. In spatial domain pixels values are modified directly to embed secret message such as LSB technique. Examples of frequency domain techniques are Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), and Discrete Fourier Transform (DFT). While all our works proposed in this thesis are based/implemented in spatial domain, we shall give a detail literature survey on the spatial domain hiding schemes in the next section.

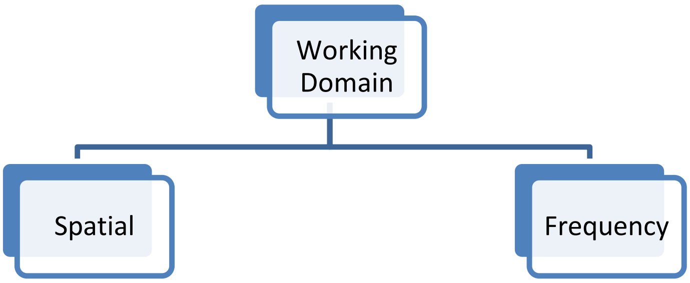


Figure 2.7: Categorized steganography based on used domain

- ***Based on Using Original Cover in Extraction Process***

Original cover object may use in extraction process. A steganographic scheme that allows extracting the embedded data without reference to the original (cover) is called blind steganographic scheme, otherwise it is called non blind (i.e. the receiver must have the original cover-object during extraction process). All proposed hiding schemes in this thesis are in type of blind steganography techniques, by taking in account the fact that in real world applications of secret communication the receiver side may not have the original object (cover) to use it for extraction process.

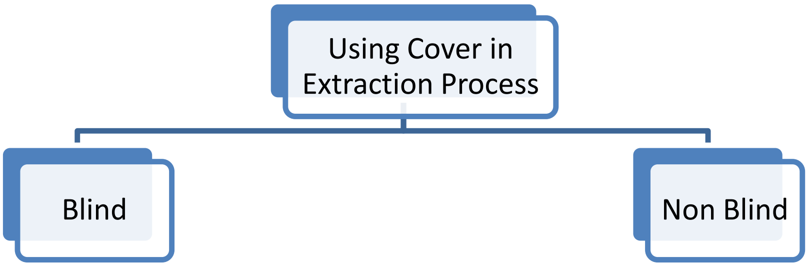


Figure 2.8: Categorized steganography based on using cover in extraction

2.2.5 The Least Significant Bit (LSB) Embedding Schemes

The most common and simplest blind steganographic method of embedding a secret message in the spatial domain of images is the Least Significant Bit (LSB) substitution. In this method LSB of a pixel is directly replaced with secret bit that need to be embedded (Yang, et al., 2008). Changing the least significant bit does not result in a human-perceptible difference because the effect of the change is very small (Lin & Delp, 2001). In the LSB technique, the information is hidden in sequential fashion. Hence the attacker can easily repeat the same technique to get the hidden information. To overcome this problem, the message that needs to be hidden is randomly spread over the cover instead of using sequential locations. Random locations are selected by using pseudo random number generator (PRNG). In this technique, a stego-key is used. The stego-key provides a seed value which is an integer that helps to generate a repeated sequence of unique pseudorandom numbers ranging from 0 to number of locations needed for embedding. At the extraction process, the same stego-key is used to extract the data (Venkatraman, et al., 2004; Singh, et al., 2007). In the same manner a new version of LSB embedding technique proposed by (Sharp, 2001), later in (Ker, 2004) the proposed named as LSB Matching (LSBM) embedding technique or ± embedding technique. In case if the secret message bit does not match the image cover's pixel value, the proposed increase or decrease randomly the pixel value by one instead of just substituting the LSB with the secret bit such as in normal LSB embedding techniques. When the process of embedding the secret message is done, LSB of the stego pixel represents a secret bit and by extracting it at the receiver side, the secret message obtained. Mielikainen (Mielikainen, 2006) propose another version of the LSB matching named as LSB Matching Revisited (LSBMR). In the method, pair of secret message embed using a pair of pixels at the same time, where the first secret message bit embed in the first pixel least significant bit, and designed binary function of the two pixel values carries the second bit of secret message. The proposed method allows embedding the same payload as LSB matching but with fewer changes to the cover image.

There is nothing that stops us to use more than one bit plane for embedding such as in (Ker, 2007), first two LSBs are used to embed two secret bits, and by doing so the payload capacity is doubled. However, embedding two bits per pixel increases the changes introduced to the cover image adversely affecting stego quality and making the stego image easier to detect. To improve robustness of the system authors in (Abdulla, et al., 2013) use first two LSBs for embedding but by embedding only one secret message bit in one of the two LSBs, by doing so authors guarantee robustness against some statistical steganalysis techniques with respect to stego image quality and payload capacity.

In the simple substitution technique we can replace n LSBs with n secret bits. However not every cover location can take the same amount of secret message. As a result, many new sophisticated LSB approaches have been proposed to improve this drawback (Yang, et al., 2008). Such as in (Dc & Tsai, 2003) pixel value differencing (PVD) based steganography is presented which let to embed less number of bits in the smooth area and higher number of bits in the edge areas by calculating the differences between each two consecutive pixels in row representation, the algorithm classify the differences in to different regions then depend on the region that the pixels are in the decision of how many bits need to be embedded will made. Using the proposed the embedding capacity increases.

In (Wu, et al., 2005) a modification of proposed technique in (Dc & Tsai, 2003) is proposed which embed in the low differences (d) level ($d < 15$) rate area (smooth area) for each two consecutive pixel, 3 bits using LSB replacement, while using the same method used in (Dc & Tsai, 2003) for number of embed bits in the edge area which is ($d > 15$), results shows that this new proposed technique increased the capacity of embedding while remain the same level of invisibility when they compared with the PVD based steganography proposed in (Dc & Tsai, 2003).

In (Yang, et al., 2008) a novel method is proposed by using LSB combined with PVD method that proposed in (Dc & Tsai, 2003) , in the proposed the number of embedded bits (k) are selected depending on difference level between two consecutive pixels , the difference levels are divided to three levels; low, medium and high. When the differences is low then selected k is small, when difference is in the high range then selected k will be large , and when the differences in the middle range then the k will be in the middle, results show that the proposed method is successful to achieve both large embed capacity and higher invisibility requirement.

In (Dc & Tsai, 2003), (Wu, et al., 2005), and (Yang, et al., 2008) which they are all used the PVD approach, the two consecutive pixels are used in the raster scanning order, this mean that in the images only the vertical edges are used to embed high number of bits while the horizontal edges used as a smooth area. For this reason authors in (Luo, et al., 2011) proposed a new method that covers the limitations of PVD by partition the original image to non-overlapping square then rotate each square by a specific degree 90,180,270. Then the new image is divided to non-overlapping group with three consecutive pixels and the second pixel of each group is used to embed. For experimental result the proposed method compared with the results obtained from (Dc & Tsai, 2003), (Wu, et al., 2005), and (Yang, et al., 2008), the results shows that the proposed method is more secure than the others.

By applying the concepts which saying that hiding secret message in the pixels that they are least like their neighbours is better than other locations, authors in (Singh, et al., 2007) proposed hiding secret message in edge pixels using Least Significant Bit algorithm and random pixel location selected among all edge locations. Authors compare the two proposed techniques with other two techniques which they are Sequential and Random Least Significant Bit algorithm embedding, for comparison purpose 20 gray images are used as a test, the experiments shows that the secret text length that embedded using new algorithm cannot estimated by blind LSB detection technique.

In embedding techniques based on edge positions we will reach the problem that some pixels that detected as an edge before embedding may not be remain as an edge after embedding, therefore this issue needed to be solved. Regarding this issue, two embedding strategy are proposed in (Chen, et al., 2010), and (Hempstalk, 2006). In (Chen, et al., 2010) a new algorithm proposed using hybrid edge detector combined with the LSB, the main aim of using hybrid edge is to increase the number of edges by using two edge detectors then combined the two edges images. The algorithm is done by blocking the image into non-overlapping raster block which the first pixel in each block contain the information about the rest pixels in the block, explain that the next pixels are edge or not. The proposed algorithm is also embed less bits of secret message in the non-edge pixels while embed large number of bits in the edge pixels. In the extraction process the same information that saved in the first pixel in each block are used to tell the receiver which pixel is edge. Experimental shows that the proposed method achieved high capacity. To guarantee the same number and positions of edges in an image, authors in (Hempstalk, 2006) proposed two new algorithms depend on using image filtering to select the embedding location (Edges) named proposed algorithms as FilterFirst and BattleSteg.In FilterFirst edges are found in r most significant bits of the pixel and embedding done in t least significant bits where $r = 8 - t$. By doing so, the algorithm guaranteed the same numbers and locations of the edges before and after embedding. While BattleSteg is combination between Filter First with hide Seek algorithm (i.e. first find the edge positions then randomly selecting the positions among edge positions for embedding). Result shows that embedding in the image feature like edge is better than using sequential and randomly choosing positions for embedding. Authors in (Islam, et al., 2014) proposed an extension version of proposed method in (Hempstalk, 2006), instead of using one LSB of the pixel for embedding and the rest 7 bits for detecting edges, here two LSB used for embedding and the other remain 6 bits are used for detecting edge positions. By doing so embedding capacity increased. Also in proposed algorithm the edges are dynamically selected based on the length of the secret message.

2.2.6 Steganalysis Tools

Steganalysis is the science of detecting the use of steganography by a third party (unauthorized entity). The main goal of any steganalysis is to collect evidences about the presence of embedded message and to break the security of its carrier. Analysis on hidden information could be described under several forms: detecting, extracting, and disabling or destroying hidden information (Johnson & Jajodia, 1998). With the growing researches in the field of steganography, the researches on steganalysis grow as well. Therefore, nowadays there are number of different and accurate steganalysis techniques have been proposed in the literature. Regarding the amount of information that is known about the embedding schemes, steganalysis schemes are pretty similar to traditional cryptanalysis methods. The steganalysis attack schemes can be divided into six types:

- Steganography-only attack: Only the data-embedded file is available for analysis.

- Known-carrier attack: Both the original carrier file and the final (hidden message embedded) files are available for analysis.
- Known-message attack: The original message before being embedded in the carrier is known.
- Chosen-steganography attack: Both the algorithm used to embed the data and the final (hidden message embedded) file are known and available for analysis.
- Chosen-message attack: The original message and the algorithm used to embed the message are available, but neither the carrier nor the final (hidden message embedded) file are. This attack is used by the analyst for comparison to future coming files.
- Known-steganography attack: All components of the system (the original message, the carrier message, and the algorithm) are available for analysis (Dickman, 2007).

As a very early stage in the field, presence of the secret message is detected visually, therefore named as visual steganalysis (attack). Visual steganalysis is defined as the process of detecting hidden messages in stego files through inspection by naked eye or by assistance of a computer. This kind of attacks may detect sequential LSB steganography techniques but not true for other techniques (Westfeld & Pfitzmann, 1999). Visual attacks examine the entire stego file (i.e. image) by remove all parts of the image covering the message that embedded in LSB plane. Figure 2.9 below shows an example of the visual steganalysis techniques which aimed to detect the four black and white images embedded in the LSB-plane.

The statistics of an image undergo alterations after embedding secret message in it using steganography. Therefore, number of steganalysis schemes proposed to detect the statistical changes in the images and named these schemes as statistical steganalysis schemes. Based on the embedding schemes that steganalysis designed for, statistical steganalysis can be divided into two types: ***Specific (Target) statistical steganalysis*** and ***Universal statistical steganalysis***.

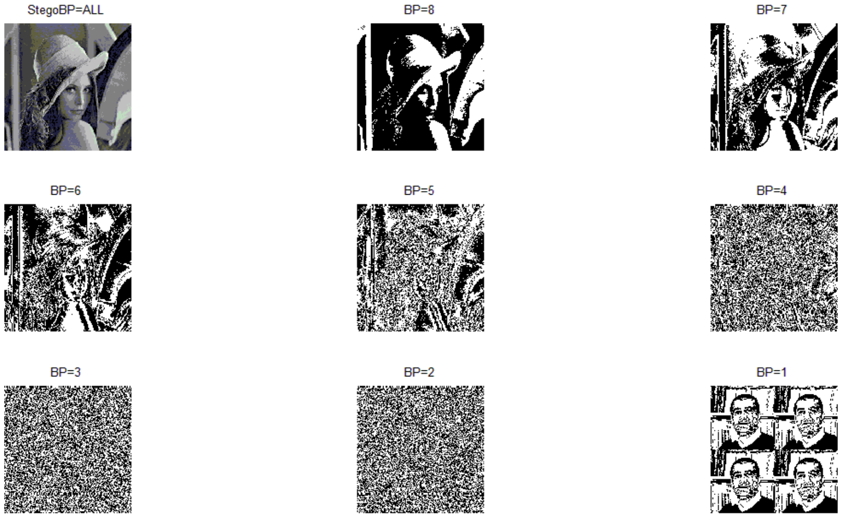


Figure 2.9: Result of visual attack

- ***Specific statistical steganalysis***

This kind of steganalysis includes the statistical steganalysis techniques that target a specific steganography embedding technique or its variations. A steganalysis technique that designed to specific steganographic algorithm would give interest results when tested only on that embedding algorithm and might fail on all other steganographic algorithms (Bera & Sharma, 2010). The design of such techniques needs a detailed knowledge of embedding process.

While the most popular and frequently used steganographic techniques including proposed/investigated techniques in this thesis are based on LSB, therefore more attention of steganalyzers go for breaking such kind of embedding techniques. The first statistical steganalysis tool is proposed by Westfield and Pfitzman (Westfeld & Pfitzmann, 1999) named as Pairs of Value (POV). This approach is preliminary designed to detect the sequential LSB embedding in greyscale cover images also the proposed shows its ability to detect randomly spread LSB in case that the number of embedded message comparable to the cover size. In (Fridrich, et al., 2000) the Raw Quick Pair (RQP) detection method is proposed when LSB method used for embedding in the 24 bit true colour images. The proposed method is based on analyzing close pairs of colours inside a colour image. The method works reliably well in case that the numbers of unique colours are not exceed 30% of the total number of pixels. A more accurate technique Regular and Singular (RS steganalysis) proposed by Fridrich et al. (Fridrich, et al., 2001) that used to detect the embedding in greyscale as well as the colour images. The technique is based on dividing images into disjoint groups and classifying groups to “regular” or “singular” based on whether the pixel noise within the group increased or decreased after flipping LSB plane. The ratio of each group is used as a base for decision whether the tested image is cover or stego. Andrew D. Ker (Ker, 2004; Ker, 2004), have evaluated POV and RS steganalysis tools and shows that the RS steganalysis performs slightly better than POV for greyscale images. Therefore, some improvements of both steganalysis are proposed that work well when greyscale images used. The improvement of RS steganalysis reliability was further increased by using different kind of flipping strategies, while POV steganalysis was improved by excluding non-adjacent pixels from the homogeneity calculation. In (Zhi, et al., 2003), the relation between the length of the embedded message and the gradient energy is used as a base for detecting presence of the embedding, therefore the method named as Gradient Energy Flipping Rate Detection (GEFR). The technique calculates gradient energy of the test image as well as the images after flipping LSB with different rates. Then the gradient energy curve is used to estimate the embedded message length. Tao Zhang and Xijian Ping (Zhang & Ping, 2003), proposed the steganalysis tool that uses the difference image histogram (DIH) method as a classifier for distinguishing between stego-images and cover images. The translation coefficients between difference image histograms used as the measure of weak correlation between the LSB plane and other bit-planes of the image as a result of randomness of the LSB in natural images. One of the best structural steganalysis tools and most sensitive targeted steganalysis of LSB based steganography currently available is revisited weighted stego-image steganalysis (RWS) proposed by Andrew D. Ker (Ker & Böhme, 2008) . The RWS steganalysis tool, is an enhanced version of the scheme that originally proposed by Fridrich and Goljan’s (Fridrich & Goljan, 2004). The technique considers that a given test image S can be used to obtain the predicted cover $\hat{C}$ image by adaptive filtering S that minimize difference between S and $\hat{C}$. And based on this idea the estimated change rate will be calculated. To detect the presence of secret message embedded using LSBM scheme Harmsen and Pearlman (Harmsen & Pearlman, 2003), proposed a steganalysis tool by exploiting that the embedding technique works as a low-pass filter on the histogram of the cover image. The method is then introduced a detector using the centre of mass (COM) of the histogram characteristic function (HCF) and they named HCF-COM.

That work was tested on colour images. In (Ker, 2005) by showing and proving that the original HCF-COM method does not work well on grayscale images. Therefore, Ker proposed a new version of HCF-COM based on the calibration (down-sampling) technique. Therefore the relation between HCF-COM obtained from original size and down-sampled one used as criteria for deciding the tested image is cover or not.

- ***Universal statistical steganalysis***

Universal statistical steganalysis tools can be defined as a tool that aims to detect different embedding schemes (i.e. not used for only specific steganography embedding technique). This kind of steganalysis need a training phase of statistical features on clean and stego images obtained from different embedding schemes. The trick of such kind of steganalysis is to find out appropriate statistical parameters with 'distinguishing' capabilities.

The very early universal statistical steganalysis tool is proposed by Ismail Avcıbas et al. (Avcibas, et al., 2001), in the proposed the detection is based on the exploiting the statistical evidence that the steganographic techniques leaves with the aid of analyzing image quality metrics and multivariate regression. In (Farid, 2002) wavelet-like decomposition is used to construct higher order statistical models of natural images. Then a Fisher Linear Discriminant Analysis (FLDA) used to discriminate between untouched and adulterated images. In (Lyu & Farid, 2002) modified version of (Farid, 2002) is proposed, instead of using FLDA they used support vector machine (SVM) to obtain better classification accuracy. The statistics of first and higher order colour wavelet decomposition and a one-class support vector machine (OC-SVM) proposed in (Lyu & Farid, 2004). As a continues work, in (Lyu & Farid, 2006), Lyu and Farid include phase statistics to the statistical model for colour images in addition to the first and higher order magnitude statistics. Therefore the feature vector size obtained is 432-D feature vector of magnitude and phase statistics. The steganalysis proposed in (Xuan, et al., 2005) based on the statistical moment in the wavelet decomposition. 39-D feature vectors are proposed for steganalysis which include first three moments of characteristic function of wavelet subbands with the 3-level Haar wavelet decomposition. The proposed shows that the extracted features after embedding will cause the changes of wavelet subbands histogram. Bayes classifier is used to classify the incoming images. Texture based steganalysis proposed in (Lafferty & Ahmed, 2004) , the tool used the Local Binary Pattern (LBP) texture operator to calculate the amount of texture present in an image followed by calculating some statistics parameters extracted from the LBP. The outputs of LBP algorithm are provided to the artificial neural network which already trained with the same statistics parameters extracted from clean and stego images. Recent powerful universal steganalysis tool is proposed by Jessica Fridrich et al. (Fridrich & Kodovský, 2012). The method named as spatial rich models (SRM) and based on calculating a very large number of different types of dependencies among neighbouring pixels to enable the detection of a wide range of embedding algorithms on the bases of the fact that any embedding scheme will create few local distortions at different scales.

As a conclusions of this section we can say some general comments;

- It is difficult to find out an effective steganalysis tool that can detect all steganographic methods.
- Most targeted steganalysis tools try to estimate the secret message embedded after the stego-image detected, while the universal steganalysis schemes are binary classification without estimating embedded secret.
- Targeted steganalysis tools not need training phase, while universal steganalysis tools are need training the system for classification purpose.

More details of individual used steganalysis tools in this thesis will be given in the next chapters especially in chapters 3 and 6, when we attempt to use them as a tool to measure the robustness of our proposed embedding techniques.

2.3 Biometric Hiding

In recent years using biometrics data for user authentication and verification increased because of its advantages over the traditional security schemes. A biometric system is vulnerable to a variety of attacks aimed at undermining the integrity of the authentication process. These attacks are intended to either circumvent the security afforded by the system or to deter the normal functioning of the system.

In (Jain, et al., 2005) an overview of the several types of attacks that affected the biometric system are described with giving some interest solutions that prevent or eliminates some of those attacks like using encryption , steganography and watermarking when the biometric needed to be transferred via unsecure communication channel. Literature survey about some used methods to secure the biometric templates is also presented. In (Dong & Tan, 2009) the overview on the methods that used in the field of security enhancement of biometric data, cryptography and data hiding are presented. Some techniques that combined the cryptography concept with biometric and other methods that combined the data hiding concept with biometric are explained also. Then problems of cryptographic key management and protection of biometric templates is presented.

Concept of steganography can be used for securely transferring biometric data, the way of using this concept are different from one application to another or from one type of biometric data to another. For example in the following proposed secure systems, each of them use different technique for hiding and also each of them used for specific application, in (Jain & Uludag, 2003) two type of scenarios are presented, the first one is hide the biometric data (fingerprint minutiae) in an image which is not related to the biometric data and transferred via unsecure communication channel to increase the security of transferring biometric data. In the second scenarios the facial information (eigen-face coefficient) is embedded in fingerprint image to increase the security of the fingerprint image. The size of the hidden data used in first scenario is only 85 byte while in the second scenario is only 56 bytes. In (Kapczynski & Banasik, 2011) an approach proposed to enhance biometric access control by utilizing steganography. Proposed method hides keyboard dynamic templates in fingerprint templates using LSB Method.

Wavelet-based watermarking method proposed in (Zebbiche, et al., 2006) , proposed hide the fingerprint minutiae data in fingerprint images. The application provides a security to both hidden data (i.e. fingerprint minutiae) and the host image (i.e. fingerprint). The method is essentially introduced to increase the security of fingerprint minutiae transmission and can also be used to protect the original fingerprint image. While authors in (Ntalianis, et al., 2011) propose a method that hides the biometric signal in the video object used for biometric authentication over error prone networks. The method apply 2 level of wavelet transform and choose two subbands for embedding with the idea of redundancy which is the same biometric signal embedded in the two subbands.

Discrete Cosine Transform (DCT) used for embedding biometric features such as in (Agrawal & Savvides, 2009) a modified DCT embedding technique is proposed by hiding the secret message which is either iris codes or fingerprint depend on the sign of the DCT coefficients. In proposed method every 3by3 DCT block used to embed single bit, to increase the capacity proposed also tried to hide more than one bit in the single 3by3 block. The proposed shows that the method more robust under the JPEG compression attack. The robustness calculated by finding hamming distance between recovered and original embed logo and the results shows that it is good for reconstruction the iris code after attacks. While in (Na, et al., 2010) two keys used one for encryption the iris code and the other is to select randomly the blocks of the coefficients in DCT domain. In each selected block middle high frequency is used to embed which they are more robust to various types of image processing attacks. For experimental, proposed method used 756 iris images from 108 eyes images, and feature of iris are extracted using 2D-Gabor filter to create a 512 bits code, this 512 bits are embedded in the cover image.

To enhance the security of transferring biometric features, different kind of combination of cryptography, steganography, and watermarking can be establish, such as in (Kathuria, 2010) a method proposed to enhance the performance of identification system using vein Biometric. Proposed method combines the principle of steganography and cryptography to ensure the security of transferring biometric data over insecure channel. And also proposed used the Run Length Encoding (RLE) as a compression technique that compresses the vein image before embedding stage. Also to achieve more secure transferring biometric data in unsecure channel authors in (Sonsare & Sapkal, 2011) combined the principles of cryptography with steganography. Proposed algorithm encrypt the biometric code by using RSA public key encryption algorithm then the encrypted data is embedded in cover image by using DCT technique which replaces the least significant bit of DCT coefficient by secret message bit. Related to the subject in (AL-Assam, et al., 2013) we proposes an approach that combines steganography with biometric cryptosystems effectively to establish robust remote mutual authentication between two parties as well as key exchange that facilitates one-time stego-keys.

Combination of asymmetric digital watermarking and steganography proposed in (Whitelam, et al., 2013), the algorithm presents a multilayer framework that first encodes eigen-features extracted from raw face images, into a fingerprint image. Secondly, each watermarked fingerprint image is encoded within an arbitrary host image unrelated to biometrics or forensics. The contributions of the work are as follows: developed an application of biometric watermarking face eigen features into fingerprint images that are usable to provide authentication; developed the process of encoding the fingerprint images into an arbitrary host image, which provides an increased level of security and authentication. Also in (Lu, et al., 2008), and (Li, et al., 2009) combination between watermarking and steganography used to improve the security and secrecy of biometric verification using lossless and content-based hidden transmission method of biometric images. Proposed hide digital watermark losslessly in the region of interest (ROI) of palm print. The watermarked ROI is hidden in the general public image using content-based steganography technology and transmitted secretly. For embedding, greyscale images are segment into different regions using watershed algorithm. The entropy of each region is calculated and the stego palm print image is embedded into cover image according to the entropy values. More information embeds in highly textured regions than in uniform regions.

Recently, one of the applications that biometric hiding used for is the transaction system and online shopping such as in (Hussam, et al., 2006) fingerprint verification technique to verify the customer (cardholder) uses in secure online shopping system that gives the Internet users the confidence to use their online shopping cards or their credit cards. The proposed system encrypts the sensitive card's information and hides it in an image using a steganography algorithm, while in (Murugesh, 2012) system proposed to establish a highly secured money transaction system. In system, protection to user integrity is given the highest priority. Proposed method as follows, a fingerprint scanner is used to get the fingerprint of the user, after which the system requests for the PIN (Personal Identification Number). Once the user enters the PIN, the user is prompted to enter the OTP (One Time Password) which is a 4-digit random password sent by the server to the user’s registered mobile number. On cross verification with the data stored in the system database, the user is allowed to make a transaction. The underlying mechanism involves combining the concepts of Cryptography and Steganography. The PIN and OTP are encrypted using AES 256. Then the encrypted data is steganographed with the fingerprint image which acts as the BASE image. The Steganographed image is sent to the server, where it is de-steganographed and verified with the data available in the system database.

In this section we explained and presented some different information hiding algorithms that used for biometric hiding. Every algorithm has its advantages and disadvantages and there is no algorithm that successfully achieves all the hiding requirements for example some of them hide more data but they are not mention to the other two requirements which they are invisibility and robustness, others achieves invisibility requirement but with low level of robustness. On the other hand, there are little number of papers that deal with hiding biometric data and mentioning the accuracy of the biometric system. For the above reasons we aimed to design and create a secure biometric hiding system that achieve the acceptable level of the requirements (Rashid, et al., 2013), more details about proposed will give in chapter 3. Also to increase invisibility of hiding system in (Rashid, et al., 2013) we proposed a very high invisibility face biometric data hidding technique by reducing number of face features need to embed with remain the face recognition accuracy rate as it is or even higher accuracy in some cases. The proposed method decomposes a face image into multiple frequency subbands using wavelet transform. Each subband in the wavelet domain is divided into non-overlapping blocks. After that local binary pattern histograms (LBPHs) are extracted from each block in each subband using only 4 neighbours to extract LBP code. Then, all of the LBPHs are concatenated into a single feature histogram to effectively represent the face image. Finally, the extracted face features are embedded in an image using one of the robust steganography techniques that proposed in (Rashid, et al., 2013) in order for them to be ready for transmission. More details will give in chapter 4.

All above mentioned methods including our own proposed schemes embed the biometric features like embedding any other secret types, by first convert the features after extracted from the biometric data to the bit stream and then embed inside the cover image bit by bit. None of them mentions that how the biometric features embedding can be differentiated from other kind of secret message embedding. We propose an algorithm that focuses on differentiate embedding biometric features from embedding other messages by benefits from characteristics of texture features such as LBPH. Proposed method try to find the match patterns between the bits of the secret message in each segment and the LSBs of pixels in the cover-image. By doing so, we can decrease the number of LSB of the pixels that are changed during embedding process. As a result of that, the distortion or noise that appear in the pixels of the stego-image will be decrease and the immunity of the stego-image against the steganalysis becomes strong. More details about such proposed schemes will give in chapters 5 and 6.

Chapter 3
Face Biometric Hiding Techniques

So far we have identified steganography as offering a suitable alternative to encryption as a mean of securing transmission or storage of biometric data, and enabling secure remote biometric based authentication. The need for such techniques can arise in law enforcement, forensics, counter terrorism, internet or mobile banking and border control. In the last two chapters we described the research problem dealt with in this thesis, reviewed and described basic steganographic concepts, challenges, and techniques of hiding secret messages (expressed in binary) inside digital images. We have also reviewed basic concepts of biometrics together with the main challenges of biometric based authentication. In this chapter we initiate our investigations and development of robust schemes to hide face biometrics in digital images. We will first describe in section 3.1 the two most efficient face feature extraction techniques (LBP and wavelet-bases). In section 3.2, we analyse the main approaches to spatial domain secret embedding techniques (including various versions of LSB), and conclude with the development of our first proposed hiding technique whereby we do not change the LSB but modify the 2nd LSB as a witness to the presence of the secret message in the 1st LSB. In section 3.3, we analyse the witness-based hiding scheme for general steganography use in terms of invisibility, payload capacity and robustness against specific statistical steganalysis techniques. In section 3.4, we shall test the suitability of the two chosen face feature vectors for embedding using the witness scheme with particular interest in payload capacity and maintenance or loss of recognition accuracy as a result of the embedding procedure.

3.1 Extracting Face Feature

One of the effective steps in any biometric recognition system is feature extraction process (Shan, et al., 2009; Sellahewa, 2006). The extracted feature represents the biometric data which is our aim to transmit it securely based on steganography techniques. In steganography field the extracted feature named as a secret message. In this thesis, face feature will be used as secret information after being converted to binary stream.

Following the discussion we had on the various biometrics and suitability for use as a secret message that can be hidden in an image we summarise the basic requirements that a face feature extraction and recognition scheme must satisfy as well as related factors.

1. Face biometric trait samples must be easy to map and represent by binary strings.
2. Capacity and invisibility requirements require the secret to be sufficiently short.
3. For security and privacy reasons the process of obtaining the binary secret string cannot be reversed to obtain the original biometric trait sample
4. The act of embedding the secret should preserve the accuracy of matching.

Unfortunately except for the LBP face recognition scheme, all schemes discussed in Chapter 2 are not suitable but for different reasons. Sure, most schemes can be binarised but into rather very long strings and may result in loss of recognition accuracy on top of having serious implications for payload capacity. Moreover, except for the LBP scheme, from the binarised feature vector the recorded sample can be approximated. In what follows we shall describe different block-wise based LBP face feature vector as well as wavelet-based face feature vectors. The suitability of these face feature vectors for embedding using the proposed witness hiding scheme in terms of the above requirements will be tested at the last part of this chapter.

3.1.1 Wavelet-based Features

Discrete wavelet transform (DWT) can be used as a face feature extraction scheme which after one level of 2D decomposition, a face image is divided into four subbands: LL (Low-Low), which is generated by the approximation coefficients; LH (Low-High), HL (High-Low), and HH (High-High), which are generated by the detail coefficients. After applying Haar wavelet transform, the given image is decomposed into $3k + 1$ frequency subbands where k is the level of the decomposition (Sellahewa, 2006). Figure 3.1 shows two level of DWT decomposition. To extract face features we applied Haar DWT to 3 decomposition levels on face image and we select one subband to represent face feature vector.

Our scheme is based on hiding binary string into images; therefore we need to binaries the extracted face feature vector. There are a number of ways of binarising face images or the coefficients in their wavelet subbands, but here we will use simple and easy method to represent wavelet subbands of face coefficients which preserve the most important features. This binarization is based on thresholding the coefficients in terms of their mean and standard deviation of the wavelet subband.

$$\text{Coefficient} = \begin{cases} 0 & \text{if abs(coeficient} - \text{mean)} < \alpha * \text{std} \\ 1 & \text{if abs(coeficient} - \text{mean)} \geq \alpha * \text{std} \end{cases} \quad (3.1)$$

Here, mean is the mean of the coefficients of a given subband, std is the standard deviation of the same subband, and $\boldsymbol{\alpha}$=0.1, 0.25, 0.5, 0.75, 1, 1.25, 1.5. Where experimentally we chose value of $\boldsymbol{\alpha}$=0.5.

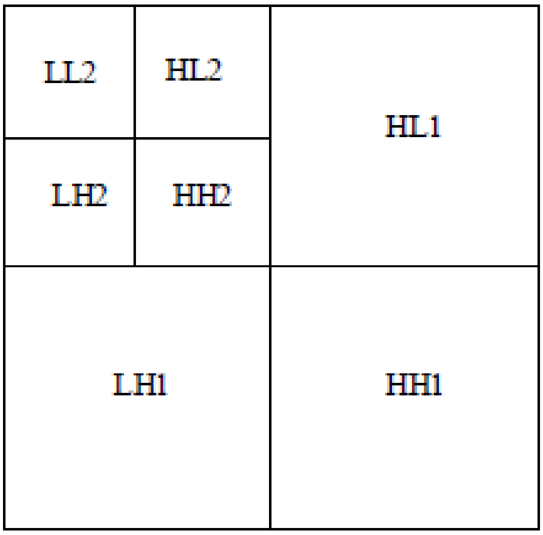


Figure 3.1: Two level wavelet decomposition of an image

3.1.2 LBP-based Features

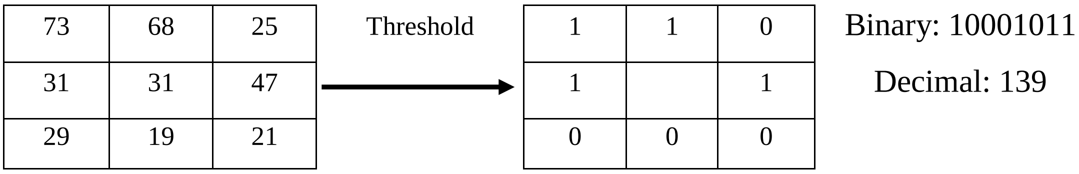
The original LBP operator was introduced by Ojala et al. (Ojala, et al., 1996). LBP normally refers to replacing image pixels with an 8-bit binary code that is derived from the pixel’s neighbourhood. For a 3×3 block, the value of the centre pixel is subtracted from that of each of its 8 neighbouring pixels and depending on the sign of the subtraction result 1 or 0 assigned to a bit. The generated bits for all the neighbouring pixels are then concatenated and encoded into binary strings in clockwise direction. The derived binary strings are called Local Binary Patterns or LBP codes. The decimal value of the LBP code for the centre pixel (xc, yc) is calculated as follows:

$$LBP(x_c, y_c) = \sum_{n=0}^{n=7} s(i_n - i_c)2^n \quad (3.2)$$

Where n runs over the 8 neighbours of the central pixel, i_c and i_n are grey level values of the central pixel and the surrounding pixels respectively, and the function $s(x)$ is defined as:

$$s(x) = \begin{cases} 1 & if\ x \geq 0 \\ 0 & if\ x < 0 \end{cases} \tag{3.3}$$

Figure 3.2 shows an example of obtaining the binary code and then converting to decimal value. After the centre pixel value 31 checked with the 8 neighbours, the binary values are assigned to the corresponding positions. Then obtained binary values are sorted in clockwise order to obtain binary code 10001011. Finally the binary code is converted to decimal value which is will be 139.



73	68	25
31	31	47
29	19	21

1	1	0
1		1
0	0	0

Binary: 10001011

Decimal: 139

Figure 3.2: Basic LBP operator

After an image is labelled with the LBP operator, a histogram of the labelled image is calculated. This LBP histogram contains information about the distribution of the local micro-patterns such as edges, spots and flat areas, over the whole image. The LBP operator $\mathrm{LBP}_{\mathrm{P,R}}$ produces 2^p different output values, corresponding to 2^pdifferent binary patterns formed by the p pixels in the neighbourhood of radius R. It has been demonstrated that certain patterns contain more information than others. To describe the texture of the images, it is possible to use only a subset of the 2^p binary patterns. Ojala et al. named these patterns as uniform patterns denoted by $\mathrm{LBP}_{\mathrm{P,R}}^{\mathrm{u2}}$. A local binary pattern is called uniform if it contains maximum two bitwise transitions from 0 to 1 or from 1 to 0 when the corresponding bit string is considered circular. For instance, 00000000 (0 transitions) and 01111110 (2 transitions) are uniform whereas 11101101 (4 transitions) and 01011011 (6 transitions) are not uniform patterns. Experimentally showed that uniform patterns constitute about 90% of all patterns in the (8,1) neighbourhood in texture images. It is easy to show that within the (8,1) neighbourhood there are only 58 uniform LBP-patterns, and the traditional uniform LBP histogram consists of 59 bins accounting for the 58 uniform patterns and one bin that corresponds to the sum of the set of non-uniform patterns (Shan, et al., 2009; Meng & Gao, 2010).

The histogram of LBP computed over the whole face image encodes only the occurrences of the micro-patterns without giving any hint regarding their locations. In order to consider the aspect of ‘shape information’ of faces, Ahonen et al. (Ahonen, et al., 2004; Ahonen, et al., 2006) proposed the division of face images into m local regions to extract LBP histograms (LBPHs), and concatenating them into a single feature histogram to represent hole image. Figure 3.3 illustrates the concept. The histogram encodes both local texture and global shape of the face images (Shan, et al., 2009). The majority of existing works including ours adopt the above scheme to extract LBP features for facial representation.

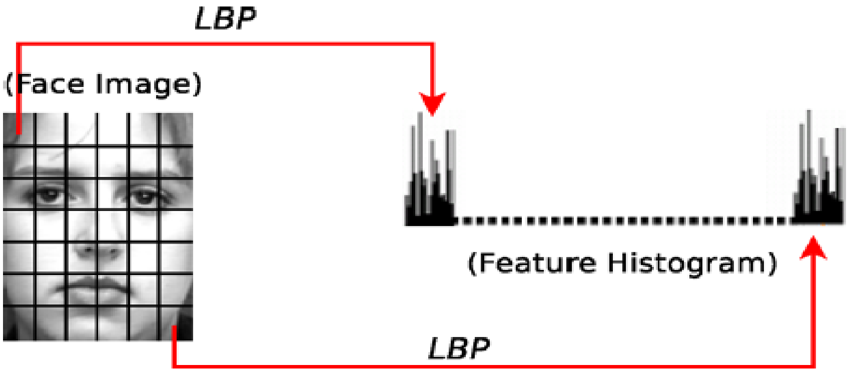


Figure 3.3: Sub block histogram concatenating (Ahonen, et al., 2004)

Therefore, for represent face features we subdivided face image into a number of blocks to represent local face features. Histogram of uniform feature set is then calculated from each block. After that, we concatenated all histogram feature sets to generate one larger feature set to be used as a final face feature representation set. Because of some bins may have larger number of 255 and we wanted to represent each bin histogram by only 8-bits, therefore final face features are normalized to integer values between 0 and 255. Normalized face features are converted to binary stream to be ready for embedding and extraction process in the hiding system.

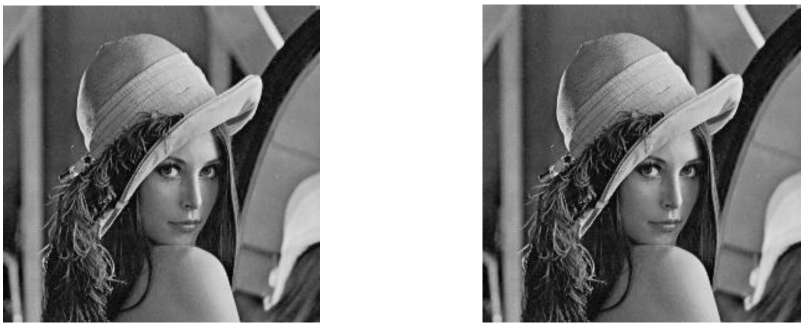
3.2 Hiding Techniques

In order to design and implement our hiding technique which is meant to be more robust than traditional ones against different steganalysis techniques we shall first analyze and discuss traditional hiding techniques that widely used in spatial domain, discussion include the strength and weakness of each of them.

3.2.1 Traditional LSB-based Steganography

In digital image terminology, the Least Significant Bit (LSB) plane in any colour channel refers to the smallest (right-most) bit of a binary sequence therefore for images this bit is refers to the smallest bit value of every pixels after the pixels converted to binary bit string. The simplest and easiest way to embedding data in an image is substitution technique. The substitution is done by replacing Least Significant Bit of image pixel with the secret bit (Johnson & Jajodia, 1998; Chan & Cheng, 2004). For this reason the embedding technique named as LSB steganography.

LSB steganography techniques will either change the value of the pixel by 1 or the pixel value remains unchanged. In case of change, the pixel value either increase by 1 or decrease by 1. This is depending on the value of the secret message bit as well as the first LSB of the corresponding pixel value. For example if three pixels of an 8-bit image values are 172, 93, and 220, then grid for 3 pixels is as follows (10101100 01011101 11011100). When the binary string representation is "***100***" and need to embed in the pixels, embedding them into the least significant bits of this part of the image will results in a grid as follows: (1010110***1*** 0101110***0*** 1101110***0***) and pixel values become 173, 92, and 220. Since there are 256 possible intensities of each grey pixel values, changing the LSB of a pixel results in small changes in the intensity of the colours. These changes cannot be perceived by the human eyes as shown in figure 3.4 thus the message is successfully hidden (Morkel, et al., 2005).



(a) Cover Image **(b) Stego Image**

Figure 3.4: Image before and after embedding using LSB

Embedding in all or part of the image pixels sequentially (pixel by pixel) named as Sequential LSB (SLSB). Changing the LSB of each pixel typically achieves high capacity. This is not secure as an attacker can simply repeat the process to quickly recover the hidden information (Hempstalk, 2006). Such as in (Westfeld & Pfitzmann, 1999), visual and statistical attacks proposed. For example the idea of visual attacks is to remove all parts of the image covering the message. The human eye can now distinguish whether there is a potential message or still image content. Figure 3.5 shows the bit planes of stego-image after sequentially embedding the logo in the LSB plane.

We can increase the capacity of embedding in one bit plane steganography twice or three times by using more than one bit plane for embedding; for example using second and third LSBs planes. In this case, the quality of the image may be affected and the technique may lose its main requirement which is invisibility (Chen, et al., 2010; Bailey & Curran, 2006). Generally noticeable distortion is appearing when the number of embedded bits for each pixel exceeds three (Amirtharajan, et al., 2010). As it is illustrated in figure 3.6:

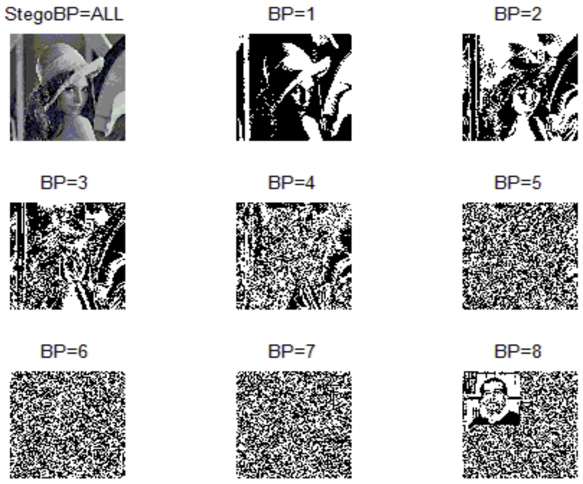


Figure 3.5: Stego-Image bit planes

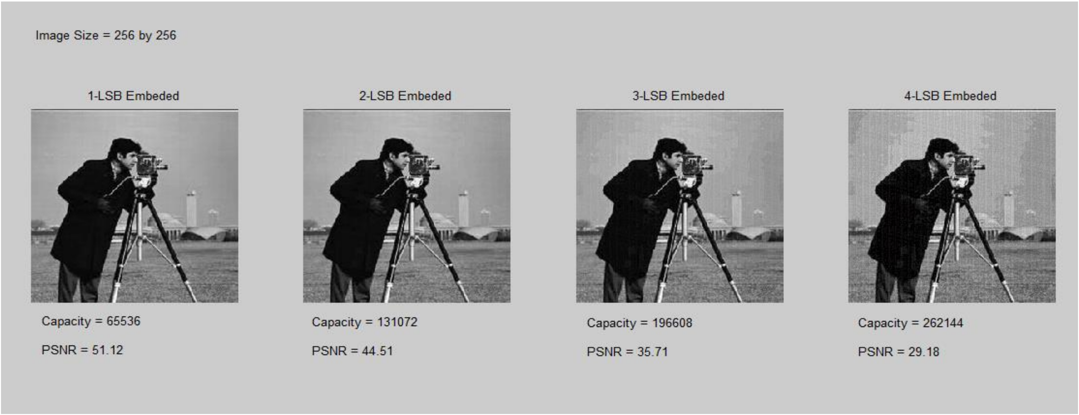


Image Size = 256 by 256

1-LSB Embeded
Capacity = 65536
PSNR = 51.12

2-LSB Embeded
Capacity = 131072
PSNR = 44.51

3-LSB Embeded
Capacity = 196608
PSNR = 35.71

4-LSB Embeded
Capacity = 262144
PSNR = 29.18

Figure 3.6: Effect of using more than one bit plane for embedding.

To increase the robustness of embedding, the pixels that are used for embedding can be selected randomly over the hole or part of the image instead of sequentially selecting pixels, these technique named as random LSB (RLSB). Random embedding positions selected based on generating random sequence using pseudo random number generator (PRNG). To generate this sequence, a seed is used. This seed used as a stego-key shared between sender and receiver to generate the same random sequence numbers ranging from $1\ to\ N$; where N is the number of pixels available in the image (Venkatraman, et al., 2004). The noise introduced by RLSB is randomly placed and often causes the resulting stego-image to look speckled (Singh, et al., 2007). Again RLSB is not robust to the statistical steganalysis that proposed in (Fridrich, et al., 2000) and (Fridrich, et al., 2001), RLSB is not robust to the proposed method in (Westfeld & Pfitzmann, 1999) especially when message length become comparable with the number of pixels.

3.2.2 The Proposed LSB-Witness Hiding Technique

As we explained in previous section, in traditional LSB image steganography, a grey value of pixels are not altered if its first LSB is the same as the bit of the secret message that needs to be embedded. Otherwise, if the first LSB is not equal to the bit of the secret message that needs to be embedded, then pixel value will change. The change is as follows: the even pixel values will increase by 1 when embedding a 1; and the odd pixel values will decrease by 1 when embedding a 0. Therefore most of the image steganalysis techniques that designed to detect LSB based steganographic techniques including the two steganalysis (Fridrich, et al., 2001; Westfeld & Pfitzmann, 1999) approaches, discussed later in section 3.3.3 exploit the above property in detecting the presence of secret data without looking to other bit-planes of the cover image. Our proposed scheme will benefit from the above properties to guarantee that the embedding does not change the LSB plane and thus robust against existing statistical steganalysis techniques.

Instead of changing LSB plane of the cover image we propose to change the second LSB plane, so that the 2nd LSB plane becomes as informer to tell the other side (receiver) how to use the 1st LSB plane relates to the next secret message bit. This uses the idea that if the secret message bit, which needs to be embedded, is equal to the 1st LSB bit of the cover image, then we make the 2nd LSB equal to 0, otherwise make it equal to 1. With this idea we can guarantee that LSB plane is not changed during the embedding process. For the extraction process, receiver only need to check the 2nd LSB plane, if the value of the 2nd LSB plane of the stego-image is equal to 0 then the secret bit is equal to 1st LSB bit, otherwise the secret bit is the inverse of 1st LSB bit. In other words, it can be said that the 2nd LSB plane is used as a witness to the first LSB plane for the extraction of the secret message in the extraction process which will be done in receiver side. For this reason, we have named our proposed method as 'LSB-Witness'. To clarify we present the following example, if M is a secret message and C is the cover image then m_k is k^{th} bit in M and $C(i,j)$ is an image pixel at the position (i,j), after we convert the pixel value to 8-bit representation we get 8-bit plane $c_8c_7c_6c_5c_4c_3c_2c_1$, which c_8 is Most Significant Bit (MSB), c_1 is 1st LSB, and c_2 is 2nd LSB of the pixel. Table 3.1 shows the process of embedding and extracting m_k bit in C. From the table we can conclude that the embedding process simply is based on logical XORing between secret bit and 1st LSB plane, the result of the process is saved in the 2nd LSB plane, while for extraction process, the secret message will obtained based on XORing between 1st and 2nd LSB planes.

Table 3.1: LSB-Witness embedding and extraction

a- Embedding truth table

Secret bit (m_k)	1st LSB (c_1)	2nd LSB (c_2)
0	0	0
0	1	1
1	0	1
1	1	0

b- Extraction truth table

2nd LSB (c_2)	1st LSB (c_1)	Extracted bit (m_k)
0	0	0
0	1	1
1	0	1
1	1	0

3.3 Analysis of the Proposed Hiding Technique

Before we analysis and discuss the experimental results obtained in real application based on proposed hiding technique which is in our case the aim is to hiding face biometric features in cover image, in this section we will discuss and analysis our proposed hiding technique in general. As any steganography technique, we should analyse and evaluate the proposed hiding technique by checking how the method achieves the main steganography requirements which they are explained and discussed in section 2.2.3. While our proposed hiding technique is based on the LSB embedding, therefore in our analysis of the method we need to compare the proposed with techniques based on traditional LSB embedding. Here the proposed method was analyzed and compared with simple LSB replacement using sequential and random spread of the secret message in the cover in terms of the main requirements described in 2.2.3.

3.3.1 Capacity

Capacity means how much information can be carried inside cover image using embedding techniques. While we change only one bit in the cover image pixel, therefore our technique can carry 1 bit per pixel (bpp) such as in normal LSB embedding (i.e. Both, our method and normal LSB are in the same level of capacity which is 1 bpp).

3.3.2 Invisibility

Since we have changed the second LSB plane in our proposed, some image quality would be lost when compared with simple LSB, still remains in an acceptable range however. To measure the invisibility of our proposed we applied the proposed on 20 grey cover images with size 512×512 shown in figure 3.7, five different payload size with two embedding strategy, sequentially and randomly.

All results are compared with simple LSB in case of sequentially and randomly respectively. Table 3.2 shows Peak Signal to Noise Ratio (PSNR) between original and stego images after embedding different sizes of secret messages, the results are average of 20 cover images that used, the results demonstrates that by increasing payload size, quality of the images will lost. In other hand we can notice that using our methods we lose some degree of the PSNR when compared with the original LSB techniques that is because we changed the 2nd LSB plane during embedding process.

Table 3.2: PSNR between cover and stego image in different payload size

Payload	Sequential LSB	Sequential LSB-Witness	Random LSB	Random LSB-Witness
0.2	58.1184	52.1235	58.1391	52.0989
0.4	55.1152	49.1036	55.1241	49.0935
0.6	53.3524	47.343	53.3634	47.3358
0.8	52.1036	46.086	52.1113	46.0879
1	51.1327	45.1163	51.1434	45.1236

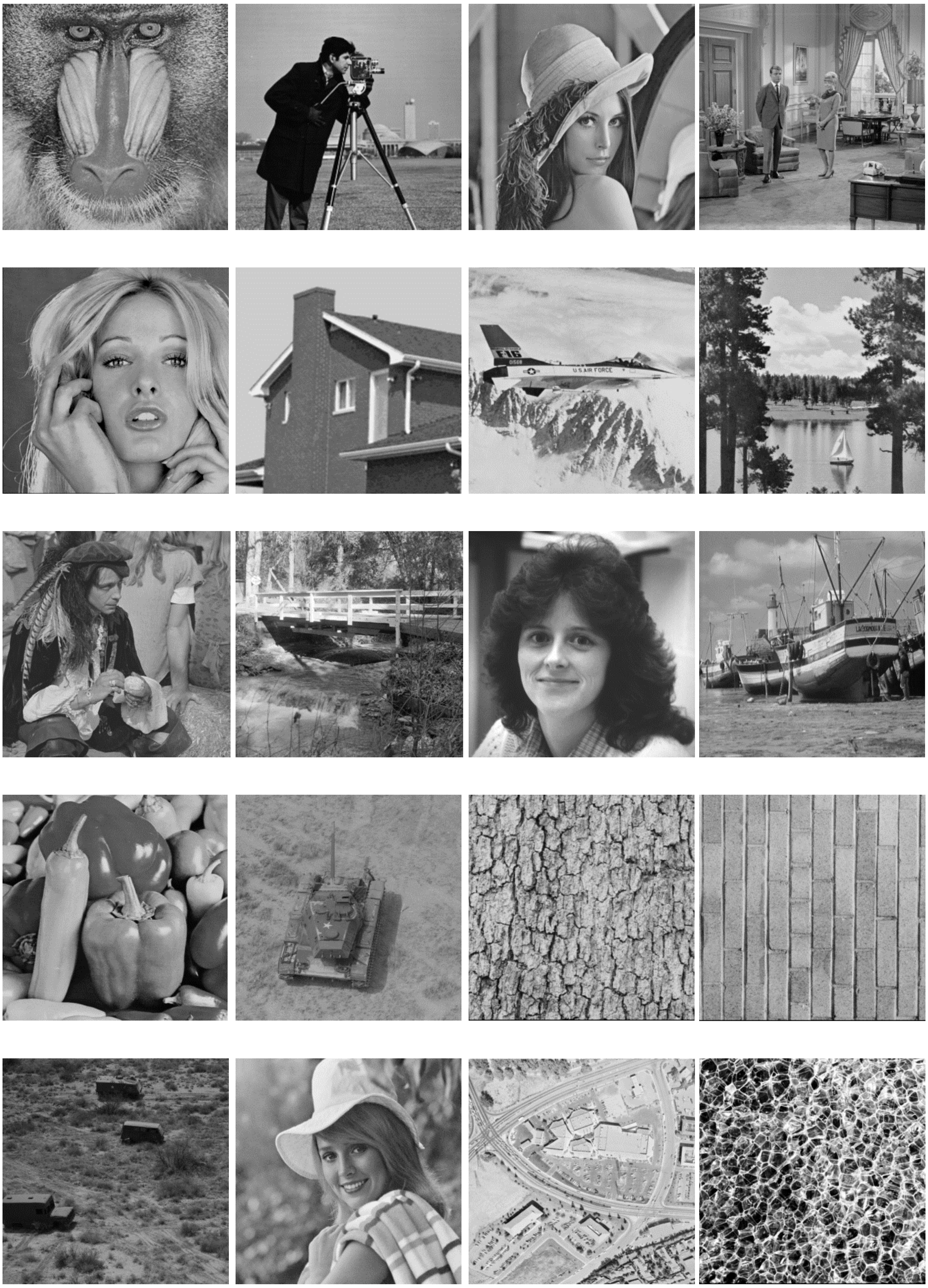


Figure 3.7: Cover images used

3.3.3 Robustness

In general, the steganalysis techniques are used to test the robustness (detectability) of any embedding scheme. Steganalysis has long been recognised as a classification techniques which aims to decide whether the tested image is clear (Cover) or not clear (Stego) image. Depending on the applications, steganalysis methods are divided into *specific* methods and *universal* methods. Specific steganalysis methods are designed to test the performance of certain steganography techniques by exploiting known implications of their embedding schemes. These specific steganlysis may not be applicable on the other techniques. Universal steganalysis methods, on the other hand, attempts to detect hidden secrets embedded by several kinds of steganography without having knowledge about the embedding technique(s). Normally this kind of steganalysis methods are based on extracting large number of different features in images that may result from embedding (Fridrich & Kodovský, 2012; Kodovský & Fridrich, 2013).

In this chapter we are only interested in test the robustness of the proposed scheme by applying some specific steganalysis techniques that are designed specifically for detecting LSB embedding. More specifically to test the robustness of the proposed scheme(s), Pair of Value (PoV) (Westfeld & Pfitzmann, 1999) steganalysis and the Regular and Singular (RS) (Fridrich, et al., 2001) are used. The PoV is to suitable and more accurate to detect sequential embedding, while the RS scheme targets random embedding strategies (Fridrich & Goljan, 2002; Li, et al., April, 2011).

3.3.3.1 Pairs of Value (PoV) steganalysis

In LSB embedding techniques, LSB's of some pixels of the original cover image are flipped if they are not equal to the secret bits. The LSB flipping causes pairs of pixel values that differ in their LSB's, (i.e. the pixel value pair patterns 0↔1, 2↔3, …, 254↔255) to be mapped to each other. The above pairs of values (2_i ,2_{i+1}) are known as the PoVs. If the bits of the secret bit stream are equally distributed, then the frequencies of both components of any PoV become equal. Therefore, the idea of the so called Chi-square ($\chi 2$) attack proposed in (Westfeld & Pfitzmann, 1999), is used to compare the theoretically expected frequency distribution of each component of a PoV with some sample distribution in the suspect image. The theoretical expected frequency distribution is, in general, estimated as the average of the two PoV components.

If n$_{2i}$ denotes the number of pixels with a gray value 2_i, then the theoretical expected frequency distribution is $(n_{2i} + n_{2i+1})/2$. For greyscale images there are 128 categories of PoVs. The χ2 test calculated between the theoretical expected frequency distribution and distribution of n_{2i}'s in the observed image is:

$$x^2 = \sum_{i=1}^{k} \frac{[n_{2i} - \frac{n_{2i} + n_{2i+1}}{2}]^2}{(n_{2i} + n_{2i+1})/2} \tag{3.4}$$

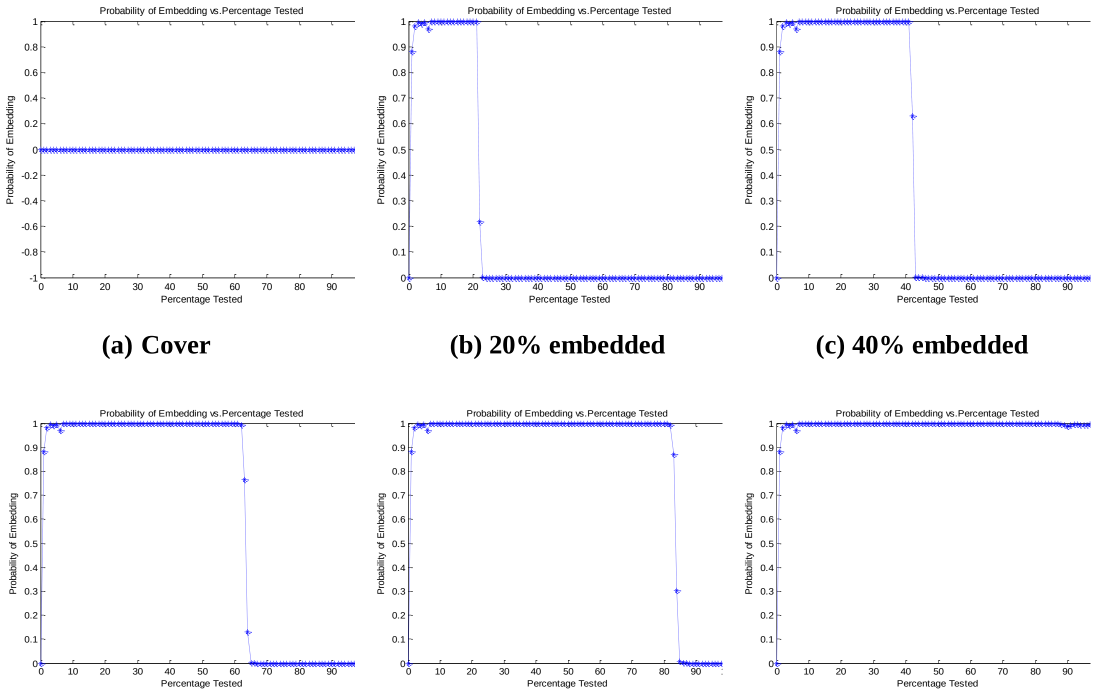
And the probability that the presences of n$_{2i}$ and n$_{2i+1}$ are equal is given by:

$$p = 1 - \frac{1}{2^{\frac{k-1}{2}}\Gamma[(k-1)/2} \int_0^{x^2} \exp(-\frac{t}{2})t^{\frac{k-1}{2}-1}dt \tag{3.5}$$

This p value determines the probability of embedding in the tested image.

For a sequentially embedded message, one can scan the image in the same order in which the message has been embedded and evaluate the p value for the set of all already visited pixels. The p value will at first be close to 1 and then it suddenly drops to 0 when we arrive at the end of the message. It will stay at zero until we get to the lower right corner. Thus, this test enables us not only to determine with a very high probability that a message has been embedded, but also determine the size of the secret message and this method provides very reliable results when we know the message placement such as sequential embedding.

With simple LSB replacement the number of modified pixel is about 50% of the stego-bits and the number of pixels with a grey value 2_i becomes roughly the same as that of 2_{i+1}. By using LSB-Witness sequential embedding the LSB plane histogram is preserved so that the signature that is detectable to the χ2 test is removed. Figures 3.8 and 3.9 show the robustness of the simple sequential LSB and sequential LSB-Witness of the same image respectively with different load of secret messages (See Appendix A for more examples). The demonstrated curves represent the p value as a function of the pixel numbers that were embedded in the test image. It can be noticed that the technique detects the stego image in simple LSB after embedding small capacity length of the image size; while it fails in our embedding algorithm when we use any size of embedding even with embedding 100% of the capacity.



(a) Cover

(b) 20% embedded

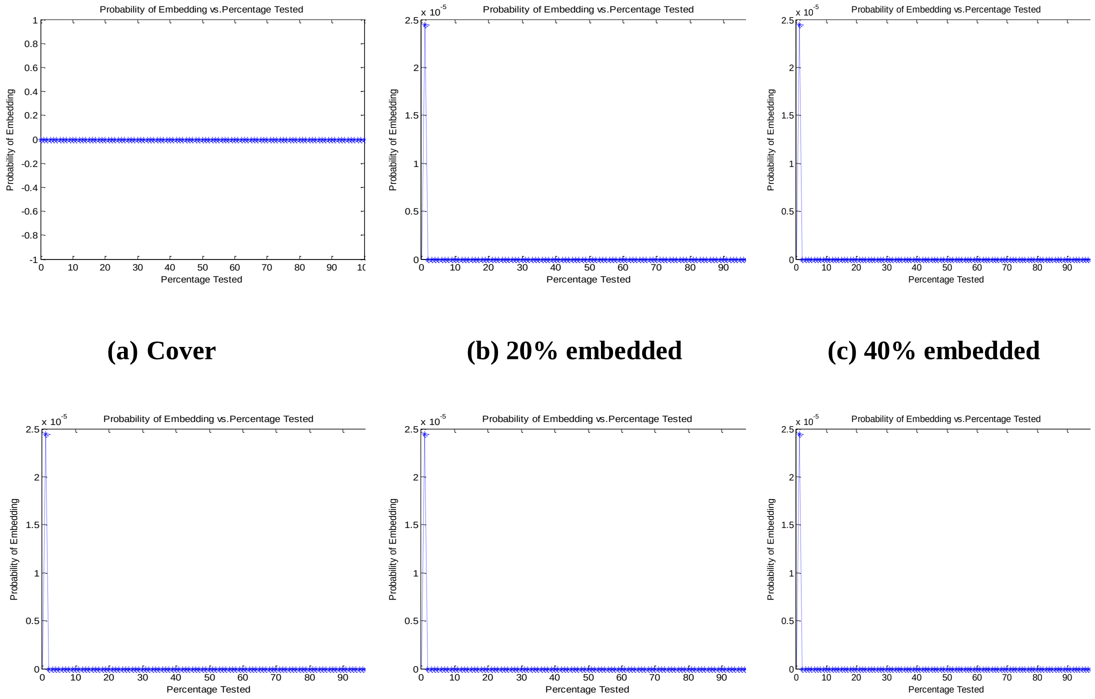
(c) 40% embedded

(d) 60% embedded

(e) 80% embedded

(f) 100% embedded

Figure 3.8: SLSB detection using PoV steganalysis for different payload for Woman blonde image



(a) Cover

(b) 20% embedded

(c) 40% embedded

(d) 60% embedded

(e) 80% embedded

(f) 100% embedded

Figure 3.9: SLSB-Witness detection using PoV steganalysis for different payload for Woman blonde image

3.3.3.2 RS steganalysis

This tool, introduced by Fridrich et al. (Fridrich, et al., 2001), is based on grouping non-overlapping blocks of consecutive pixel of an image into three groups: Regular, Singular and Unchanged. This grouping is based on the order relation between the sum of differences between all pairs of neighbouring pixels in the original block and the same sum when the LSB values in the group pixels are flipped. If the sum of the differences increases (decreases) after flipping then the block is said to be singular (regular) and the block is said to be unchanged if sum of the differences do not change after flipping. The relation between the relative number of regular groups and singular groups in the image will determine whether the image is clean (cover) or not clean (stego). The RS scheme can also be defined using a different flipping scheme to the traditional one (see below).

The RS algorithm works as follows. Given an M×N greyscale image (i.e. pixel values between 0 and 255 represented as an 8-bit unsigned byte). The image is subdivided into small disjoint groups G of n consecutive pixels x. For each block we calculate the following discrimination function before and after applying a specific flipping map

$$f(x_1, x_2, \dots, x_n) = \sum_{i=1}^{n-1} |x_{i+1} - x_i| \tag{3.6}$$

This method adopt two flipping F maps: F_1 for 0↔1, 2↔3, …, 254↔255 and shifted F_{-1} for −1↔0, 1↔2, …, 255↔256. Each block G is labelled as regular (R), singular (S), or unchanged (U) as follows:

```
If f(F(G)) > f(G), G is labelled as an R block
    Elseif f(F(G)) < f(G), G is labelled as an S block
        Else G is called an unchanged U block.
```

When f(G) is a discrimination value of received image, while f(F(G)) is a discrimination value of received image after applying flipping strategy. When using the F flipping map the groups are labelled as R, S, and U. While, when using the F_{-1} flipping map the groups are labelled as R_{-1}, S_{-1}, and U_{-1}.

R_M is defined as the ratio of blocks of regular R groups, and S_M as the ratio of blocks of singular S groups. Similarly, another two parameters R_{-M} and S_{-M} defined when F_{-1} is applied.

For 'clear' image (i.e. images with no hidden secret), the expected values of the ratios satisfy the inequality:

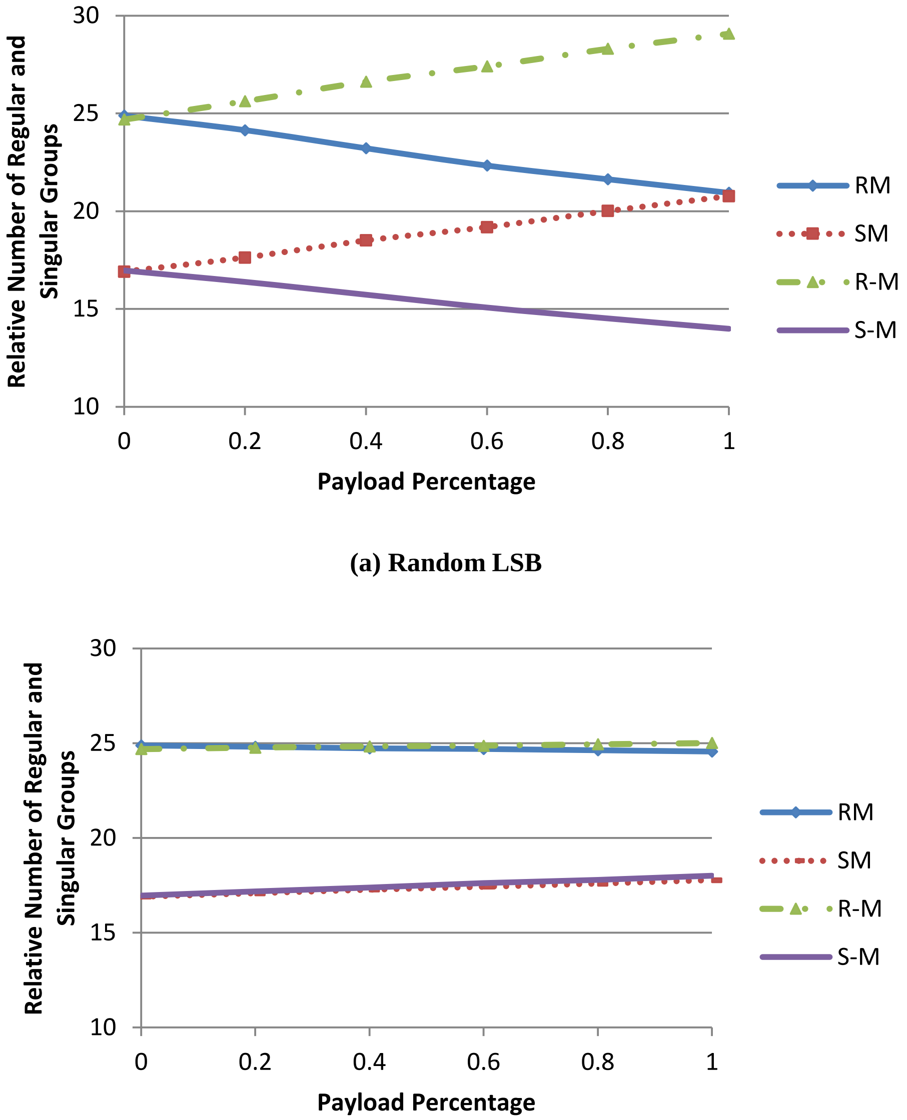
$$R_M \approx R_{-M} > S_M \approx S_{-M} \tag{3.7}$$

However, for images that contained secret bits the difference between R_M and S_M is decreases to zero as the length of the secret message increases. Embedding has the opposite effect on relation between R_{-M} and S_{-M} in which the difference between them will increase.

After applying simple LSB replacement techniques, the number of regular and singular groups become closer to each other when F_1 and F_{-1} are applied to part or all of the pixels in a stego-image so that $R_M \approx S_M$.

We subjected stego images obtained with our witness embedding algorithm with different payload, using both F_1 and F_{-1} mappings, we found that in all cases the RS steganalyser did not distinguish them from clean images, i.e. $R_M \approx R_{-M} > S_M \approx S_{-M}$.

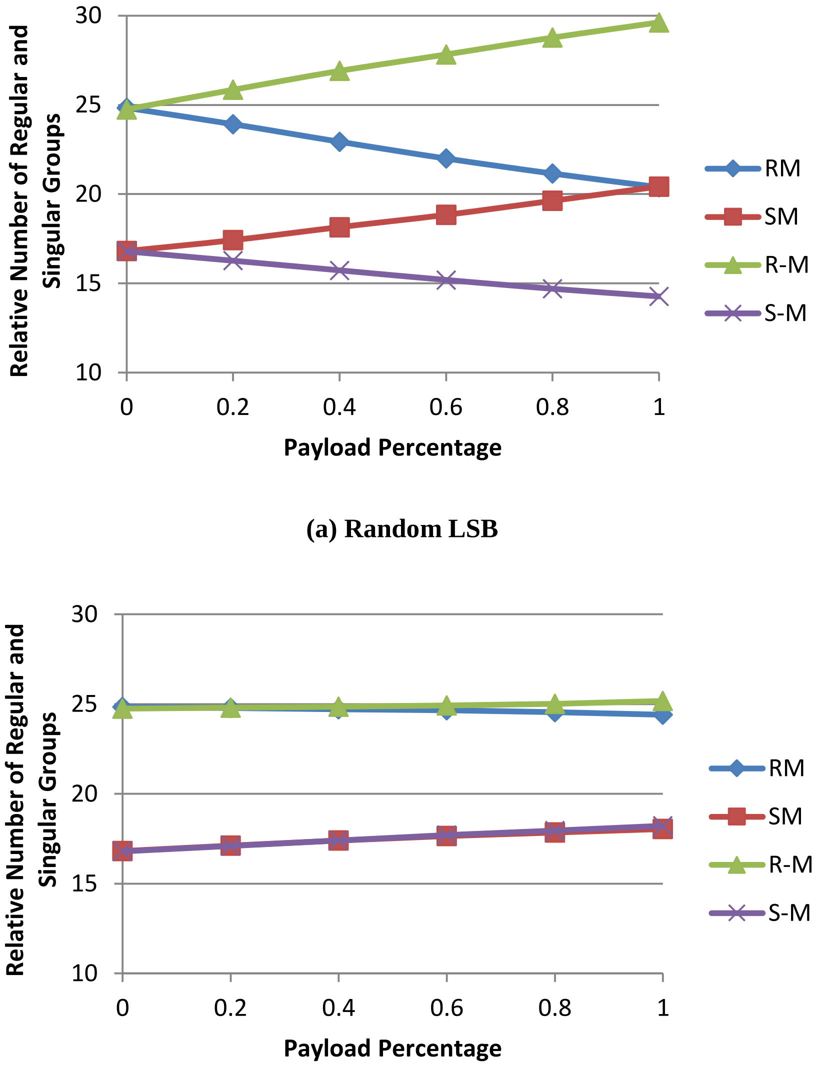
This conclusion is based on applying our algorithm as well as the random LSB on 20 images. Figure 3.10 shows the results obtained for Lena image while figure 3.11 shows the output average charts for the regular Vs singular group for different embedding payloads using the simple random LSB embedding technique and our algorithm where used (See Appendix B for more examples). From the figures, it can be noticed that when using the random LSB after using 20% of the cover image for embedding, the difference between values of R_M and S_M decreases, the difference between them continues to decrease further until a point is reached where the value of R_M and $S_M$becomes nearly the same. This occurs when 100% of the cover image is used for embedding. This does not occur when we use our method for embedding and the difference between R_M and $S_M$remains as a clean image. In other words, unlike the LSBR scheme, our scheme is robust against RS at all payload proportions.



(a) Random LSB

(b) Random LSB-Witness

Figure 3.10: RS-diagram for different payload, Lena image used



(a) Random LSB

(b) Random LSB-Witness

Figure 3.11: Average RS-diagram of using 20 images

3.4 Embedding Face biometrics using LSB-Witness Scheme

In this section we shall investigate the embedding of the two chosen face biometric feature vectors, namely the wavelet features and LBPH features. We shall test and compare the performance of the LSB-witness scheme for those two types of secrets in terms of the steganography requirements as well as preservation of recognition rates. For that we shall use a benchmark face database for which we already know the performance of the two chosen biometric schemes. For cover images we also need to select a number of different images that have different properties in terms of texture as well as the statistical properties of the bit-planes.

In real steganography application scenarios, one may not use all pixels of the cover images for the purpose of embedding. For this reason in the following experiments we embed the exact extracted binarised face feature vectors as explained in the beginning of this chapter in section 3.1. The general framework of face biometric embedding system explained in figure 3.12 below.

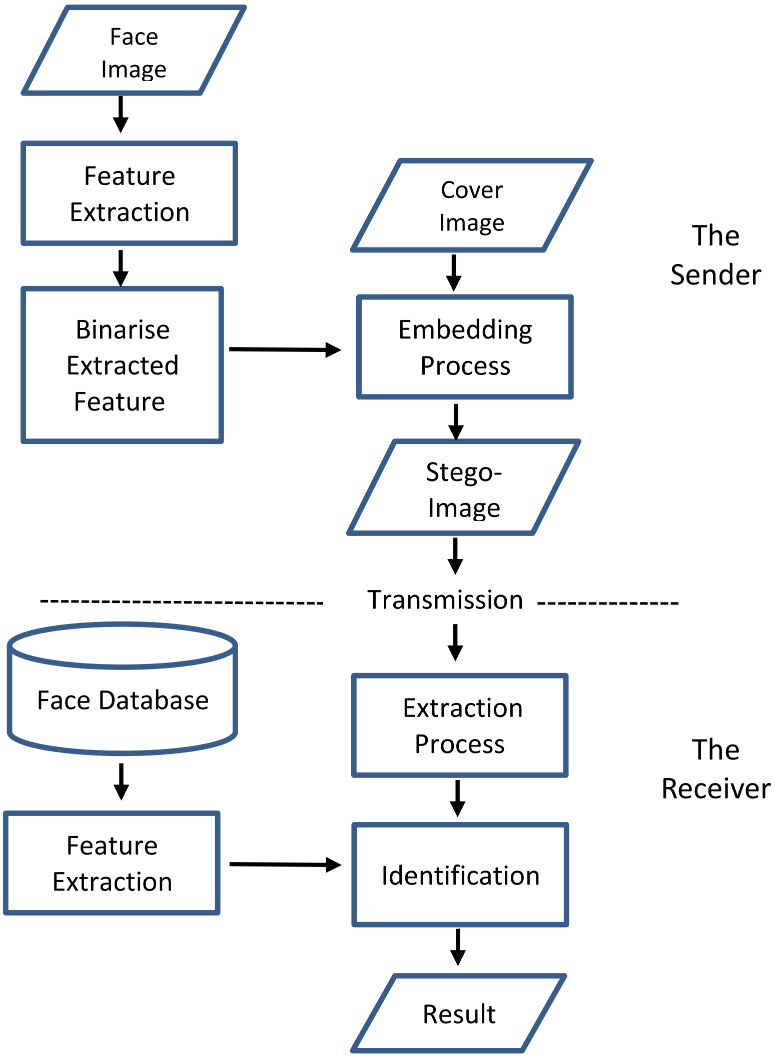


Figure 3.12: General framework of proposed face feature hiding system

For the purpose of the experiments, the same 20 images that shown in figure 3.7 were used as cover images with size of 512 x 512 pixel resolution, selected images are commonly used in the field of image processing which they are different in properties regarding containing smooth and textures areas. While our main aim at this stage is to test the performance of the proposed LSB-Witness embedding scheme we just select and use the well-known Yale Face Database as a secret message as well as for the purpose of testing biometric recognition performance. The extracted face features are used as secret messages for embedding as well as testing the recognition rate after extraction. The database consists of 15 individual subjects and there are 11 different greyscale images per subject more detail about database can be founded in section 2.1.4.

In the case of DWT face biometric, we select the 3rd level of wavelet subbands to represent face images from which the secret feature vectors is extracted. Accordingly we would have 4 different wavelet schemes. After the entire subband binaries, then the binarised features will be ready for embedding process. While in the case of LBPH face feature vectors, we shall use 4 different spatial domain schemes using different blocking number. Again here we binaries the extracted LBPH features to be ready for embedding. These various face recognition scheme are by no mean the most performing schemes in terms of recognition, but here our interest is testing the impact of the LSB-witness embedding scheme on the face recognition accuracy rate of each scheme. In what follows we shall analyse our experimental results in terms of each steganography and face recognition requirement separately.

3.4.1 Payload

Payload requirements can be checked by the number of bits needed to be embedded as well as the suitable locations. We summarize payload need using each type of feature with different sub-blocking and different sub-bands in table 3.3. Recall that in the case of LBPH, we represent each histogram bin by 8-bits under the assumption that there would be no uniform or non-uniform LBP code that has a frequency greater than 255. This assumption is based on the fact that the face image (or the block) size is modest and the likely hood of having LBP codes repeated by more than 255 is fairly small. However we could remedy this by using k-bit representation of bins where k is the maximum size of any of the bins. Instead of this approach, we opted to final face features are normalized to integer values between 0 and 255, and we accept that the consequences of that is a slight loss of accuracy of recognition at the other end (see section 3.4.4). Accordingly, the payload values given in this table for the LBPH schemes are only estimates of the actual values, due to the possibility of having some of the bins having more than 255, and this seem to be only probable when we do not divide the image or the case of 2x2 subdivisions. Note that in the case of wavelet face features; each coefficient is binarised using the mean and standard deviation in the subband, to 0 or 1. Consequently the length of the secret is fixed.

Table 3.3: Payload for each extracted feature

Extracted Feature	No. of block / Subband	No. of feature	Payload in bits
LBP Histogram	1×1	59	472
	2×2	236	1888
	3×3	531	4248
	5×5	1475	11800
Binariesed Wavelet coefficients	LL3	120	120
	HL3	120	120
	LH3	120	120
	HH3	120	120

For the choice of the cover image we assume that payload cannot be larger than the number of available locations for embedding, i.e. dependent on image size. The payload values above are all modest and image sizes in the range 100x120 should be sufficient. In our experiments we opted for images of size 512x512, and hence our LSB-witness scheme comfortably meets the requirement even for 5% payload.

3.4.2 Invisibility

PSNR is calculated between original cover and stego image after embedding secret message (face features) in each case and is compared with simple LSB embedding. Results (average of 20 images) are shown in table 3.4 in which it is clear that we lose some degree of PSNR in our method when compared with simple LSB but still in acceptable ranges of quality. Also it can be noticed that we will get higher value of invisibility in case of using wavelet subband coefficients compared with using LBPH features; this is because the number of features that was used as a secret message is low. How using a fewer number of features may affect face recognition rate is investigated and explained in section 3.4.4.

Table 3.4: PSNR between original and stego images

Extracted Feature	No. of block / Subband	Sequential LSB	Sequential LSB-Witness	Random LSB	Random LSB-Witness
LBP Histogram	1×1	78.5865	72.9423	78.6009	72.5176
	2×2	72.5527	66.5625	72.5409	66.5272
	3×3	69.0165	63.0357	69.034	62.9388
	5×5	64.579	58.5864	64.5962	58.5904
Binariesed Wavelet coefficients	LL3	84.383	78.4019	84.6797	78.3312
	HL3	84.3885	78.4542	84.6637	78.4209
	LH3	84.3873	78.4162	84.6466	78.2221
	HH3	84.4208	78.443	84.6435	78.3066

3.4.3 Robustness

Robustness of our LSB-witness algorithm against the two main LSB-related PoV and RS steganalysers were established in section 3.3.3 for all payload proportions including 100% embedding. Using the above calculations of the payload requirements for the two face feature vectors, one can conclude that both features require less than the full capacity if we to use reasonable size cover image, and hence our biometric features are secure when transmitted, hidden in an innocuous image, over an open channel.

3.4.4 Recognition Accuracy

As we describe earlier in chapter 2 that the process of differentiating two or more classes by labelling each similar set of data with one class called recognition accuracy. To test the goodness of features extracted in this chapter we calculate the recognition accuracy post embedding a biometric template by adopting the Leave-One-Out strategy or protocol. This means we present each of the images of each person in the database for recognition, while all other images are as belonging to the gallery. The classification is based on the nearest neighbour (NN) with Euclidean distance. We normalizes LBPH features to the range of integer values between 0 and 255. For the wavelet-based recognition we binaries the wavelet subband coefficients before embedding, therefore the face recognition accuracy may be affect compared with the original face feature vectors used. Table 3.5, shows the average recognition accuracy rate for all cases before and after normalization or binarisation process. We notice from the results in case of using LBPH features; the recognition rate will degrade but fortunately by a small amount as compared with the original LBPH features (i.e. without normalization) before embedding. The effects are higher when the numbers of blocks are smaller such as in case 1x1 and 2x2 blocking, due to the fact that in those cases there are more full bins, i.e. have greater than 255 LBPH values. The degradation in accuracy was worse in the case of 1x1 blocks. This could easily be explained by the fact that, in this case, 1375 bins out of a total of 9735 bins had bin values > 255. However, when the face feature vectors were the binarised wavelet subbands coefficients then except in case of using LL subband, in all other subbands we obtain better recognition rate if compared with not binarised coefficients. The large drop in accuracy for the case of the LL3 subband, compared with the significant improvements for the other high frequency subbands, can be attributed to the fact that the adopted binarisation for the non-LL subbands is based on the fact that the coefficients in each of these subbands have Laplacian distributions where the significant coefficients (in terms of face recognition) are the furthest away from the mean of the subband (Al-Jawed, 2009; Al-Assam, 2013). This is not true for the LL subband.

Table 3.5: Face biometric recognition accuracy

Extracted Feature	No. of block / Subband	Recognition Accuracy after Embedding	Recognition Accuracy before Embedding
LBP Histogram	1×1	73.93	77.57
	2×2	85.45	86.66
	3×3	91.51	92.12
	5×5	95.75	96.36
Binaries Wavelet coefficients	LL3	76.36	83.03
	HL3	75.75	74.54
	LH3	87.87	77.57
	HH3	69.09	55.15

In summary, we note that the embedding requirement (normalization/binarisation) does have some mixed effects on the face recognition accuracy, but the pattern of accuracy rate before and after embedding is different for the two schemes. Taking accuracy rates only as the bases of selecting the desirable face feature vectors would certainly favours the use of the LBPH with 5x5 block partitioning. However, the price for this would in significantly higher payload capacity than that needed for embedding any of the wavelet subband feature vectors. While each of the wavelet subband schemes requires only 120 bits, the 5x5 LBPH scheme requires 11800 bits. The implication of these different capacity payloads in terms of invisibility would certainly be a factor that needs to be taken into account when deciding the choice of face feature vector. Table 3.4 that with witness-embedding scheme the 5x5 LBPH scheme achieve a PSNR of 58.5904, while the best performing LH3 wavelet scheme achieves a much higher PSNR of 78.222. The outcome from these results raises the possibility of investigating a new solution to be based on combining these two approaches (wavelet-based and LBPH-based) to extract one final face feature vector rather than using one of them alone. Extracting LBPH features from wavelet subbands reduces the block sizes and may reduce, if not element, the need for normalising the corresponding LBPH bins. These investigations will be conducted in the next chapter.

3.5 Conclusions

In this chapter we proposed a robust steganographic scheme which was primarily developed for hiding two different face biometric feature vectors. The proposed LSB-witness embedding scheme, is based on modifying the 2nd LSB as a witness for the presence of the secret bits in the 1st LSB, and was motivated by the requirement for robustness against steganalysis schemes that target LSB-only hiding schemes. We analysed and evaluated the proposed scheme for robustness and invisibility for different payload capacity. We have shown that for general secret messages the proposed scheme is robust against PoV and RS steganalysis tools for all and up to 100% payload without introducing additional visual distortion to the cover image. We have also investigated two types of face biometric schemes (blockwise LBPH and Wavelet subbands) that could be binarised and hidden in natural image for remote authentication. We tested the performance of the various schemes belonging to these two types, before and after embedding in a number of natural images in terms of recognition accuracy. We also tested the effect of embedding these various feature vectors on robustness of the LSB-witness steganographic scheme, invisibility and payload capacity. These experiments had shown beyond any doubt the viability of using steganography for remote biometric-based recognition provided that the biometric feature vectors can be binarised, without leaking information on the freshly recorded biometric sample, with reasonable length. The various test results have demonstrated that each of the two types of face feature vectors have advantages and disadvantaged, when hidden in natural images, but to different degrees in relation to the various success parameters. This has provided strong motivation to combine the two schemes for optimal benefits. In the next chapter, we investigate an innovative solution that extracts a variety of LBPH features from wavelet-subbands of face image to be embedded in natural images for remote biometric authentication.

Chapter 4
DWT-based LBPH Face Feature for Secure LSB-Witness Hiding

From the discussion and reviews conducted in the earlier chapters we noted that embedding smaller size secret messages results in higher invisibility of the hiding system achieved. In the last chapter we initiated our investigation into our hypothesis that steganography can provide reliable tools for remote biometric based authentication developed our new LSB witness hiding scheme to meet robustness against known steganalysis tools that target LSB-only hiding schemes and tested viability of our hypothesis using two types of binarised face feature vectors. The various experiments in the last chapter have demonstrated the validity of our hypothesis but also raised the need to combine more than one face scheme for improved and optimal face recognition accuracy. In this chapter we propose various wavelet-based LBPH face feature schemes generate lower payload while achieving the same level of face recognition rate or even higher when compared with the spatial domain LBPH scheme discussed in the last chapter. We test the performance of these schemes in relation to the embedding success criteria defined earlier.

4.1 Multi-scale LBP and Wavelet Decomposition

Discrete Wavelet Transform (DWT) decomposition of a face image yields a low-frequency subband and number of high-frequency subbands in a multi-resolution manner at multiple scales (Sellahewa & Jassim, 2010). From chapter 3, one can deduce that each subband provides a representation of the face with its person discriminative contribution or capability that is suitable for steganographic embedding.

The 3x3 neighbourhood of the spatial domain LBP operator, discussed in sub-section 3.1.2, is of limited texture representation when the dominant features are part of large scale structures. The LBP operator in the spatial domain can be extended to deal with such cases using neighbourhoods of different sizes. For this it is customary to use the notation (P, R) to denote a neighbourhood of P sampled points on a circle of radius of

R (Ojala, et al., 2002). Such an extension can be achieved in two ways; either by applying LBP operator in the spatial domain neighbourhood (P,R) with increased radius R as shown in figure 4.1 or by down-sampling the original image prior to applying the LBP operator with a fixed radius.

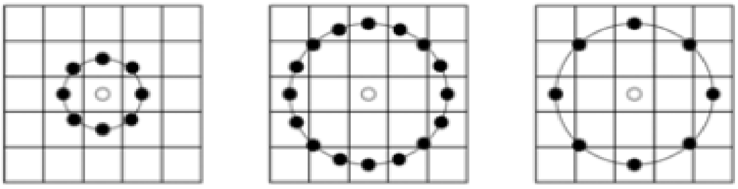
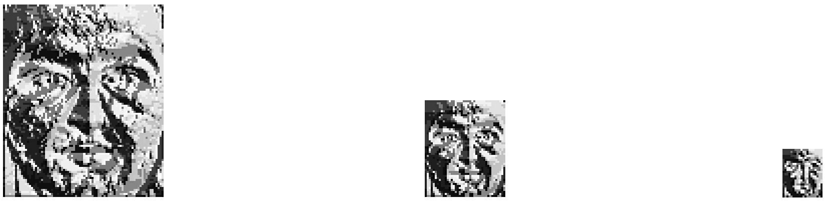


Figure 4.1: The extended LBP operator: the circular (8, 1), (16, 2), and (8, 2) neighbourhoods

However, DWT image decomposition is the natural alternative, to the above approach, for simultaneously extracting textures at different scales. In chapter 3 we concluded that combining the advantages of DWT and the LBP operator could lead to a more suitable face biometrics for steganographic embedding. Here we shall describe different ways of applying an LBP operator on the wavelet subbands to represent face features (Wang, et al., 2011; Wang, et al., 2011; Liu, et al., 2010; Tang, et al., 2010), and represent each subband by the corresponding LBPH histograms as a face descriptor feature vector. In order to avoid the need for the normalisation of the LBPH bins, as described in chapter 3, we shall subdivide the subbands into blocks as before. Figure 4.2 show the usual (8,1) LBP code image of a face image in the spatial domain as well as in the LL-subbands at 2 different decomposition levels.

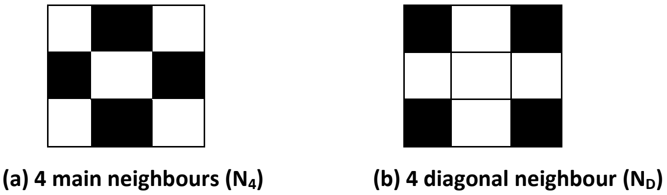


(a) Original Image **(b) LL1 subband** **(c) LL2 subband**

Figure 4.2: LBP code images

4.2 LBPH Schemes in the DWT Domain

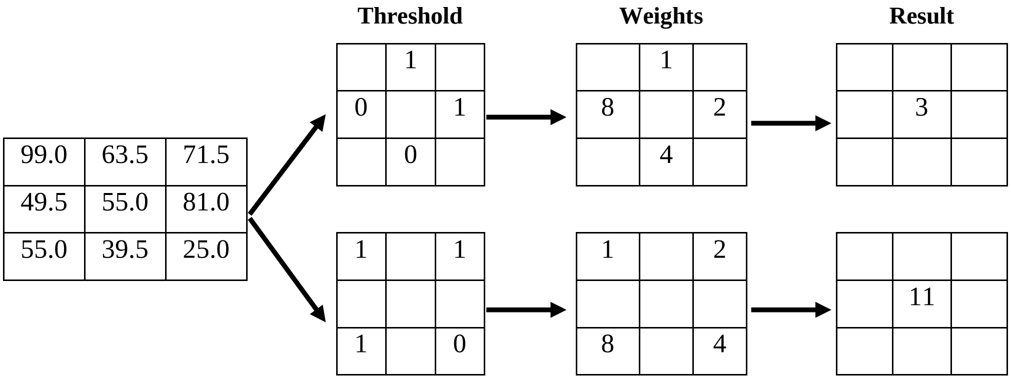
There are various ways of defining DWT-based LBP with reduced number of features (bins) for a face image while maintaining the face recognition accuracy at the same level, or even increase, when compared to using the original spatial or wavelet domain LBPH features. Given any wavelet subband of a face image, we define a new LBP operator using only 4 neighbours instead of the normal 8 neighbours. For any wavelet coefficient its 8-neighbours can be separated into two parts, the four main neighbours N_4 and the four diagonal neighbours N_D. In this way, the LBP code at any wavelet coefficient can be represented by only 4-bits obtained as before by checking the order relation between the central coefficients and its 4 designated neighbours. There are two obvious complementary ways of designating 4 neighbour coefficients: the main N_4 and the diagonal N_D forms as illustrated in figure 4.3.



(a) 4 main neighbours (N_4) (b) 4 diagonal neighbour (N_D)

Figure 4.3: 4-Neighbours positions

In figure 4.4, we give examples of both LBP codes extracted from an imagined 3x3 block of DWT subband. Examples shows the process of assigning LBP codes by first checking the centre value with the selected 4 neighbours; if the centre value is less than checked neighbour value then we will assign 1 at the neighbor position, otherwise we will assign 0. Secondly we will assign decimal weights to the neighbour positions in clockwise orders. Then we will multiply the assigned binary code with the corresponding decimal weight value. Finally all obtained decimal values from previous step added together to obtain final decimal value (Result).



99.0	63.5	71.5
49.5	55.0	81.0
55.0	39.5	25.0

Threshold (N4):

	1	
0		1
	0	

Weights (N4):

	1	
8		2
	4	

Result (N4):

	3	

Threshold (ND):

1		1
1		0

Weights (ND):

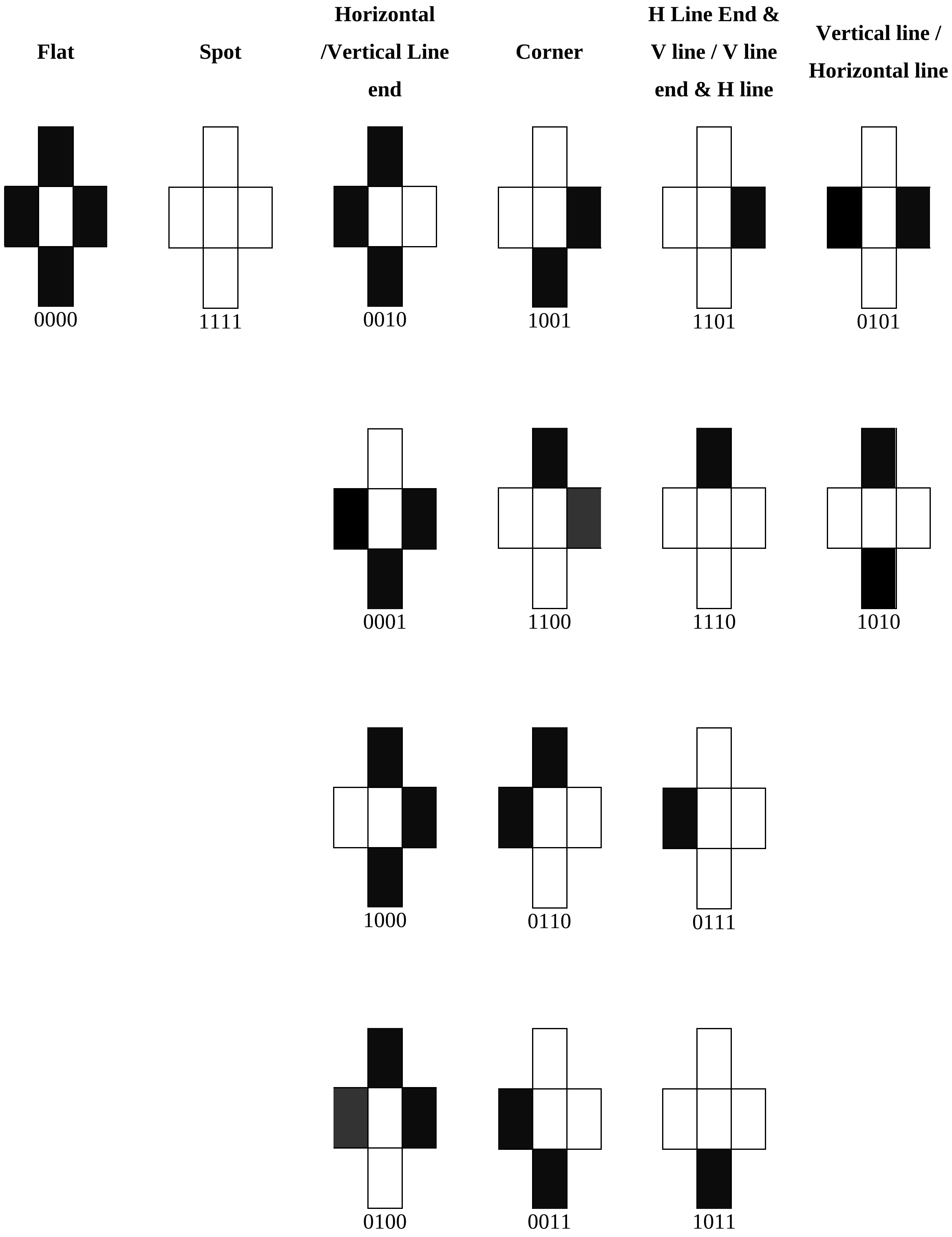
1		2
8		4

Result (ND):

	11	

Figure 4.4: An example of the 4 neighbours LBP operator

One or both of 4-neighbour parts can be used for extracting face features. The 4 neighbour LBP extract texture patterns of the face image that are very similar to the textures extracted using the 8 neighbours LBP especially when used with non LL subbands in the wavelet domain.



Flat
Spot
Horizontal /Vertical Line end
Corner
H Line End & V line / V line end & H line
Vertical line / Horizontal line
0000
1111
0010
1001
1101
0101
0001
1100
1110
1010
1000
0110
0111
0100
0011
1011

Figure 4.5: 4-Neighbours Local Binary Patterns

Figure 4.5 shows 16 textures patterns can be extract using our proposed N_4 LBP. It can be noticed that textures can be extracted using our proposed 4 neighbours scheme include spot, flat, horizontal line, horizontal line ends, vertical line, vertical line ends, and corners. Extracted textures are look like extracted 59 codes of uniform N_8 LBP proposed by Ojala (i.e. binary pattern contains maximum two bitwise transitions from 0 to 1 or from 1 to 0 when the corresponding bit string is considered circular). Out of these 16 LBP codes only two codes are non-uniform (0101 and 1010) which they have 4 transitions. Figure 4.6 shows the results of applying LBP with 8 sampling points and 4 sampling points on a face image in the wavelet subbands.

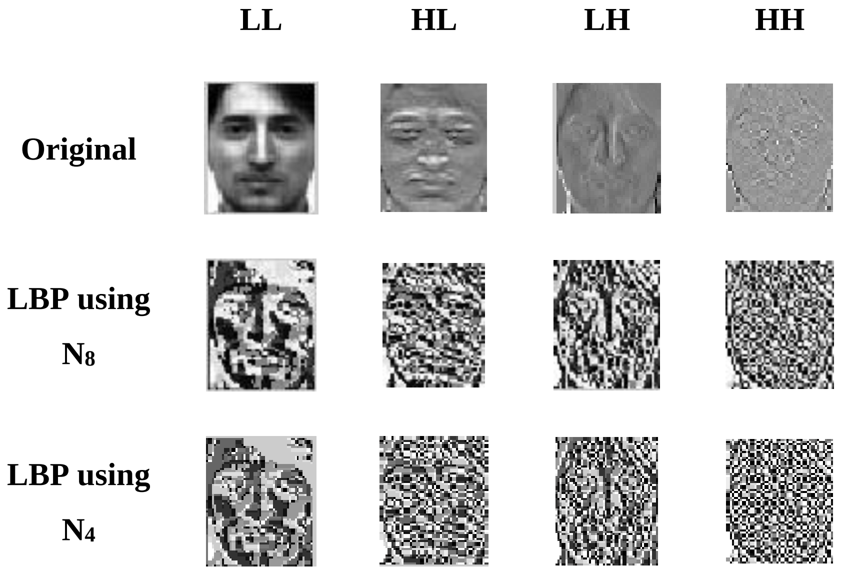


Figure 4.6: LBP image in different subbands using 8 and 4 neighbours

Based on the above new representation of LBPH using 4-neighbours we propose a new multi-scale wavelet based LBPH: a given image is decomposed into two level of wavelet subbands using Haar filter. Selected subband is divided into non-overlapping blocks of size nxn. Then LBPHs extract from each of the blocks of a given subband using the main N_4, diagonal N_D, or both of them. The final face feature vector is obtained by concatenating LBPHs extracted from all blocks that subband divided for.

From the literature, it has been shown that face features based on high-frequency wavelet subbands are invariant to illumination changes, whilst features based on approximation subbands are robust against facial expressions (Sellahewa & Jassim, 2008). The fusion of features from the different wavelet subbands has resulted in an improvement in face recognition accuracy (Sellahewa & Jassim, 2010). Therefore, it is reasonable to propose another new scheme by combine the LBPHs of more than one wavelet subbands to represent a final face image. For each wavelet subbands that selected for the purpose of combination, the same process of the proposed extracting LBPH from single subband done and the final face feature vector is obtained by concatenating LBPHs extracted from selected subbands. The general frame work of the above proposed scheme is shown in figure 4.7.

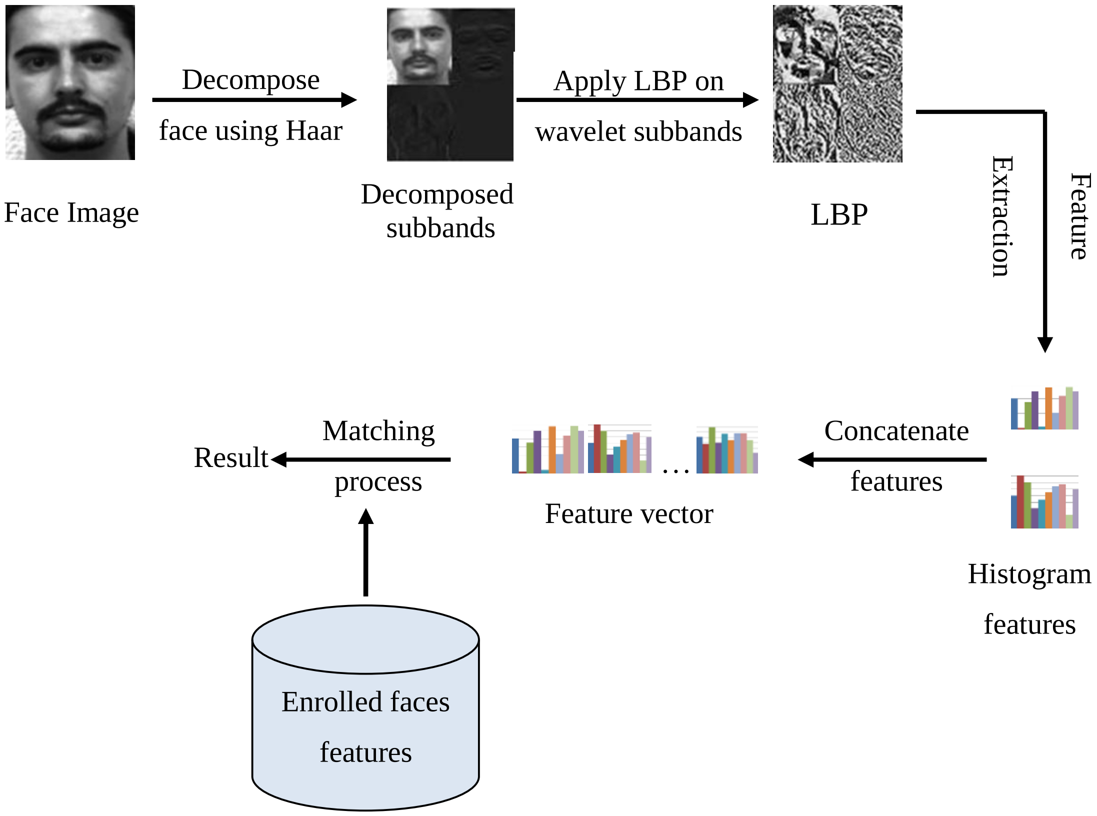


Figure 4.7: Wavelet-based LBPH face recognition system

4.3 Experimental Setup

This section include the discussion of the experimental setup to tests the performance of the different proposed wavelet-based LBPH schemes such as the selection of the experimental databases and different protocols that govern the partitioning of the data samples into training and testing sets.

4.3.1 Databases

We have used two publically available face biometric databases to evaluate the accuracy of all proposes face recognition schemes that will give in the next section of this chapter. The two databases are Yale face database and ORL face database; both databases are described in details in section 2.1.4.

4.3.2 Evaluation Protocols

We conducted our experiments with 3 different protocols:

One training image (P1): In this case only one face image per subject will select as training and the rest remain face images are used as testing images. Experiments were repeated (n) times, where (n) is the number of individual images in each subject. For example when Yale face database is used we repeat the experiments 11 times since the database include 11 different individuals for each subject, while in case of using ORL face database, the experiment is repeated 10 times. All the results shows in the next sections are the average of repeated times.

50% Training and 50% Testing (P2): Here, half images per subject were used as training and the rest used as testing. For ORL database, 5 images per subject were used as "training" and the remaining 5 were used as "testing"; while for Yale database, 5 images per subject were used as "training" and the remaining 6 images were used as 'testing". Experiments were repeated 10 times and samples for training were selected randomly. Again, results were averaged.

Leave-One-Out strategy (P3): In this strategy, each time only one image was taken off the database for test and all the remaining images were used as training. Experiments were repeated (m) times, where (m) is the total number of images in the database, for Yale database m is equal 165 while for ORL database m equal to 400, recognition rate is averaged.

4.4 The Performance of DWT-based LBPH Schemes

For clarity of discussion and comparisons we present the experimental results, in 5 separate subsections, for the different LBP codes (N_4, and N_D), followed by the results of fusing these two schemes together as well as fusing with N_8 scheme. In each of these subsections, we compare the performance of the corresponding scheme with that of the usual wavelet-based LBPH using N_8 scheme. All the experiments will be based on the nearest neighbour classifier using the Euclidean distance function. Moreover, we shall consider Haar wavelet subbands at levels 1 and 2 decomposition level together with combination of these. In all cases, performances of the different single-subband schemes as well as the multi-stream fusion of a combination of subbands are presented in tables each showing results for all the evaluation protocols for ease of comparison. For each of the two testing databases (Yale and ORL), we display two tables one for each subband blocking strategy (3x3 blocks and 5x5 blocks).

4.4.1 LBP with 4 Main Neighbours (N$_4$)

In these experiments we extracted the LBP code using the 4 main neighbours (i.e. the N$_4$ selection of the two horizontal and two vertical neighbours). In this case the LBP histogram consists of only 16 bins for each sub-block instead of representing LBP histogram by 256 bins in case of using $\mathrm{LBP}_{8,1}$ or 59 bins using$\mathrm{LBP}_{8,1}^{u2}$. The results for the 2 databases and the 2 blocking strategies are presented in Tables 4.1 to 4.4.

Table 4.1: N$_4$ Recognition rate, Yale database used, each subband divided to 3x3

Subband(s)	One training(P1)		5training & 6testing(P2)		Leave one out(P3)	
	N$_8$	N$_4$	N$_8$	N$_4$	N$_8$	N$_4$
LL$_1$	76.36	68.18	90.33	84.22	89.69	86.06
HL$_1$	49.27	60.66	71.11	81.88	79.39	85.45
LH$_1$	53.15	63.87	75.44	83.66	79.39	85.45
HH$_1$	18.66	22.36	28	33.33	30.3	36.96
LL$_2$	70.36	63.75	86.22	83.44	87.88	87.27
HL$_2$	37.15	46.78	58.88	72.55	69.69	80.6
LH$_2$	43.87	46.72	66.44	65.22	75.15	72.12
HH$_2$	14.54	15.27	26.66	20	28.48	22.42
LL1,HL1	77.69	72.72	93.11	87.33	93.33	90.3
LL1,LH1	78.08	72.02	91.55	87.22	91.55	89.09
LL1,HL1,LH1	79.21	75.27	92.66	89.77	**93.93**	92.12
ALL Level 1	78.08	75.21	92.66	90.11	93.33	90.3
LL2,HL2	71.81	68.36	88.88	87.33	89.69	91.51
LL2,LH2	73.75	69.51	87.44	85.44	90.09	89.09
LL2,HL2,LH2	75.93	74	90.88	90.22	**93.93**	**93.33**
ALL Level 2	75.93	75.57	90.88	**90.77**	**93.93**	**93.33**
LL1,HL1,LH1, LL2,HL2,LH2	**80.66**	**75.81**	**93.55**	90.55	**93.93**	91.51

Table 4.2: N$_4$ Recognition rate, Yale database used, each sub-block divided to 5x5

Subband(s)	One training(P1)		5training & 6testing(P2)		Leave one out(P3)	
	N$_8$	N$_4$	N$_8$	N$_4$	N$_8$	N$_4$
LL$_1$	82.84	76.36	94.33	91.88	94.54	93.33
HL$_1$	59.09	68.48	80.55	91.22	88.48	95.75
LH$_1$	59.51	73.63	81.66	89.66	87.27	90.3
HH$_1$	22	28.9	29.88	44.55	29.69	51.51
LL$_2$	78.18	76.06	93.55	90.77	96.96	93.33

Subband(s)	**One training(P1)**		**5training & 6testing(P2)**		**Leave one out(P3)**	
	N_8	**N_4**	**N_8**	**N_4**	**N_8**	**N_4**
HL_2	46.3	57.39	71.33	81.55	76.96	87.87
LH_2	52.6	60.3	77.77	84.22	84.24	85.45
HH_2	18	19.93	28.22	31.44	32.72	37.57
LL1,HL1	84.36	78.78	96.11	94	96.36	96.36
LL1,LH1	83.63	79.51	95.11	94.11	96.36	96.36
LL1,HL1,LH1	84.04	82	95.88	96	96.96	**98.18**
ALL Level 1	83.81	82	95.77	95.33	96.36	96.96
LL2,HL2	80.3	80.54	95	95.11	96.36	96.96
LL2,LH2	82.66	81.33	93.66	94.33	96.36	95.15
LL2,HL2,LH2	83.09	83.21	96	95.44	**98.18**	96.96
ALL Level 2	83.09	**83.45**	96	**96**	**98.18**	97.57
LL1,HL1,LH1, LL2,HL2,LH2	**85.03**	82.42	**96.22**	95.55	**98.18**	97.57

Table 4.3: N_4 Recognition rate, ORL database used, each sub-block divided to 3x3

Subband(s)	**One training(P1)**		**5training & 5testing(P2)**		**Leave one out(P3)**	
	N_8	**N_4**	**N_8**	**N_4**	**N_8**	**N_4**
LL_1	68.02	69.36	**96.40**	96.55	99.50	**99.50**
HL_1	36.05	43.61	61.50	69.70	67.50	78.00
LH_1	20.66	25.83	35.70	41.10	43.00	48.50
HH_1	7.55	7.69	9.75	9.95	10.00	12.25
LL_2	68.94	62.66	95.20	93.22	98.50	98.00
HL_2	29.97	34.83	52.65	60.25	60.50	68.75
LH_2	20.36	24.94	38.95	41.80	49.25	53.00
HH_2	5.22	5.41	6.60	7.20	6.25	8.25
LL1,HL1	69.77	71.61	95.80	96.75	**99.75**	**99.5**
LL1,LH1	68.83	70	96.10	96.45	99.50	99
LL1,HL1,LH1	70.36	71.69	96.30	96.7	**99.75**	**99.5**
ALL Level 1	70.30	71.83	96.05	**97**	**99.75**	**99.5**
LL2,HL2	67.83	64.83	95.15	95	99.00	98.75
LL2,LH2	67.27	64.75	94.65	94.1	98.75	98.75
LL2,HL2,LH2	67.77	66.3	94.60	95.45	98.25	99
ALL Level 2	67.05	65.69	94.95	94.6	98.00	98.5
LL1,HL1,LH1, LL2,HL2,LH2	**71.63**	**72.63**	96.35	96.65	**99.75**	**99.5**

Table 4.4: N_4 Recognition rate, ORL database used, each sub-block divided to 5x5

Subband(s)	**One training(P1)**		**5training & 5testing(P2)**		**Leave one out(P3)**	
	N_8	**N_4**	**N_8**	**N_4**	**N_8**	**N_4**
LL_1	67.91	66.86	95.35	95.40	**99.00**	98.75
HL_1	41.27	50.52	72.45	83.10	83.50	89.50
LH_1	27.75	35.94	49.35	64.35	57.00	73.00
HH_1	7.44	8.50	10.10	11.70	9.75	12.75
LL_2	65.25	60.75	94.35	93.15	**99.00**	98.00
HL_2	33.80	42.69	63.65	76.33	75.50	85.50
LH_2	26.33	36.27	51.90	64.95	62.50	75.50
HH_2	6.11	8.13	10.15	14.65	12.25	15.50
LL1,HL1	68.44	68.38	96.15	96.15	98.25	98.75
LL1,LH1	68.52	67.77	95.45	96.3	98.75	**99**
LL1,HL1,LH1	69.11	69.27	96.15	96.2	98.50	**99**
ALL Level 1	69.16	69.36	95.70	96.4	98.75	98.75
LL2,HL2	64.13	62.22	94.50	92.7	98.75	97.5
LL2,LH2	65.02	61.52	94.90	93.9	98.75	98.25
LL2,HL2,LH2	64.25	63.02	93.55	93.05	98.75	98
ALL Level 2	63.61	62.91	94.05	94.2	98.00	98
LL1,HL1,LH1, LL2,HL2,LH2	**69.52**	**69.41**	**96.25**	**96.9**	98.75	**99**

Analyses of these results lead to a complex pattern that can be summarised by the following observations and conclusions:

1. For Yale database, using 5x5 blocking strategy outperform the 3x3 blocking strategy for all protocols. However, for the ORL database, the results are in the opposite direction except for the single non-LL subbnad schemes.
2. In terms of the effect of using N_4 or N_8 LBP neighbourhood selection:
   - For Yale database, if single non LL subband is used, then N_4 outperforms N_8, but for the LL-subband N_8 is the better option. This is true for both wavelet levels. For ORL database, this pattern remains valid except for the LL-subband at level 1 where the N_4 ALSO outperforms N_8.
   - For Yale database when more than one wavelet subband is used the picture is mixed. While the N_8 outperforms N_4 in most cases, for the 5x5 blocks the differences in accuracy is negligible and few cases the N_4 outperforms N_8.

- For ORL database when more than one subbands used, with N_4 we got same or higher recognition rate than N_8 in most cases except when combining subbands from second level of wavelet decomposition.

3. Generally in all cases, schemes that use level 1 subbands yield better performance than those using level 2 subbands.
4. The best accuracy rates achieved for the different protocols are as following:
    - Yale: P1: 85.03% (N_8 , 6 subbands and 5x5); P2: 96.22% (N_8 , 6 subbands and 5x5); and P3: 98.18% (N_4 , LL1,HL1,LH1 and 5x5);
    - **ORL**: P1: 72.63% (N_4, 6 subbands and 3x3); P2: 97% (N_4 , All level 1, and 3x3); and P3: 99.75% (N_8 , LL1,HL1 and 3x3);

When evaluating the performance of these various schemes, one takes into account that N_4 require much lower embedding capacity compared to N_8.

4.4.2 LBP with 4 Diagonal Neighbours (N_D)

As we mention and explained earlier in this chapter that we can separate the 8 neighbours of a given wavelet subband coefficient in to two kinds of 4-neighbors(N_4 and N_D), here in these experiments we use the diagonal 4-neighbours (N_D) for extracting face features using LBP code after decomposing face image into two wavelet decomposition levels. Tables 4.5 to 4.8 shows face recognition rate of different databases with using three different scenarios of separating images, and different number of blocks that each subband divided to.

Table 4.5: N_D Recognition rate, Yale database used, each subband divided to 3x3

Subband(s)	One training(P1)		5training & 6testing(P2)		Leave one out(P3)	
	N_8	N_D	N_8	N_D	N_8	N_D
LL_1	76.36	66.54	90.33	82.22	89.69	83.03
HL_1	49.27	50.72	71.11	74.44	79.39	81.81
LH_1	53.15	61.63	75.44	83.11	79.39	84.84
HH_1	18.66	19.33	28	31.33	30.3	36.36
LL_2	70.36	60.84	86.22	80	87.88	83.03
HL_2	37.15	43.15	58.88	66.55	69.69	74.54
LH_2	43.87	53.54	66.44	76.66	75.15	84.24
HH_2	14.54	15.75	26.66	20.66	28.48	23.63
LL1,HL1	77.69	70.84	93.11	87.22	93.33	86.66
LL1,LH1	78.08	72.42	91.55	86.44	91.55	86.66
LL1,HL1,LH1	79.21	74.6	92.66	89	**93.93**	89.09

Subband(s)	One training(P1)		5training & 6testing(P2)		Leave one out(P3)	
	N_8	N_D	N_8	N_D	N_8	N_D
ALL Level 1	78.08	**75.39**	92.66	89.33	93.33	89.09
LL2,HL2	71.81	66.24	88.88	83.22	89.69	84.84
LL2,LH2	73.75	67.63	87.44	86.11	90.09	86.06
LL2,HL2,LH2	75.93	71.27	90.88	86.88	**93.93**	88.48
ALL Level 2	75.93	71.81	90.88	88	**93.93**	**90.3**
LL1,HL1,LH1, LL2,HL2,LH2	**80.66**	74.78	**93.55**	**89.77**	**93.93**	**90.3**

Table 4.6: N_D Recognition rate, Yale database used, each sub-block divided to 5x5

Subband(s)	One training(P1)		5training & 6testing(P2)		Leave one out(P3)	
	N_8	N_D	N_8	N_D	N_8	N_D
LL_1	82.84	74.06	94.33	87.44	94.54	89.09
HL_1	59.09	65.03	80.55	89.22	88.48	91.51
LH_1	59.51	71.31	81.66	90.88	87.27	92.72
HH_1	22	24.84	29.88	36.22	29.69	44.24
LL_2	78.18	67.57	93.55	85.33	96.96	90.3
HL_2	46.3	53.69	71.33	78.22	76.96	87.27
LH_2	52.6	62.12	77.77	85.44	84.24	87.87
HH_2	18	25.21	28.22	38.77	32.72	41.21
LL1,HL1	84.36	77.27	96.11	91.77	96.36	93.93
LL1,LH1	83.63	77.57	95.11	90.33	96.36	91.51
LL1,HL1,LH1	84.04	80.36	95.88	93.55	96.96	95.15
ALL Level 1	83.81	**80.96**	95.77	93.88	96.36	95.15
LL2,HL2	80.3	72.72	95	88.87	96.36	92.12
LL2,LH2	82.66	73.45	93.66	90.22	96.36	91.51
LL2,HL2,LH2	83.09	76.36	96	91.66	**98.18**	95.15
ALL Level 2	83.09	77.21	96	92.88	**98.18**	95.15
LL1,HL1,LH1, LL2,HL2,LH2	**85.03**	**80.96**	**96.22**	**94.33**	**98.18**	**95.75**

Table 4.7: N_D Recognition rate, ORL database used, each sub-block divided to 3x3

Subband(s)	One training(P1)		5training & 5testing(P2)		Leave one out(P3)	
	N_8	N_D	N_8	N_D	N_8	N_D
LL_1	68.02	64.22	**96.40**	93.15	99.50	98.5
HL_1	36.05	47.86	61.50	74.25	67.50	81.75
LH_1	20.66	22.52	35.70	36.15	43.00	40.5

Subband(s)	One training(P1)		5training & 5testing(P2)		Leave one out(P3)	
	N_8	N_D	N_8	N_D	N_8	N_D
HH_1	7.55	5.69	9.75	7.6	10.00	8.5
LL_2	68.94	64.97	95.20	93.4	98.50	97.25
HL_2	29.97	41.63	52.65	68.35	60.50	78
LH_2	20.36	25.83	38.95	49.7	49.25	59.25
HH_2	5.22	4.47	6.60	5.4	6.25	6
LL1,HL1	69.77	67.91	95.80	**96.4**	**99.75**	**99.5**
LL1,LH1	68.83	65.5	96.10	94.65	99.50	98.75
LL1,HL1,LH1	70.36	68.3	96.30	95.1	**99.75**	99.25
ALL Level 1	70.30	68.75	96.05	94.95	**99.75**	99.25
LL2,HL2	67.83	69.47	95.15	94.35	99.00	98
LL2,LH2	67.27	66.16	94.65	94.25	98.75	97.5
LL2,HL2,LH2	67.77	**69.75**	94.60	94.45	98.25	98
ALL Level 2	67.05	68.94	94.95	96	98.00	98
LL1,HL1,LH1, LL2,HL2,LH2	**71.63**	**69.75**	96.35	95.65	**99.75**	99

Table 4.8: N_D Recognition rate, ORL database used, each sub-block divided to 5x5

Subband(s)	One training(P1)		5training & 5testing(P2)		Leave one out(P3)	
	N_8	N_D	N_8	N_D	N_8	N_D
LL_1	67.91	64.77	95.35	94.75	**99.00**	98
HL_1	41.27	54.72	72.45	83.85	83.50	91
LH_1	27.75	32.69	49.35	59.45	57.00	68.75
HH_1	7.44	5.63	10.10	7.3	9.75	7.75
LL_2	65.25	61.33	94.35	91.4	**99.00**	96.5
HL_2	33.80	50.13	63.65	81.3	75.50	89.25
LH_2	26.33	36.52	51.90	67.5	62.50	80.5
HH_2	6.11	6.8	10.15	12.3	12.25	13.5
LL1,HL1	68.44	66.69	96.15	95.55	98.25	**98.5**
LL1,LH1	68.52	65	95.45	94.5	98.75	98.25
LL1,HL1,LH1	69.11	67.05	96.15	94.9	98.50	**98.5**
ALL Level 1	69.16	67.11	95.70	95.55	98.75	**98.5**
LL2,HL2	64.13	64.66	94.50	93.5	98.75	97.25
LL2,LH2	65.02	61.33	94.90	92.65	98.75	97
LL2,HL2,LH2	64.25	64.36	93.55	93	98.75	97.5
ALL Level 2	63.61	63.91	94.05	93.45	98.00	97.75

Subband(s)	**One training(P1)**		**5training & 5testing(P2)**		**Leave one out(P3)**	
	N_8	**N_D**	**N_8**	**N_D**	**N_8**	**N_D**
LL1,HL1,LH1, LL2,HL2,LH2	**69.52**	**67.58**	**96.25**	**95.95**	98.75	**98.5**

From results showed in tables 4.5 to 4.8, most the discussion done on the results obtained from previous section when N_4 scheme used and compared with using N_8 scheme is true here. Here we summarised results obtained by the following observations and conclusions:

1. For Yale database, using 5x5 blocking strategy outperform the 3x3 blocking strategy for all protocols. However, for the ORL database, the results are in the opposite direction except for the single non-LL subbnad schemes.
2. In terms of the effect of using N_D or N_8 LBP neighbourhood selection:
   - For Yale database, if single non LL subband is used, then N_D outperforms N_8, but for the LL-subband N_8 is the better option. This is true for both levels. For ORL database, this pattern remains valid.
   - For Yale database when more than one wavelet subband is used the N_8 outperforms N_D in all cases,
   - For ORL database when more than one subbands used the picture is mixed, with N_D we got same or higher recognition rate than N_8 in some cases and other way around in others.
3. The best accuracy rates achieved for the different protocols are as following:
   - Yale: P1: 85.03% (N_8 , 6 subbands and 5x5); P2: 96.22% (N_8 , 6 subbands and 5x5); and P3: 98.18% (N_8 , LL2,HL2,LH2 and 5x5);
   - ORL: P1: 71.63% (N_8, 6 subbands and 3x3); P2: 96.4% (N_D , LL1,HL1, and 3x3); and P3: 99.75% (N_8 , LL1+HL1 and 3x3);

In addition to the discussion of the results obtained here in this section, when we compare N_4 and N_D schemes that explained in sections 4.4.1.and 4.4.2, we can conclude that using N_4 scheme obtain higher face recognition rate than using N_D scheme in most cases. The best accuracy rates achieved for the different blocking and different protocols, and different databases for the two schemes are as following:

1. Yale Database:
   - 3x3 blocking:
     - P1: 75.81% (N_4 and 6 subbands) , 75.39% (N_D and All level 1)

    - P2: 90.77% (N_4 and All level 2) , 89.77% (N_D and 6 subbands)
    - P3: 93.33% (N_4 and LL1,HL1,LH1) , 90.3% (N_D and All level 2)
  - 5x5 blocking:
    - P1: 83.45% (N_4 and All level 2) , 80.96% (N_D and All Level 1)
    - P2: 96.0% (N_4 and LL1,HL1,LH1) , 94.33% (N_D and 6 subbands)
    - P3: 98.18% (N_4 and LL1,HL1,LH1) , 95.75% (N_D and 6 subbands)

2. ORL Database:
   - 3x3 blocking:
     - P1: 72.63% (N_4 and 6 subbands) , 69.75% (N_D and LL2,HL2,LH2)
     - P2: 97.0% (N_4 and All Level 1) , 96.4% (N_D and LL1,HL1)
     - P3: 99.5% (N_4 and LL1) , 99.5% (N_D and LL1,HL1)
   - 5x5 blocking:
     - P1: 69.41% (N_4 and 6 subbands) , 67.58% (N_D and 6 subbands)
     - P2: 96.9% (N_4 and 6 subbands) , 95.95% (N_D and 6 subbands)
     - P3: 99.0% (N_4 and LL1+LH1) , 98.5% (N_D and LL1+HL1)

As a conclusion of the comparison between N_4 and N_D schemes recognition accuracy, we can say that most textures features such as (edges, lines) are in HL and LH wavelet subbands. Therefore, extracting texture features from horizontal and vertical neighbours of the wavelet subband coefficients leads to obtain better representation of the texture features than using diagonal neighbours. As a result, using N_4 scheme to extract texture features can guarantee higher face recognition rate if compared with using N_D scheme.

4.4.3 Combining LBP with 4 Main (N_4) and 4 Diagonal (N_D) Neighbours

Extracting LBP code using only 4-neighbours and excluding the other 4-neighbours as explained and proposed in previous sub-sections 4.4.1 and 4.4.2 may lose some important texture features that any wavelet subband may have. To overcome this issue we propose here a new extraction method that gathers information from all 8-neighbours of the pixel but not using all of them together as a traditional $\mathrm{LBP}_{8,1}$. First, we separate the 8 neighbours of a coefficient into two parts, the four main neighbours (N_4) and the four diagonal neighbours (N_D). Second, we calculate two separate LBP codes, LBP_4 and LBP_D (i.e., one based on N_4 neighbours and the other based on N_D neighbours) at radius of 1. Then finally, the histogram of each LBP set is calculated and the two histograms, LBP_4H and LBP_DH, are concatenated to represent the final sub-block of the subband of the given face. Using the proposed approach, we are able to represent LBP histograms using only 32 bins (16 bins for each of the two 4 neighbours).

Tables 4.9 to 4.12 shows face recognition rates of different databases with using different scenarios of separating images, and for different number of blocks that each subband was divided into. Results of the proposed are compared with those achieved with features based onLBP$_{8}^{u2}$.

Table 4.9: N$_4$&N$_D$ Recognition rates, Yale database used, each wavelet subband is divided to 3×3 blocks

Subband(s)	One training(P1)		5training & 6testing(P2)		Leave one out(P3)	
	N$_8$	N$_4$ & N$_D$	N$_8$	N$_4$ & N$_D$	N$_8$	N$_4$ & N$_D$
LL$_1$	76.36	72.72	90.33	85.33	89.69	87.27
HL$_1$	49.27	63.69	71.11	84.88	79.39	91.51
LH$_1$	53.15	70.3	75.44	87.33	79.39	89.69
HH$_1$	18.66	25.33	28	41.44	30.3	41.21
LL$_2$	70.36	67.09	86.22	84.77	87.88	86.06
HL$_2$	37.15	53.45	58.88	79.88	69.69	85.45
LH$_2$	43.87	60.9	66.44	81.33	75.15	85.45
HH$_2$	14.54	19.39	26.66	30.66	28.48	34.54
LL1,HL1	77.69	76.42	93.11	89.66	93.33	90.3
LL1,LH1	78.08	76.12	91.55	90.77	91.55	91.51
LL1,HL1,LH1	79.21	79.57	92.66	93.0	**93.93**	94.54
ALL Level 1	78.08	79.51	92.66	**94.22**	93.33	93.93
LL2,HL2	71.81	71.87	88.88	89.55	89.69	91.51
LL2,LH2	73.75	72.6	87.44	87.33	90.09	90.3
LL2,HL2,LH2	75.93	77.57	90.88	91.33	**93.93**	94.54
ALL Level 2	75.93	78.72	90.88	91.77	**93.93**	**96.36**
LL1,HL1,LH1, LL2,HL2,LH2	**80.66**	**80.0**	**93.55**	93.22	**93.93**	94.54

Table 4.10: N$_4$&N$_D$ Recognition rates, Yale database used, each wavelet subband is divided to 5×5 blocks

Subband(s)	One training(P1)		5training & 6testing(P2)		Leave one out(P3)	
	N$_8$	N$_4$ & N$_D$	N$_8$	N$_4$ & N$_D$	N$_8$	N$_4$ & N$_D$
LL$_1$	82.84	79.15	94.33	90.88	94.54	90.3
HL$_1$	59.09	72.78	80.55	94.11	88.48	96.36
LH$_1$	59.51	78.24	81.66	94.66	87.27	96.96

Subband(s)	**One training(P1)**		**5training & 6testing(P2)**		**Leave one out(P3)**	
	N$_8$	**N$_4$ & N$_D$**	**N$_8$**	**N$_4$ & N$_D$**	**N$_8$**	**N$_4$ & N$_D$**
HH$_1$	22	34.78	29.88	54.44	29.69	66.06
LL$_2$	78.18	77.93	93.55	91.77	96.96	93.93
HL$_2$	46.3	62.54	71.33	86.33	76.96	91.51
LH$_2$	52.6	71.45	77.77	92.55	84.24	95.15
HH$_2$	18	31.57	28.22	49.44	32.72	59.39
LL1,HL1	84.36	82.12	96.11	95.44	96.36	95.15
LL1,LH1	83.63	82.72	95.11	94.55	96.36	94.54
LL1,HL1,LH1	84.04	84.24	95.88	96.77	96.96	96.96
ALL Level 1	83.81	84.24	95.77	**96.88**	96.36	96.96
LL2,HL2	80.3	81.93	95	95.55	96.36	**97.57**
LL2,LH2	82.66	82.48	93.66	94.44	96.36	96.36
LL2,HL2,LH2	83.09	84.66	96	95.77	**98.18**	97.57
ALL Level 2	83.09	**85.51**	96	95.88	**98.18**	96.96
LL1,HL1,LH1, LL2,HL2,LH2	**85.03**	84.48	**96.22**	96.77	**98.18**	**97.57**

Table 4.11: N$_4$&N$_D$ Recognition rates, ORL database used, each wavelet subband is divided to 3×3 blocks

Subband(s)	**One training(P1)**		**5training & 5testing(P2)**		**Leave one out(P3)**	
	N$_8$	**N$_4$ & N$_D$**	**N$_8$**	**N$_4$ & N$_D$**	**N$_8$**	**N$_4$ & N$_D$**
LL$_1$	68.02	69.0	**96.40**	96.55	99.50	99.0
HL$_1$	36.05	56.97	61.50	85.55	67.50	92.0
LH$_1$	20.66	33.77	35.70	57.2	43.00	66.25
HH$_1$	7.55	8.33	9.75	11.8	10.00	12.25
LL$_2$	68.94	69.66	95.20	95.95	98.50	98.25
HL$_2$	29.97	50.08	52.65	81.35	60.50	87.75
LH$_2$	20.36	35.02	38.95	63.5	49.25	73.5
HH$_2$	5.22	7.05	6.60	10.25	6.25	12.75
LL1,HL1	69.77	71.94	95.80	97.35	**99.75**	99.5
LL1,LH1	68.83	70.16	96.10	96.45	99.50	99.5
LL1,HL1,LH1	70.36	72.55	96.30	97.6	**99.75**	**99.75**
ALL Level 1	70.30	72.8	96.05	**97.65**	**99.75**	99.5
LL2,HL2	67.83	71.88	95.15	96.1	99.00	98.5
LL2,LH2	67.27	69.5	94.65	96.2	98.75	99.25
LL2,HL2,LH2	67.77	71.83	94.60	96.95	98.25	99.0

Subband(s)	One training(P1)		5training & 5testing(P2)		Leave one out(P3)	
	N_8	N_4 & N_D	N_8	N_4 & N_D	N_8	N_4 & N_D
ALL Level 2	67.05	71.94	94.95	96.6	98.00	99.25
LL1,HL1,LH1, LL2,HL2,LH2	**71.63**	**73.58**	96.35	97.05	**99.75**	**99.75**

Table 4.12: N_4&N_D Recognition rates, ORL database used, each wavelet subband is divided to 5×5 blocks

Subband(s)	One training(P1)		5training & 5testing(P2)		Leave one out(P3)	
	N_8	N_4 & N_D	N_8	N_4 & N_D	N_8	N_4 & N_D
LL_1	67.91	67.94	95.35	96.3	**99.00**	98.75
HL_1	41.27	60.22	72.45	88.6	83.50	94.75
LH_1	27.75	42.77	49.35	75.15	57.00	84.5
HH_1	7.44	9.22	10.10	13.1	9.75	15.0
LL_2	65.25	64.11	94.35	94.6	**99.00**	98.25
HL_2	33.80	55.69	63.65	88.05	75.50	93.75
LH_2	26.33	43.02	51.90	77.6	62.50	88.75
HH_2	6.11	10.91	10.15	18.5	12.25	24.0
LL1,HL1	68.44	69.3	96.15	96.65	98.25	**99.0**
LL1,LH1	68.52	68.41	95.45	95.85	98.75	98.75
LL1,HL1,LH1	69.11	69.86	96.15	96.3	98.50	**99.0**
ALL Level 1	69.16	69.94	95.70	**97.0**	98.75	**99.0**
LL2,HL2	64.13	66.66	94.50	95.1	98.75	98.75
LL2,LH2	65.02	64.33	94.90	94.9	98.75	98.5
LL2,HL2,LH2	64.25	66.36	93.55	93.75	98.75	98.75
ALL Level 2	63.61	66.3	94.05	94.45	98.00	98.5
LL1,HL1,LH1, LL2,HL2,LH2	**69.52**	**70.25**	**96.25**	95.45	98.75	**99.0**

The results obtained in tables from 4.9 to 4.12 can be analysis and summarised by the following observations and conclusions:

1. For Yale database, using 5x5 blocking strategy outperform the 3x3 blocking strategy for all protocols. However, for the ORL database, the results are in the opposite direction except for the single non-LL subbnad schemes.
2. In terms of the effect of using (N_4 and N_D) or N_8 LBP neighbourhood selection:
   - For Yale database, if single non LL subband is used, then (N_4 and N_D) outperforms N_8, but for the LL-subband N_8 is the better option. For ORL database, (N_4 and N_D) outperforms N_8 if single non LL subband is used but for

the LL-subband, the recognition accuracy obtained using both (N_4 and N_D) or N_8 are very close to each other with very little differences.

- For both (Yale and ORL) databases, when more than one wavelet subband is used the recognition accuracy that obtained from both used schemes are very close and the differences of the obtained recognition accuracy in most cases are very small. However, in some cases N_8 outperforms (ND and N_4) while in others (ND and $N_{4)}$ outperforms N_8.

3. The best accuracy rates achieved for the different protocols are as following:
   - Yale: P1: 85.51% (N_4 and $N_{D\,,}$ All level 2 and 5x5); P2: 96.88% (N_4 and $N_{D\,,}$ All level 1 and 5x5); and P3: 98.18% ($N_{8\,,}$ LL2,HL2,LH2 and 5x5);
   - ORL: P1: 73.58% (N_4 and $N_{D,}$ 6 subbands and 3x3); P2: 97.65% (N_4 and $N_{D\,,}$ All level 1, and 3x3); and P3: 99.75% (N_4 and $N_{D,}$ LL1,HL1,LH1 and 3x3);

On the other side, if we compare the results obtained here in this scheme (N_4 and N_D) with the results obtained using two other schemes (N_4) or (N_D) discussed in previous sub sections (4.4.1 and 4.4.2), we can notice that, (N_4 and N_D) outperform both schemes regarding the recognition accuracy, this true for all cases (i.e. using different protocols and different blocking strategies for both databases). Only one drawback with previous schemes is that; number of bins that represent each block of the wavelet subbands in this case is 32 bin while in previous schemes are only 16 bins, but still if we compare with 256 bins in case of using traditional $\mathrm{LBP}_{8,1}$ or 59 bins in $\mathrm{LBP}_{8,1}^{u2}$ this scheme can be represented with less number of features.

4.4.4 Fusion of LBP8 with LBP4

From sub-sections 4.4.1 and 4.4.2, generally we can conclude that:

1- Using 8 neighbours for extracting features from LL subband(s) is superior to using 4 neighbours; while for non LL subbands, using 4 neighbours give higher face recognition rate than using 8 neighbours.

2- In most cases using more than one wavelet subbands outperform of using single wavelet subband.

Based on the above conclusions, in this scheme, when more than one wavelet subbands used to represent final face feature vector, 8 neighbours scheme were used for LL subband(s) and 4 neighbours for non LL subband(s). And based on previous conclusion that using N_4 strategy is better than using N_D strategy, therefore in this case we use N_4

strategy to extract features from non-LL subband(s). Tables from 4.13 to 4.16 shows face recognition rate when different combination with different number of wavelet subbands used.

Table 4.13: N_8&N_4 Recognition rate, Yale database used, each wavelet subband divided to 3x3

Subband(s)	One training(P1)		5training & 6testing(P2)		Leave one out(P3)	
	N_8	N_8&N_4	N_8	N_8&N_4	N_8	N_8&N_4
LL1,HL1	77.69	81.03	93.11	94.55	93.33	95.75
LL1,LH1	78.08	80.6	91.55	93	91.55	94.54
LL1,HL1,LH1	79.21	83.21	92.66	95.22	**93.93**	95.15
ALL Level 1	78.08	82.78	92.66	95.44	93.33	96.36
LL2,HL2	71.81	75.69	88.88	90.44	89.69	92.12
LL2,LH2	73.75	75.09	87.44	88.88	90.09	91.51
LL2,HL2,LH2	75.93	79.45	90.88	92.88	**93.93**	94.54
ALL Level 2	75.93	79.45	90.88	92.88	**93.93**	94.54
LL1,HL1,LH1, LL2,HL2,LH2	**80.66**	**84.3**	**93.55**	**95.88**	**93.93**	**96.96**

Table 4.14: N_8&N_4 Recognition rate, Yale database used, each wavelet subband divided to 5x5

Subband(s)	One training(P1)		5training & 6testing(P2)		Leave one out(P3)	
	N_8	N_8&N_4	N_8	N_8&N_4	N_8	N_8&N_4
LL1,HL1	84.36	85.63	96.11	96.55	96.36	96.96
LL1,LH1	83.63	85.21	95.11	97.11	96.36	98.18
LL1,HL1,LH1	84.04	86.48	95.88	97.77	96.96	98.18
ALL Level 1	83.81	86.3	95.77	97.44	96.36	96.96
LL2,HL2	80.3	82.54	95	95.55	96.36	98.18
LL2,LH2	82.66	84.12	93.66	95.88	96.36	98.78
LL2,HL2,LH2	83.09	85.27	96	96.22	**98.18**	**100**
ALL Level 2	83.09	85.27	96	96.22	**98.18**	**100**
LL1,HL1,LH1, LL2,HL2,LH2	**85.03**	**87.39**	**96.22**	**98.22**	**98.18**	98.18

Table 4.15: N_8&N_4 Recognition rate, ORL database used, each wavelet subband divided to 3x3

Subband(s)	One training(P1)		5training & 5testing(P2)		Leave one out(P3)	
	N_8	N_8&N_4	N_8	N_8&N_4	N_8	N_8&N_4
LL1,HL1	69.77	71.00	95.80	97.00	**99.75**	99.50
LL1,LH1	68.83	69.55	96.10	96.55	99.50	99.75
LL1,HL1,LH1	70.36	71.94	96.30	96.80	**99.75**	99.50

Subband(s)	**One training(P1)**		**5training & 5testing(P2)**		**Leave one out(P3)**	
	N_8	**N_8&N_4**	**N_8**	**N_8&N_4**	**N_8**	**N_8&N_4**
ALL Level 1	70.30	72.00	96.05	96.05	**99.75**	99.50
LL2,HL2	67.83	68.38	95.15	95.10	99.00	98.50
LL2,LH2	67.27	69.11	94.65	96.20	98.75	99.00
LL2,HL2,LH2	67.77	68.33	94.60	94.65	98.25	98.25
ALL Level 2	67.05	68.19	94.95	95,75	98.00	99.00
LL1,HL1,LH1, LL2,HL2,LH2	**71.63**	**73.58**	**96.35**	**97.20**	**99.75**	**100.00**

Table 4.16: N_8&N_4 Recognition rate, ORL database used, each wavelet subband divided to 5x5

Subband(s)	**One training(P1)**		**5training & 5testing(P2)**		**Leave one out(P3)**	
	N_8	**N_8&N_4**	**N_8**	**N_8&N_4**	**N_8**	**N_8&N_4**
LL1,HL1	68.44	69.05	96.15	96.80	98.25	99.00
LL1,LH1	68.52	69.22	95.45	96.30	**98.75**	**99.25**
LL1,HL1,LH1	69.11	70.25	96.15	96.45	98.50	98.75
ALL Level 1	69.16	70.52	95.70	**97.35**	**98.75**	**99.25**
LL2,HL2	64.13	66.22	94.50	94.20	**98.75**	98.00
LL2,LH2	65.02	65.19	94.90	95.00	**98.75**	98.50
LL2,HL2,LH2	64.25	65.77	93.55	94.60	**98.75**	98.75
ALL Level 2	63.61	65.33	94.05	94.35	98.00	98.50
LL1,HL1,LH1, LL2,HL2,LH2	**69.52**	**70.86**	**96.25**	96.50	**98.75**	99.00

The results can be analysis and summarised by the following observations and conclusions:

1. For Yale database, using 5x5 blocking strategy outperform the 3x3 blocking strategy for all protocols. While for the ORL database, the results are in the opposite direction.
2. In terms of the effect of using (N_8 and N_4) or N_8 LBP neighbourhood selection: For Yale database, (N_8 and N_4) outperforms N_8 for all cases with different protocols and different blocking numbers. For ORL database, again (N_8 and N_4) outperforms N_8 for most cases, in few cases N_8 outperform (N_8 and N_4) but with very small amount.
3. The best accuracy rates achieved for the different protocols are as following: Yale: P1: 87.39% (N_8 and N_4, 6 subbands and 5x5); P2: 98.22% (N_8 and N_4, 6 subbands and 5x5); and P3: 100% (N_8 and N_4, LL2,HL2,LH2 and 5x5);

ORL: P1: 73.58% (N_8 and N_4, 6 subbands and 3x3); P2: 97.35% (N_8 and N_4,All level 1 and 5x5); and P3: 100% (N_8 and N_4, 6 subbands and 3x3);

Comparing the results obtained using this scheme and all other 3 previous schemes, we can say that the face recognition accuracy with this scheme have higher rate in all cases.

4.4.5 Fusion of LBP8 with Combined LBP4 and LPBD

Again by looking to the results obtained from the experiments reported in section 4.4.3, where a single subband was used to represent a face image, we notice that the combination of LPB_4 and LBP_D features achieve higher recognition accuracy for non-LL subbands. On the other hand, $LBP_{8,1}^{u2}$ performs better for LL subbands. Therefore, in this scheme in case of using more than one subbands to represent face feature vector, N_8 scheme used for LL wavelet subband and combined N_4 and N_D used for non-LL wavelet subband(s). Tables from 4.17 to 4.20 shows face recognition accuracy with using different number of subbands, different protocols, and different blocking strategies.

Table 4.17: N_8,N_4&N_D Recognition rates, Yale database used, each wavelet subband is divided to 3×3 blocks

Subband(s)	One training(P1)		5training & 6testing(P2)		Leave one out(P3)	
	N_8	N8,N_4&N_D	N_8	N8,N_4&N_D	N_8	N8,N_4&N_D
LL1,HL1	77.69	82.00	93.11	95.88	93.33	97.57
LL1,LH1	78.08	82.42	91.55	95.88	91.55	96.96
LL1,HL1,LH1	79.21	85.21	92.66	97.66	**93.93**	98.78
ALL Level 1	78.08	83.93	92.66	97.55	93.33	98.78
LL2,HL2	71.81	74.48	88.88	90.66	89.69	93.93
LL2,LH2	73.75	76.72	87.44	91.58	90.09	92.12
LL2,HL2,LH2	75.93	82.00	90.88	94.55	**93.93**	96.36
ALL Level 2	75.93	81.51	90.88	94.88	**93.93**	96.96
LL1,HL1,LH1, LL2,HL2,LH2	**80.66**	**86.36**	**93.55**	**98.11**	**93.93**	**99.39**

Table 4.18: N_8,N_4&N_D Recognition rates, Yale database used, each wavelet subband is divided to 5×5 blocks

Subband(s)	One training(P1)		5training & 6testing(P2)		Leave one out(P3)	
	N_8	N8,N_4&N_D	N_8	N8,N_4&N_D	N_8	N8,N_4&N_D
LL1,HL1	84.36	85.63	96.11	96.88	96.36	98.18
LL1,LH1	83.63	87.03	95.11	97.55	96.36	98.78
LL1,HL1,LH1	84.04	87.21	95.88	97.88	96.96	98.18
ALL Level 1	83.81	86.48	95.77	97.33	96.36	98.18

Subband(s)	One training(P1)		5training & 6testing(P2)		Leave one out(P3)	
	N_8	N8,N_4&N_D	N_8	N8,N_4&N_D	N_8	N8,N_4&N_D
LL2,HL2	80.3	81.51	95	94.00	96.36	95.75
LL2,LH2	82.66	85.81	93.66	97.33	96.36	97.57
LL2,HL2,LH2	83.09	85.81	96	95.66	**98.18**	98.78
ALL Level 2	83.09	87.03	96	96.66	**98.18**	**99.39**
LL1,HL1,LH1, LL2,HL2,LH2	**85.03**	**88.36**	**96.22**	**98.22**	**98.18**	98.18

Table 4.19: N_8,N_4&N_D Recognition rates, ORL database used, each wavelet subband is divided to 3×3 blocks

Subband(s)	One training(P1)		5training & 5testing(P2)		Leave one out(P3)	
	N_8	N8,N_4&N_D	N_8	N8,N_4&N_D	N_8	N8,N_4&N_D
LL1,HL1	69.77	73.22	95.80	96.55	**99.75**	99.50
LL1,LH1	68.83	69.50	96.10	96.05	99.50	99.50
LL1,HL1,LH1	70.36	73.30	96.30	96.70	**99.75**	**99.75**
ALL Level 1	70.30	73.33	96.05	96.40	**99.75**	99.50
LL2,HL2	67.83	70.22	95.15	95.95	99.00	98.25
LL2,LH2	67.27	66.63	94.65	95.60	98.75	99.00
LL2,HL2,LH2	67.77	71.13	94.60	96.65	98.25	99.25
ALL Level 2	67.05	70.13	94.95	96.10	98.00	99.25
LL1,HL1,LH1, LL2,HL2,LH2	**71.63**	**74.97**	**96.35**	**97.95**	**99.75**	**99.75**

Table 4.20: N_8,N_4&N_D Recognition rates, ORL database used, each wavelet subband is divided to 5×5 blocks

Subband(s)	One training(P1)		5training & 5testing(P2)		Leave one out(P3)	
	N_8	N8,N_4&N_D	N_8	N8,N_4&N_D	N_8	N8,N_4&N_D
LL1,HL1	68.44	70.86	96.15	**96.90**	98.25	**99.00**
LL1,LH1	68.52	68.66	95.45	95.55	**98.75**	**99.00**
LL1,HL1,LH1	69.11	71.11	96.15	96.55	98.50	98.75
ALL Level 1	69.16	71.05	95.70	96.70	**98.75**	98.75
LL2,HL2	64.13	67.13	94.50	94.55	**98.75**	98.25
LL2,LH2	65.02	63.02	94.90	94.25	**98.75**	98.75
LL2,HL2,LH2	64.25	66.13	93.55	95.55	98.75	98.50
ALL Level 2	63.61	65.77	94.05	94.55	98.00	98.25
LL1,HL1,LH1, LL2,HL2,LH2	**69.52**	**71.66**	**96.25**	95.95	**98.75**	98.75

The results obtained in this scheme summarised as following:

1. For Yale database, using 5x5 blocking strategy outperform the 3x3 blocking strategy for all protocols. While for the ORL database, the results are in the opposite direction.
2. In terms of the effect of using (N_8 and (N_4 and N_D) or N_8 LBP neighbourhood selection:

   For both (Yale and ORL) database, (N_8 and (N_4 and N_D)) outperforms N_8 for most cases with different protocols and different blocking numbers.
3. The best accuracy rates achieved for the different protocols are as following:

   Yale: P1: 88.36% (N_8 and (N_4 and N_D), 6 subbands and 5x5); P2: 98.22% (N_8 and (N_4 and N_D), 6 subbands and 5x5); and P3: 99.39% (N_8 and (N_4 and N_D), All level 2 and 5x5);

   ORL: P1: 74.97% (N_8 and (N_4 and N_D), 6 subbands and 3x3); P2: 97.95% (N_8 and (N_4 and N_D), 6 subbands and 3x3); and P3: 99.75% (N_8 and (N_4 and N_D), LL1,HL1,LH1 and 3x3);

On the other hand, comparing results obtained using this scheme and all other 4 schemes discussed before, we can conclude that results obtained in this scheme outperform the 4 schemes in all cases for both databases except in some cases of using leave one out strategy with 4th scheme (i.e. fusion of N_8 and N_4).

Finally, we need to determine the effect of each of the 3 different experimental protocols on the performance of all 5 LBPH schemes together in comparison to the traditional N_8 scheme. Figures 4.8 to 4.10 below are results of experiments conducted, according to these various protocols, for this purpose on the Yale database using 3x3 sub-blocking strategies. More comparison figures can be found in the appendix C.

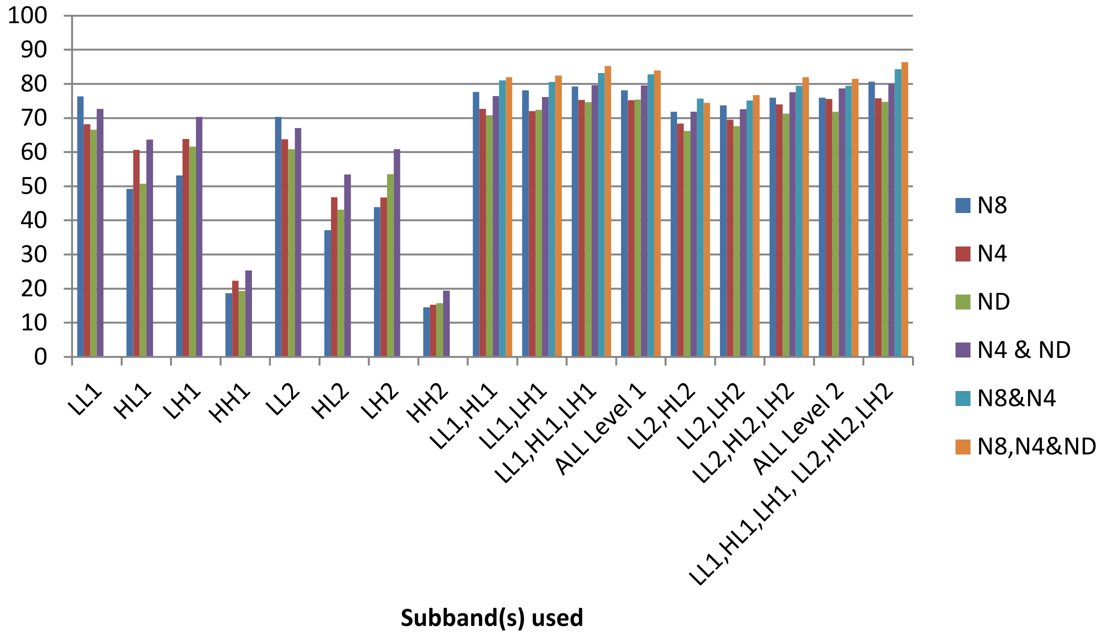


Figure 4.8: Recognition rates of Yale database for one training protocol and 3×3 blocking strategy

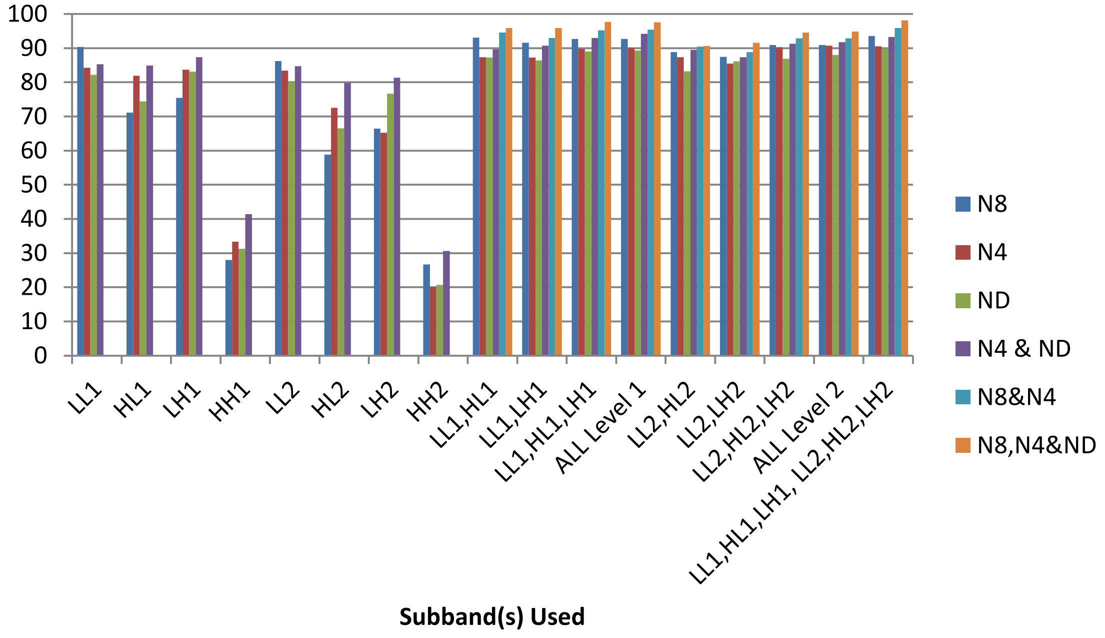


Figure 4.9: Recognition rates of Yale database for 50% training protocol and 3×3 blocking strategy

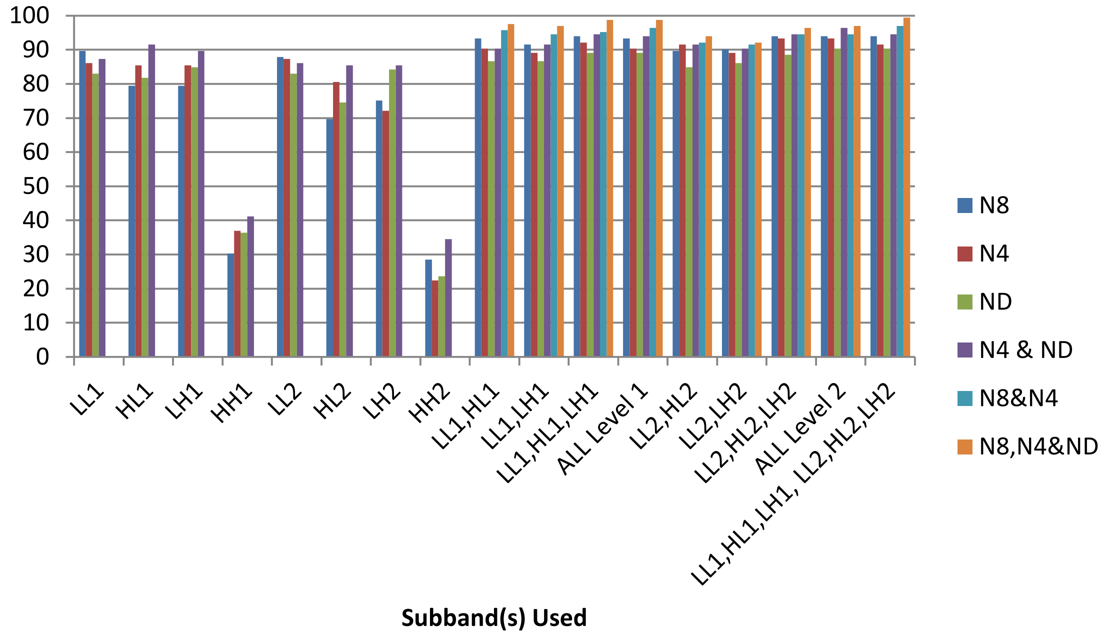


Figure 4.10: Recognition rates of Yale database for leave one out protocol and 3×3 blocking strategy

From these figures it is clear that the performance of each of feature vector schemes (single and multiple wavelet subbands) follow a very similar pattern when comparing the various LBPH representation codes (i.e. the N_4, N_D, N_4&N_D, N_8&N_4, and $N_8$with N_4&N_D) across all the 3 protocols. In other words, their relative performances in terms of the different LBPH coding do not depend on the protocol. However, for any combination of a feature subband(s) and LBPH coding the leave-one-out yields an average improvement of about 2% on the 50-50 protocol which in turn result in significant improvement of as much as 20% (for single subbands) and as little as 12% (for multiple subbands). These improvements are not surprising because the larger the gallery the better chance for accurate matches.

4.5 Trade-off between Recognition Rate and Number of Features

The above results need to be considered in relation to their effect on the adopted steganographic embedding scheme, in terms of invisibility, capacity and robustness. High number of features representation of biometric data should be avoided, if at all possible, for real-time identification and limit their usefulness for applications which require less number of feature representations. In this section we shall consider the impact of capacity on accuracy and discuss the trade-off between these two competing requirements for the schemes tested in section 4.4.

Recall that the number of bins for the 4-neighbours DWT-based LBPH schemes is 16 per block, while the traditional $\mathrm{LBP}_{8,1}$ histogram needs 256 bins per block and the $\mathrm{LBP}_{8,1}^{u2}$ needs 59 bins per block. Tables 4.21, 4.22 and Figures 4.11, 4.12 below show number of total face features for the different schemes. In all cases we compared different schemes with$\mathrm{LBP}_{8,1}^{u2}$.

Table 4.21: Total number of features (LBPH bins); each wavelet subband is divided to 3×3 blocks

Used Subband(s)	N_8	N_4 Or N_D	N_4 & N_D	N_8 with N_4	N_8 with N_4 & N_D
One	531	144	288	---	---
Two	1062	288	576	675	819
Three	1593	432	864	819	1107
Four	2124	576	1152	963	1395
Six	3186	864	1728	1638	2214

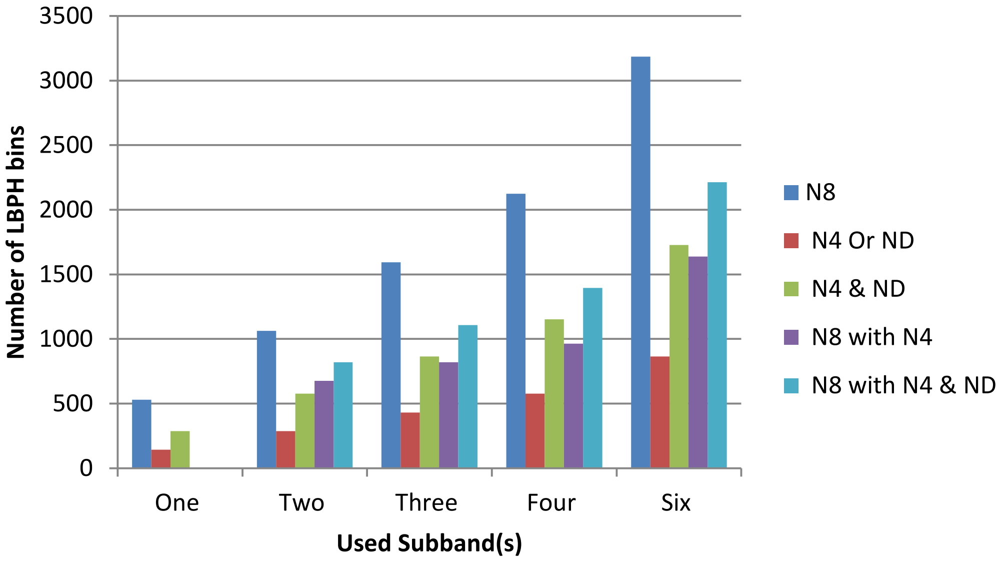


Figure 4.11: Total number of features; each wavelet subband is divided to 3×3 blocks

Table 4.22: Total number of features (LBPH bins); each wavelet subband is divided to 5×5 blocks

Used Subband(s)	N_8	N_4 Or N_D	N_4 & N_D	N_8 with N_4	N_8 with N_4 & N_D
One	1475	400	800		
Two	2950	800	1600	1875	2275
Three	4425	1200	2400	2275	3075
Four	5900	1600	3200	2675	3875
Six	8850	2400	4800	4550	6150

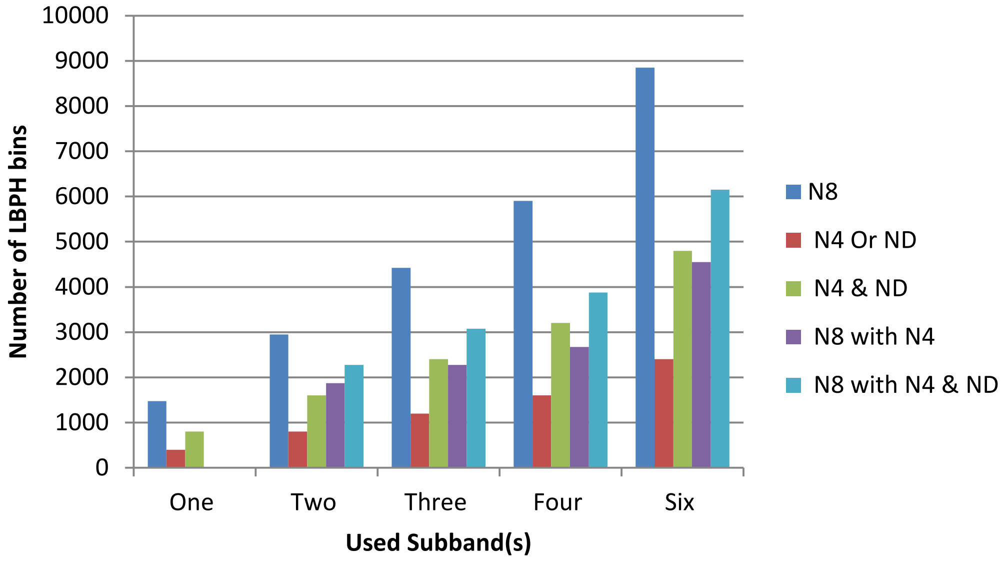


Figure 4.12: Total number of features; each wavelet subband is divided to 5×5 blocks

The above charts show that our 4-neigborhoods LBP histograms, including their combined schemes, have much reduces payload requirement compared to the uniform N_8 LBPH scheme. The reduction rates can be summarized as follows:

- N_4 or N_D: The overall number of face features (LBPH bins) used in each scheme represent a 72.8 % reduction of the number of features used by the $\mathrm{LBP}_{8,1}^{u2}$. For each block they require 16 bins as compared to 59 bins.
- N_4 and N_D: The overall number of face features used in the combined scheme represent a 45.7 % reduction of the number of face features used by the $\mathrm{LBP}_{8,1}^{u2}$. For each block they require 32 bins (16 for each N_4 and N_D) as compared to 59 bins.
- Fusion of N_8 with N_4: Reduction in the number of face features used in this fused scheme is in the range 36.4% to 54.6 % (depending on the number of subbands used) compared to the $\mathrm{LBP}_{8,1}^{u2}$.
- Fusion N_8 with (N_4 and N_D): Reduction in the number of face features used in this case is in the range 22.8 % to 34.3 % (depend on the number of subbands used) compared to the $\mathrm{LBP}_{8,1}^{u2}$.

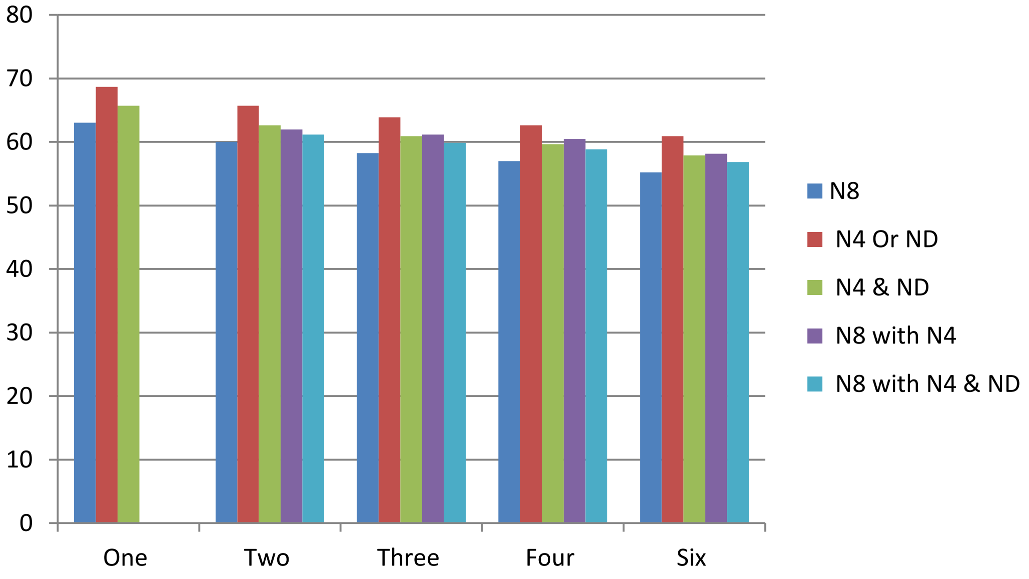
However, this pattern of reduction of space requirements is offset by a reduction in accuracy rates, i.e. accuracy of the singular schemes N_4 or N_D are reduced compared to the other 3 schemes. This may suggest that we need to make a trade-off between face feature requirements and face recognition accuracy rate. However, which the differences in the reduction rates of feature requirement is significant the improvement in accuracy in most cases are relatively marginal. Moreover, we need to remember that hiding secrets of lower payload sizes have a positive impact on stego-image quality, i.e. when we look for trade-offs we should also take into account impact on invisibility. This will be demonstrated in the next section.

4.6 Invisibility Vs Number of LBPH Features

We conducted experiment to test the invisibility achieved by our LSB-witness steganography scheme when we hide the various wavelet based LBPH face feature vectors, discussed above, in images. In these experiments, we followed the same approach adopted in the last chapter by embedding into 20 different images of size 512x512. The results shown in tables 4.23 and 4.24 are the average PSNR values when we embedded the various LBPH face features using all the face images in the Yale database, figures 4.13 and 4.14 represents corresponding tables content. It is clear that hiding face features using our N_4 or N_D LBPH features has higher level of invisibility compared to all other schemes.

Table 4.23: PSNR between cover and stego-image (3×3 blocking)

Subband(s)	N_8	N_4 Or N_D	N_4 & N_D	N_8 with N_4	N_8 with N_4 & N_D
One	63.02	68.65	65.68		
Two	60.01	65.68	62.65	61.98	61.15
Three	58.24	63.9	60.92	61.15	59.83
Four	56.99	62.65	59.66	60.44	58.83
Six	55.23	60.92	57.89	58.12	56.81



:

Figure 4.13: PSNR between cover and stego-image (3×3 blocking)

Table 4.24: PSNR between cover and stego-image (5×5 blocking)

Subband(s)	N_8	N_4 Or N_D	N_4 & N_D	N_8 with N_4	N_8 with N_4 & N_D
One	58.59	64.25	61.25		
Two	55.57	61.25	58.22	57.52	56.69
Three	53.81	59.49	56.46	56.69	55.39
Four	52.56	58.22	55.21	55.99	54.39
Six	50.79	56.46	53.45	53.68	52.37

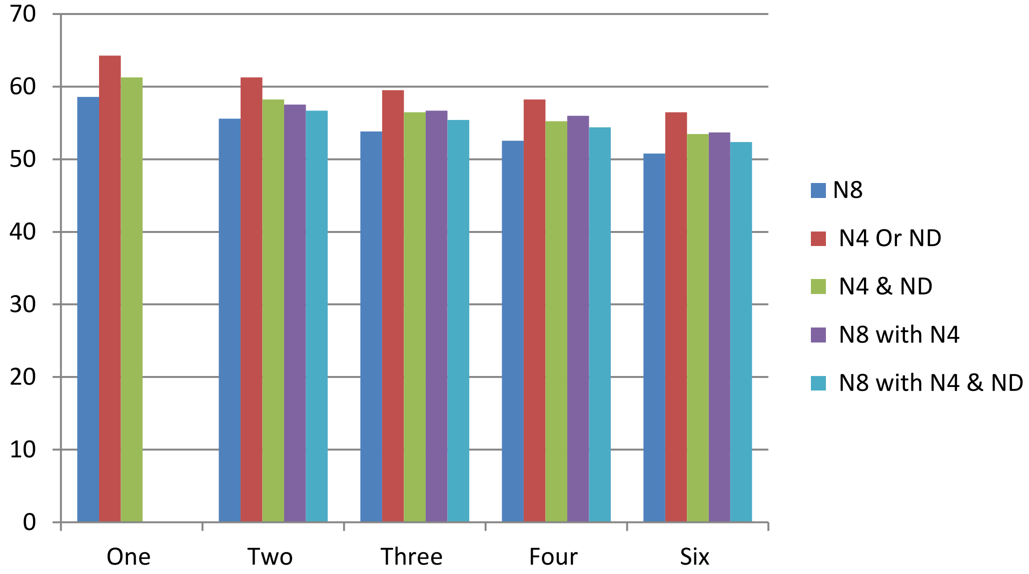


Figure 4.14: PSNR between cover and stego-image (5×5 blocking)

4.7 Conclusions

In this chapter we developed and investigated various properties of a mutli-scale wavelet based local binary pattern, that generalise existing spatial domain versions of these scheme, for use in face recognition. The main approach was to generalise LBPH coding schemes into the wavelet domain the objective being to obtain an optimally compact representation of face feature vectors that form a suitable payload for hiding in an image without loss of accuracy or degradation of stego-image quality.

In the proposed face extraction schemes we define a new LBP operator using only 4 neighbours instead of the normal 8 neighbours for any given wavelet subband. For any wavelet coefficient its 8-neighbours can be separated into two parts, the four main neighbours (N_4) and the four diagonal neighbours (N_D). Totally we propose 5 deferent face feature extraction schemes, in the first 2 schemes, the LBPH obtained from the LBP codes extracted using (N_4 or N_D). While in the 3rd scheme we concatenate the LBPH obtained from using N_4 and N_D separately to represent final face feature vector.

In the 4th scheme, in case of using multiple wavelet subbands to represent face image we calculate LBPH using N_8 for LL subband(s) and N_4 for other subband(s). While in the 5th scheme again we used N_8 for LL subband and LBPH extracted from N_4 concatenated with LBPH extracted from N_D used for non LL subbands. All 5 schemes tested and evaluated using 2 different face database (Yale and ORL), 2 different blocking (3x3 and 5x5) strategies, and 3 different protocols regarding partitioning face images as training and testing sets.

The experimental results demonstrate that new proposed schemes reduced the number of face features by 22% to 72% of the original features size. In term of face recognition our schemes 3 to 5 obtain better accuracy if compared with using original N_8 scheme, while for other first 2 schemes we obtain better accuracy in some cases while in others using N_8 outperform our schemes. Moreover, the experiments revealed that the relative performances of the various LBPH codes were following the same pattern for almost all feature vector schemes (single and multiple wavelet subbands) across all the 3 protocols, and when more templates used in the gallery, the accuracy rates increases by a similar proportion for all schemes. We consider this as an indicator of the stability of all combinations of single or multiple wavelet subbands and LBPH schemes.

Finally, for the rest of the thesis we introduce a new secret embedding content based steganography technique that is compatible with the structure of the wavelet based 4 or 8 neighbours LBP codes for further improvement of capacity, stego-image quality and more importantly robustness against different targeted and universal steganalysis tools.

Chapter 5
Content-Based Steganography

Most digital steganography schemes are designed for embedding any types of secret and therefore most performance testing work assumes that the secret is a random binary string which may represent a cryptographic key, an encrypted image, normal text, or audio file. These embedding schemes do not pay any attention to the characteristics of the secret bit-stream. Content-based steganographic scheme on the other hand refers to schemes for which the embedding benefits from the knowledge of the specific structure or nature of the content to be embedded. In this chapter we shall investigate possible approaches to benefit from secret content structure in designing efficient steganography scheme which is suitable for the hiding secrets with similar characteristics in images that minimizes the necessary changes in the cover image and maintain high quality and robustness. We shall design a content based hiding scheme specifically for hiding secrets that constructed from LBP codes extracted from the spatial or wavelet domains of face image as special cases. The experimental work will be designed to demonstrate the above claims about the designed content based scheme for LBP codes from a large database of face images, each embedded in 1000 images. In section 5.1, we shall investigate different embedding schemes in term of the probability of changing pixel values. Section 5.2 is devoted to the design of the special content-based hiding scheme. In section 5.3 we test the performance of the content-based hiding scheme with different scenarios. In section 5.4 we shall demonstrate that our scheme significantly lower pixels change ratios for embedding face biometric feature vector compared to existing lower bounds achieved by the state of the art embedding schemes. We shall also show that embedding face LBPH patterns into existing schemes that are incapable of achieving the optimal change ratio achieved by our scheme.

5.1 Perfect Vs Optimal Steganography

Andrew Ker *et al.* (Ker, et al., 2013), define perfect steganography technique as it requires that the distribution of the stego-object be identical to that of cover-object, and in optimal steganography techniques the aim is to keep distributions near each other (i.e. not identical but the sender hides the secret message while minimizing the distortion of the cover-object).

In the traditional LSB schemes, when a match is not found between the next secret bit and the LSB of the next pixel, even pixel values are increased by one, while odd pixel values are decreased by one. It is well known that the probability of non-match (equivalently the probability of changing pixel values) in this technique is 0.5 (i.e. 50 % of LSBs of the pixels may change during embedding process). This method changes the distribution of the cover-image pixel values, and makes the technique detectable using statistical steganalysis techniques such as (Fridrich, et al., 2001; Westfeld & Pfitzmann, 1999; Fridrich & Goljan, 2004; Zhang & Ping, 2003). For the LSBM scheme the embedding of an unmatched secret bit will cause random change of +1, or -1 of the pixel value. This makes LSBM harder to detect, but again there are some new proposed steganalysis techniques can detect the LSBM schemes such as (Ker, 2005; Zhang, et al., 2007). Again in this scheme, the probability of changing pixel values is remaining 0.5 as traditional LSB scheme. While in LSBMR (Mielikainen, 2006) scheme the probability of changes downgraded to 0.375 with remaining in the same level of payload capacity if compared to LSBM.

Related to the above idea, authors in (Holub, et al., 2014) mentioned and proved that the most successful techniques in steganography are those techniques that embed secret payload while minimizing the distortion of the pixel values. Recently a number of embedding schemes is proposed by group of researchers in both domains, spatial and frequency, but because we are deal with spatial domain embedding then we will focus on proposed embedding techniques in spatial domain.

Authors in (Pevný, et al., 2010; Filler & Fridrich, 2010; Holub & Fridrich, 2012; Holub, et al., 2014) proposed four steganographic schemes based on LSBM fundamental, they named the embedding schemes as Highly Undetectable SteGO (HUGO), HUGO with Bounding Distortion (HUGO BD), Wavelet Obtained Weights (WOW), and Universal Wavelet Relative Distortion (UNIWARD) respectively. Their contributions in the papers are, designing the distortion function aimed to find the best locations for embedding which make less change in cover pixels values during embedding, to make the steganographic techniques more robust against steganalysis techniques. Proposed schemes are related to each other with some modification in term of improving in designing the distortion function. Overall the probabilities of modification pixel values approximately are 0.26, 0.26, 0.25, and 0.24 per pixel for HUGO, HUGO BD, WOW, and UNIWARD respectively.

Although our LSB-witness does not change the LSB but it cannot be categorised as perfect or optimal hiding scheme. This due to the fact that our scheme makes changes in the 2nd bit-plane. The following table shows the average amount of changes in the 2nd bit plane after using the LSB-witness scheme with 5 different payloads embedded in the same 1000 images used in this chapter.

Table 5.1: Change Rate using LSB-Witness

Payload	0.2	0.4	0.6	0.8	1
Change rate	0.099	0.2	0.3	0.4	0.5

These results indicate the amount of change in the 2nd bit-plane is remaining nearly 0.5 (i.e. 50% of pixel values are change) of the payload as normal LSB embedding scheme.

In the rest of the thesis we shall develop a new hiding scheme that retains the same steganographic capabilities of the witness scheme but aiming to achieve higher invisibility and minimal amount of change to LSB plane. The new scheme will have the same capability in relation to hiding biometrics features without affecting the accuracy rates, before and after embedding. In fact, the new scheme will be shown to improve the lower bound on optimality achieved by UNIWARD scheme and reduce overall probability of pixel values changes to range between 0.13 and 0.15 for fully payload capacity. This will lead to decrease the distortion (noise) that is occurred in the pixels of the cover image, increase the quality of the stego-image, and as a result increase the immunity of the stego-image against the visual attack and steganalysis methods in general, more especially statistical steganalysis techniques. It is important to note that the amount of changes will be dependent on the structure of the secret message, and hence one may define optimality lower bound for content-based steganography in the sense that the achieved lower bound may not remain if it is applied to secrets from different type of content. In fact, in our scheme the nature of the secret message means that the embedding has a great deal of freedom in the order of selected embedding positions.

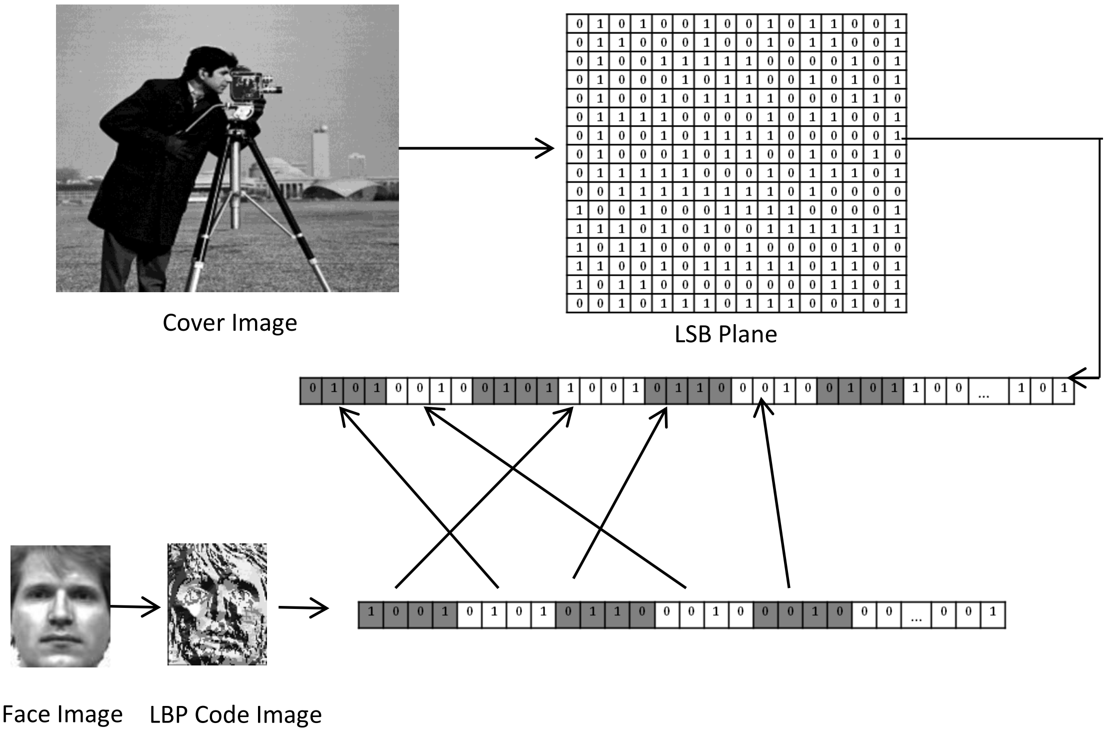
5.2 A Content-based Steganography Scheme for Face Biometric

In most LSB based schemes, the LSB bits are modified without looking to the structure of the secret message (i.e. the secret message is converted to bit stream and replaced with the LSB of the selected pixels of the cover image bit by bit). The change is invisible to human vision system but it might be visible to some steganalysis tools. Although, the review in chapter 2 has revealed a number of research publications proposing the hiding of biometric data in cover images, but none of them, including our LSB-witness, differentiate between hiding biometric features and hiding any other kinds of secret data (text, image, etc.). To the best to our knowledge, there is no critical discussion in the literature about exploiting knowledge of secret content in guiding the hiding scheme. In addition most proposed steganographic schemes before are apply in the laboratory conditions, therefore there is need to move the steganography aspect from the laboratory into the real world (Ker, et al., 2013). In the rest of this chapter, we introduce a content-based hiding scheme for the purpose of hiding face biometric feature vectors, as an example which can be extended to many other types of secrets. Our approach will emphasise an important guiding principle for content-based steganography that "*knowledge of the secret content structure must guide the selection of an appropriate cover images embedding positions to reduce changes*".

The proposed scheme is concerned with embedding the face biometric LBP code pattern features defined in the wavelet. Since it is the secrets is related to the values of the various bins obtained from the blocks of the wavelet subbands, then the developed scheme apply equally to any secret data that are based on frequency calculations. Note that embedding the values associated with the LBPH bins; give us the freedom to choose positions for embedding without having to worry about the sequence appearance of the extracted features by the receiver or an attacker. The following image (Figure 5.1) illustrates the exact matching procedure between secret message 4-bit LBPH patterns and the cover block LSB bit strings. It is clear that there are similar patterns between secret message bits and patterns in image LSBs, but in different sequence positions.

5.2.1 Embedding Process

In order to reduce the amount of changes in the LSB plane, the proposed steganography scheme try to find the match pattern between the 4 or 8 bits of the secret message (face LBP code features) and the LSBs extracted from 4 or 8 pixels of the cover-image. The main idea is to divide the cover image into blocks, the size of which is dependent on the blocking strategy of the face LBP code features and on the number of neighbours used to construct the LBP code (i.e. 4-neighbours or 8-neigbours), so that each block in the cover image must contain 4 or 8 pixels as many as the size of the face LBP code block. Each face LBP code block is embedded in one cover image block. The LSB-plane of the cover block will be partitioned into 4-bit or 8-bit strings according to whether we use LBP code of size 4 or 8. The algorithm is based on first matching as many LBP codes with LSB bit-strings to be skipped and then embedding the rest of unmatched LBP codes of the secret block in the remain cover block LSB bit strings. For the unmatched codes we can follow two different strategies for embedding them: either use the usual LSB scheme to embed the remaining LBP code bits in the remain cover block LSB bit strings OR calculate the Hamming distances between the remain cover block LSB bit strings and the un-matched LBP codes and then sequentially replace the cover strings with the LBP codes that have hamming distance 1, 2, and so on until all is embedded. Hamming distance between two binary streams of equal length is the number of positions at which the corresponding bits are different. For example if we have two binary streams, a=01011010 and b=01110010, then the hamming distance between this two binary streams is 2, while for a=11011011 and b=01101111 the hamming distance is 4.



0	1	0	1	0	0	1	0	0	1	0	1	1	0	0	1
0	1	1	0	0	0	1	0	0	1	0	1	1	0	0	1
0	1	0	0	1	1	1	1	1	0	0	0	0	1	0	1
0	1	0	0	0	1	0	1	1	0	0	1	0	1	0	1
0	1	0	0	1	0	1	1	1	1	0	0	0	1	1	0
0	1	1	1	1	0	0	0	0	1	0	1	1	0	0	1
0	1	0	0	1	0	1	1	1	1	0	0	0	0	0	1
0	1	0	0	0	1	0	1	1	0	0	1	0	0	1	0
0	1	1	1	1	1	0	0	0	1	0	1	1	1	0	1
0	0	1	1	1	1	1	1	1	1	0	1	0	0	0	0
1	0	0	1	0	0	0	1	1	1	1	0	0	0	0	1
1	1	1	0	1	0	1	0	0	1	1	1	1	1	1	1
1	0	1	1	0	0	0	0	1	0	0	0	0	1	0	0
1	1	0	0	1	0	1	1	1	1	1	0	1	1	0	1
1	0	1	1	0	0	0	0	0	0	0	0	1	1	0	1
0	0	1	0	1	1	1	0	1	1	1	0	0	1	0	1

0	1	0	1	0	0	1	0	0	1	0	1	1	0	0	1	0	1	1	0	0	0	1	0	0	1	0	1	1	0	0	…	1	0	1

1	0	0	1	0	1	0	1	0	1	1	0	0	0	1	0	0	0	1	0	0	0	…	0	0	1

Figure 5.1: 4-bits pattern matching

The embedding process shown in figure 5.2 (pseudo code) and figure 5.3 (flow chart) can be summarized as the following steps:

1- Read face image (secret message) and divide it to N blocks. Here, N selected based on the sub-blocking process that used for face recognition purpose.
2- Extract LBP code from each block using 4 or 8 neighbours (as explained in chapter 4) and save them to be ready for embedding.
3- Read greyscale cover image and convert it to bit planes.
4- Separate LSB bit-plane from other 7 bit planes.
5- Convert each 4 or 8 bits from LSB bit-plane to one sub-region pattern.
6- Select N blocks from LSB bit-plane. Size of each block based on face block size (i.e. each block of cover image must carry one block of face LBP code).
7- For each block of the cover image LSB bit-plane do the following:
    a- Find exact match pattern between extracted LBP codes from step 2 with the sub-region patterns from step 5.
    b- Kept matched sub-region patterns in cover LSB bit-plane as it's and exclude them from the next process.
    c- Repeat steps 7-a and 7-b until all face LBP codes inside selected block are checked.
    d- For remaining unmatched LBP code one of the two methods below applied:
        - M1: Search the remained sub-region patterns in the cover LSB bit-plane and make it as a remained face LBP codes using normal LSB embedding scheme.
        - M2: Search the remained sub-region patterns in the cover LSB bit-plane and make it as a remained face LBP codes first by selecting sub-region patterns that have minimum difference with the remained face LBP codes, second minimum differences selected and so on. (This step done by calculating hamming distance between remained sub-region patterns in the cover LSB bit-plane and remained face LBP codes).
8- Return back the modified blocks to obtain modified LSB bit-plane.
9- Concatenate modified LSB bit-plane with the other 7 bit planes to obtain final stego-image.

```
Input: Cover Image (C), Face Image (F), Number of block (N), Pattern size (P=4 or P=8),
       no.of bins=16 or 59
Output: Stego-Image (S)
  START
     READ Face Image (F)
     Divide Face Image (F) into N blocks.
     CALCULATE LBP code of the N blocks using P scheme neighbouring and save the
     histogram results in LBPH.
     READ Cover Image (C)
     Separate LSB plane from other bit-planes of C
     Divide LSB plane into M blocks (size of each block = P*size of Face block)
     Convert each P bits from LSB bit-plane block into K sub-region pattern (CB)
     Choose N blocks from M blocks
     SET b=1                    // block counter
     WHILE b < N                // for each block do the following
        SET R=0                 // counter for remain un-matched patterns
        FOR i=1 to K            // looking for exact matches
           FOR j=1 to no.of bins
              IF  LBPH(j) <> 0 THEN
                 IF CB(i) = LBP code of LBPH(j) THEN
                    LBPH(j)= LBPH(j)-1 GOTO 10
                 ENDIF
              ENDIF
            ENDFOR
           R=R+1                // if exact match not found increment counter
           Remain(R)=i          // to save index of remain un-matched patterns
        10 ENDFOR
        FOR i=1 to R            // embed remain un-matched patterns
           FOR j=1 to no.of bins
              IF  LBPH(j) <> 0 THEN
               CB(Remain(i)) = LBP code of LBPH(j)
               LBPH(j)= LBPH(j)-1 GOTO 20
              ENDIF
           ENDFOR
        20 ENDFOR
        b=b+1
        ENDWHILE
        Return back the modified cover blocks (CB) to the LSB plane
        Concatenate LSB plane with the other bit planes to obtain final stego-image (S)
  END
```

Figure 5.2: Embedding process Pseudo code

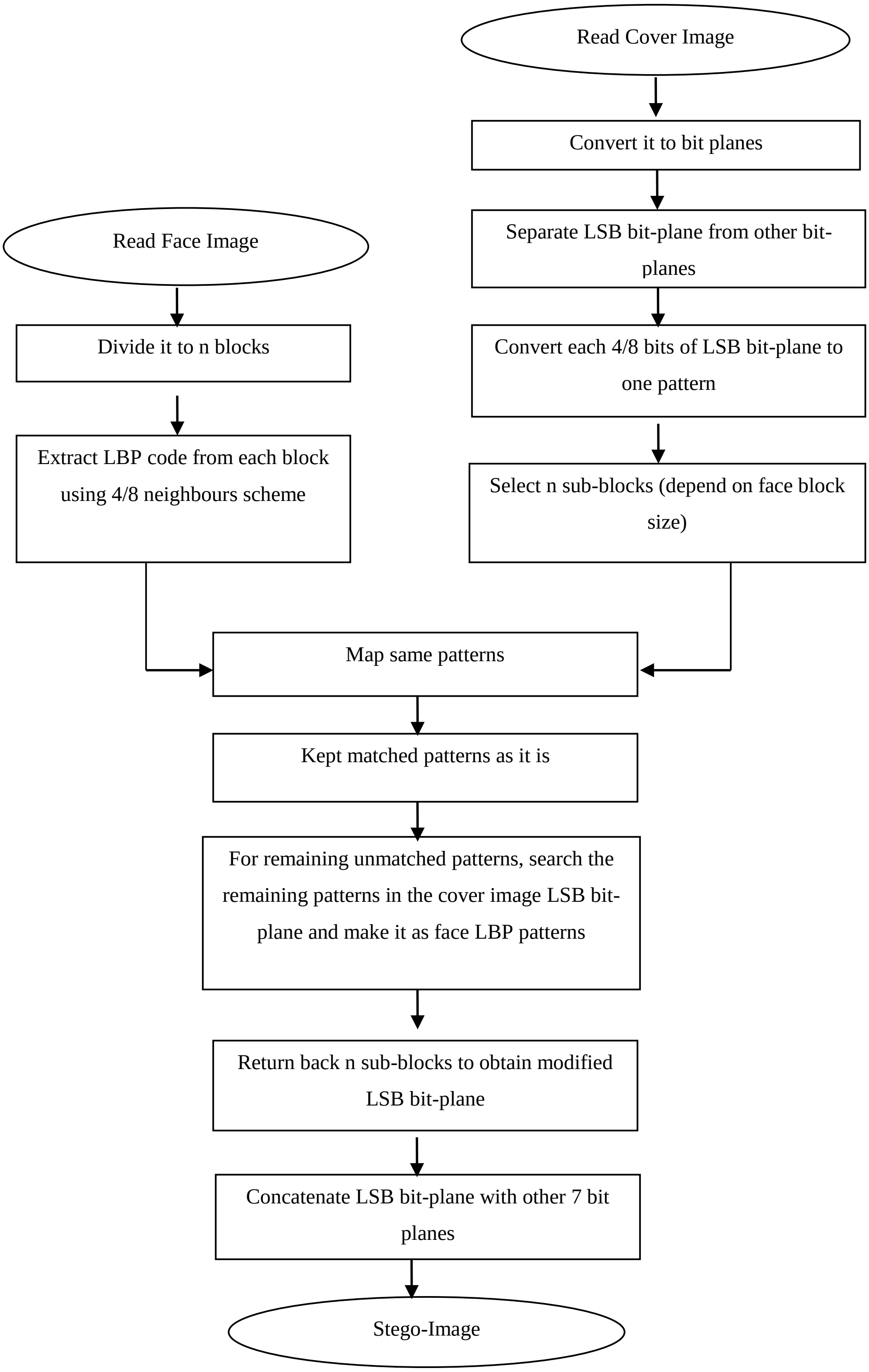

Read Cover Image
Convert it to bit planes
Separate LSB bit-plane from other bit-planes
Convert each 4/8 bits of LSB bit-plane to one pattern
Select n sub-blocks (depend on face block size)
Read Face Image
Divide it to n blocks
Extract LBP code from each block using 4/8 neighbours scheme
Map same patterns
Kept matched patterns as it is
For remaining unmatched patterns, search the remaining patterns in the cover image LSB bit-plane and make it as face LBP patterns
Return back n sub-blocks to obtain modified LSB bit-plane
Concatenate LSB bit-plane with other 7 bit planes
Stego-Image

Figure 5.3: Embedding Process flow chart

5.2.2 Extraction Process

Recovering the secret message (Face LBPH features) from the stego-image is required on the receiver side to be used for the recognition purpose. Before the extraction process starts, the sender and receiver must agree on some parameters which are needed for the purpose of extraction. For example in our case sender and receiver must agree on the number of blocks, the size of each block, and the pattern size (4 or 8) to be used for extracting the LBP codes of the face image. These parameters would either be sent or embedded within the cover by the sender, and can be used as shared key between sender and receiver as a second layer of the security that guarantees exact extraction by authorized entities only. Figure 5.4 (pseudo code) and figure 5.5 (flow chart) shows the extraction process which will be held at the receiver side.

```
Input: Stego Image (S), Number of Blocks Used (N), Pattern size (P=4 or P=8), size of Face block
Output: Face Feature vector (V)
  START
      READ Stego Image (S)
      Separate LSB plane from other bit-planes of S
      Divide LSB plane into M blocks (size of each block = P*size of Face block)
      Convert each P bits from LSB bit-plane block into K sub-region pattern (SB)
      Choose N blocks from M blocks
      SET b=1
      WHILE b < N
          Convert each K into one gray value
          Calculate the histogram of the extracted gray values and save it as H (b)
          b=b+1
      ENDWHILE
      Concatenate all the histograms (H) to obtain final face feature vector V
      Obtained V is used for the recognition purpose
  END
```

Figure 5.4: Extraction Process Pseudo code

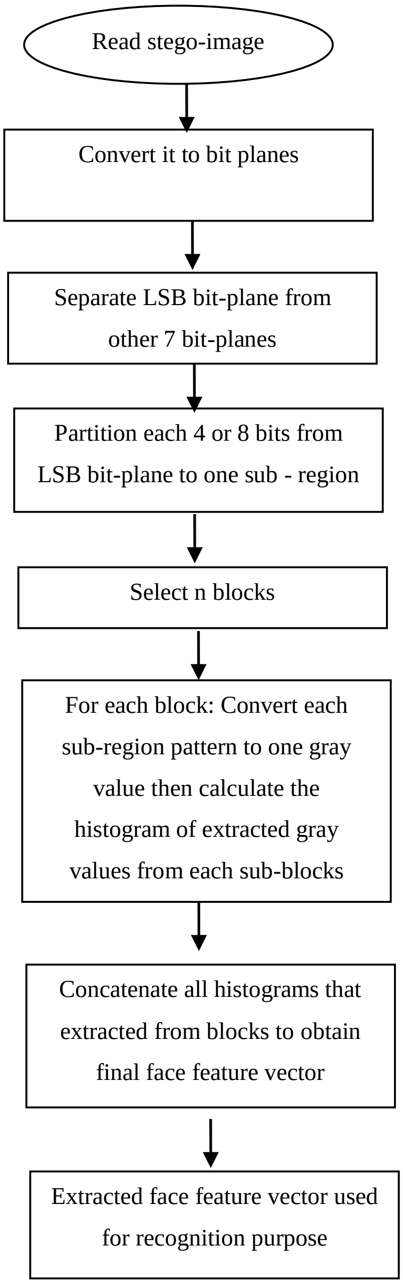

Read stego-image
Convert it to bit planes
Separate LSB bit-plane from other 7 bit-planes
Partition each 4 or 8 bits from LSB bit-plane to one sub - region
Select n blocks
For each block: Convert each sub-region pattern to one gray value then calculate the histogram of extracted gray values from each sub-blocks
Concatenate all histograms that extracted from blocks to obtain final face feature vector
Extracted face feature vector used for recognition purpose

Figure 5.5: Extraction Process Flow chart

One can summarize the extraction process shown in figure 5.4 (pseudo code) and figure 5.5 (flow chart) as following steps:

1- Read received stego-image and convert it to bit planes.
2- Separate LSB bit-plane from other 7 bit-planes.
3- Partition each 4 or 8 bits from LSB bit-plane to one sub-region pattern. (pattern size 4 or 8 agreed/communicated between sender and receiver)
4- Select n blocks from LSB bit-plane. Size of each block based on face block size (number of blocks (n) agreed/communicated between sender and receiver)
5- For each block of the stego-image LSB bit-plane do the following:

a- Convert each sub-region pattern to one gray value.

b- Calculate the histogram of the extracted gray values.

6- Concatenate all the histograms that extracted from all blocks to obtain final face feature vector.

7- The extracted face feature vector used for recognition purpose.

5.2.3 Block Mapping

Due to differences between cover image size and the size of the original face image, there may be a need to have a policy on mapping the secret blocks to the cover blocks. The selected mapping must be communicated to the receiver. For simplicity, let n = number of Face feature blocks and m = number of cover blocks. Given any LBPH feature block S, we shall that a block C from the LSB-plane of is optimally matched with S, if number of matches between the LBP codes and the LSB-plane strings is maximal among all cover blocks. In terms of the proposed steganographic schemes, block mapping need to be considered in two different scenarios;

1- First scenario (n < m) In this case not all cover image blocks are needed for embedding purpose, and there are $\binom{m}{n}$ different block mapping that could be used. So, the selected mapping could be agreed in advance or done in the order of optimal pairing between the two sets of block. Figure 5.6 shows an example of selecting 9 blocks out of 30 block in cover image.

2- Second scenario (n=m) Here the mapping could be the trivial sequential mapping, or for more security we can select the blocks in the order of optimal pairing between the two sets of block.

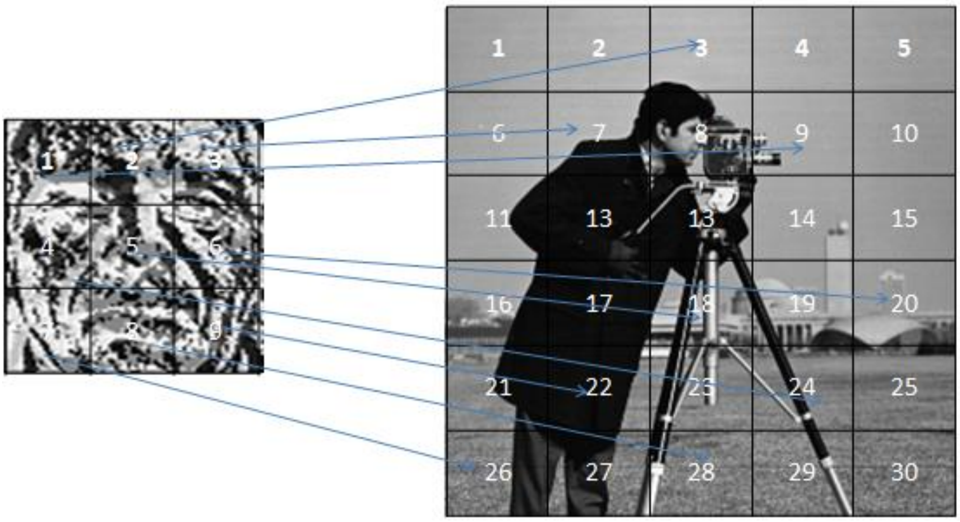


Figure 5.6: Block Selection Process (n<m)

5.3 Experimental Setup and Discussion

To test the proposed embedding scheme we extract LBP code using 8-neighbours or 4-neighbours separately, see Chapter 4. Each LBP code is represented by 8-bits or 4-bits, and matched or embedded to/in 8-bit or 4-bit strings from a block of the LSB-plane of the cover image. For simplicity, we name theses matching as 8 or 4 pattern matching.

To evaluate the performance of the proposed steganography scheme, we extracted the 4 or 8 LBP patterns for all the face images in the Yale face database each representing a secret message, details of the face database can be found in section (2.1.4). For each face image we embedded the corresponding secret in 1000 greyscale cover images gathered from the BOSSbase database ver. 1.01 (Bas, et al., 2011). Images of the BOSSbase are taken by eight different cameras, resized and uncompressed. These images are all of size 512 × 512 pixel resolution, but have different properties regarding textures and smooth areas. Figure 5.7 shows some of used image samples.

Figure 5.7: Samples of Cover Images Used from BOSSbase Database

Before we discuss results, we need to alert the reader to the fact that for the original purpose of embedding a face LBP code feature vector cannot provide a secret of sufficient size for full capacity embedding unless we choose very small cover images. For example, for face images in the Yale database even if we embed all LBP codes extracted in the spatial domain we need only around 11% or 22% of the used cover size for N_4 or N_8 scheme respectively. Therefore, for the purpose of evaluating performance of our proposed embedding schemes we embed multiple LBP code feature vectors obtained from different face images of the same person but with different expressions. Therefore, the results of the experiments reflect the use of the 5 different payload percentages (0.2285, 0.45, 0.6855, 0.9141, and 0.9902) by embedding single or multiple face feature vectors into the 512x512 cover images. For simplicity we refer to these percentages using A, B, C, D, and E, respectively. Numbers of patterns are different based on the payload capacity as well as the LBP pattern size (4 or 8). Table 5.2 below shows exact number of patterns that are to be embedded for each payload using different pattern size.

Table 5.2: Pattern numbers for each payload

Payload	8-bit pattern	4-bit pattern
A	7488	14976
B	14976	29952
C	22464	44928
D	29952	59904
E	32448	64896

In what follows, we test the performance of 3 versions of the scheme. These versions differ in the way we embed the non-matching 4 or 8 unmatched (UM) patterns. Also in the first two versions, the block mapping is not considered but the last version uses the special mapping (section 5.2.3).   Therefore, in all cases we skip the first set of LSBs extracted from 4 or 8 pixels of the cover-image that matched the 4 or 8 bits of the LBP code secret features in each block. Thus we only need to discuss the way the set UM of unmatched 4 or 8 LBP code secret patterns are embedded in the rest of the block.

5.3.1 Method 1

In each block, for the set UM of unmatched patterns, directly normal LSB embedding applied without looking at the Hamming distances between the individual LSB- pattern and the LBP code pattern. Table 5.3 and 5.4 (or figures 5.8 and 5.9) below, shows the number of exact matched patterns as well as the number of unmatched patterns for all five different payload capacities. The unmatched patterns are arranged in columns according to the Hamming distances, post embedding, between secret patterns and cover LSB patterns in case of length of each pattern is 8-bits and 4-bit patterns, respectively. In both cases we calculate ratio of match and ratio of change after embedding. All results are presented here is the average results obtained by using 1000 greyscale images as cover.

Table 5.3: M1_8-bits, Number of matched and unmatched patterns

Payload	Exact match	1-bit diff	2-bits diff	3-bits diff	4-bits diff	5-bits diff	6-bits diff	7-bits diff	8-bits diff	R. of match	R. of change
A	2510.5	144.8	509.8	1107.0	1486.8	1111.5	502.2	112.3	3.2	0.669	0.331
B	4378.2	301.2	1090.1	2318.4	3065.3	2308.9	1047.8	225.1	7.0	0.651	0.349
C	6485.8	447.1	1661.9	3592.0	4735.4	3592.0	1608.5	334.8	6.4	0.647	0.353
D	8734.6	587.5	2205.9	4769.0	6290.9	4775.2	2139.9	441.5	7.4	0.648	0.352
E	9368.3	643.7	2400.4	5186.6	6823.8	5192.7	2338.5	485.8	8.3	0.647	0.353

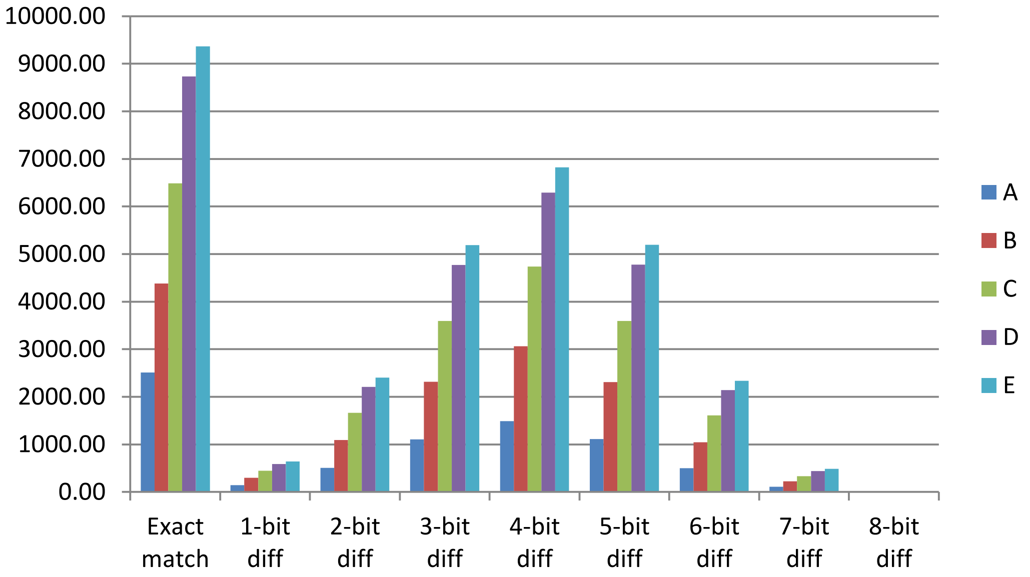


Figure 5.8: M1_8-bits, Number of matched and unmatched patterns

Table 5.4: M1_4-bits, Number of matched and unmatched patterns

Payload	Exact match	1-bit diff	2-bit diff	3-bit diff	4-bit diff	R. of match	R. of change
A	9692.64	1419.21	2964.96	869.16	30.03	0.832	0.168
B	19188.69	2888.91	5799.77	2004.56	70.08	0.827	0.173
C	28410.39	4606.89	8605.28	3198.69	106.76	0.823	0.177
D	38481.65	5854.16	11019.31	4409.46	139.42	0.826	0.174
E	41958.81	6240.48	11792.38	4756.42	147.91	0.828	0.172

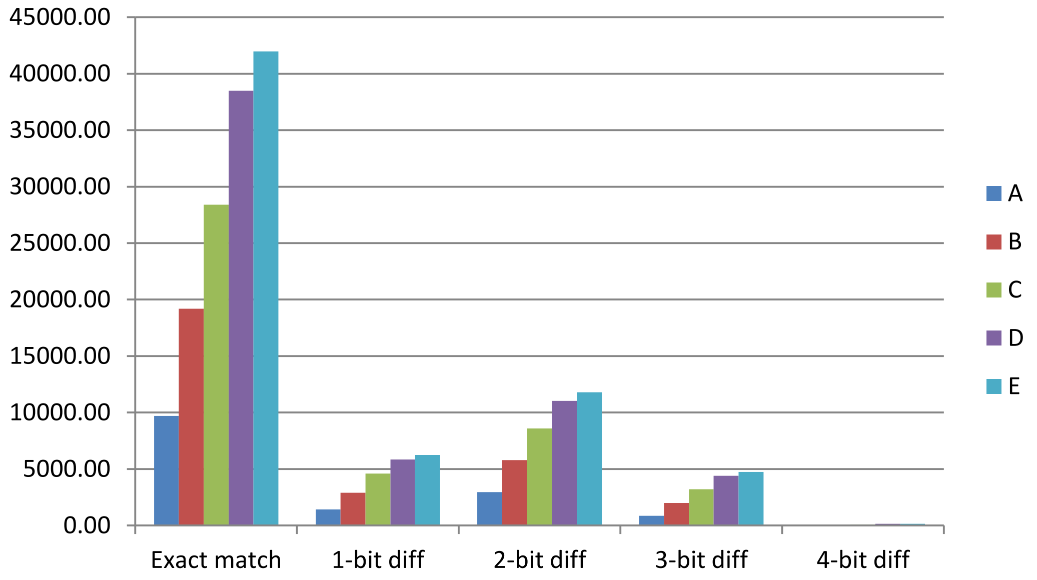


Figure 5.9: M1_4-bits, Number of matched and unmatched patterns

From the above tables or figures, we notice that a high proportion of secret patterns have exact matches with the cover patterns and after applying the normal LSB embedding technique we found that the proportion of pixel changes are very modest in this method. The ratio of match is more than 82% for the N_4, and more than 64% for the $N_{8,}$ in another word we can say that the change rate is less than 18% for N_4, and less than 36% for N_8 pattern size. We note that the percentage of the UM set of unmatched secret patterns are normally distributed over the hamming distances between them and the remaining patterns of the LSB-plane, with mean of 4-bits (2-bits) for the N_8 (N_4). This is interesting, and the next method would be based on a different embedding strategy to further reduce the amount of changes.

Further analysis of the results, demonstrate that the length of patterns affect the matching ratio between cover patterns and secret message patterns. Using short length patterns have increases matching ratio, due to the fact that the probability of finding matches of short length patterns is higher than for long length patterns. Hence we recommend to using the LBP N_4 code.

5.3.2 Method 2

This method is based on a different approach to embedding than the usual LSB for the UM set, with the aim of reducing the amount of changes beyond what was achieved by method 1. In each block, for the set UM of unmatched patterns we search for unused LSB patterns that have Hamming distances of 1 with the LBP patterns, and for each such pattern we simply replace the 8 or 4 LSB pattern with that of the LBP patterns, and when all such LBP patterns are embedded we repeat the process by searching and replacing those remaining LSB patterns with the LBP patterns at hamming distance 2, and so on. Table 5.5 and 5.6 (or figures 5.10 and 5.11) below, shows the number of matched patterns as well as the number of unmatched patterns for all five different payloads. The unmatched patterns are arranged according to the how many bits are different between secret patterns and cover LSB patterns in case of length of each pattern is 8-bits and 4-bit patterns, respectively. In both cases we calculate ratio of match and ratio of change after embedding. All results are average results from using 1000 greyscale cover images. Again, the N_4 patterns yields a better matching ratio than the N_8 patterns.

Table 5.5: M2_8-bits, Number of matched and unmatched patterns

Payload	Exact match	1-bit diff	2-bits diff	3-bits diff	4-bits diff	5-bits diff	6-bits diff	7-bits diff	8-bits diff	R. of match	R. of change
A	2510.5	2292.0	1592.0	794.9	269.5	24.0	4.0	1.4	0.5	0.848	0.152
B	4378.2	4479.9	3314.7	1731.0	707.9	122.2	5.6	1.9	0.6	0.832	0.168
C	6485.8	7078.5	5145.5	2525.9	986.6	229.2	10.2	1.6	0.5	0.832	0.168
D	8734.6	9538.4	6696.9	3367.8	1304.0	295.5	12.5	1.6	0.5	0.834	0.166
E	9368.3	10230.6	7299.1	3672.2	1472.5	388.8	14.2	1.7	0.6	0.831	0.169

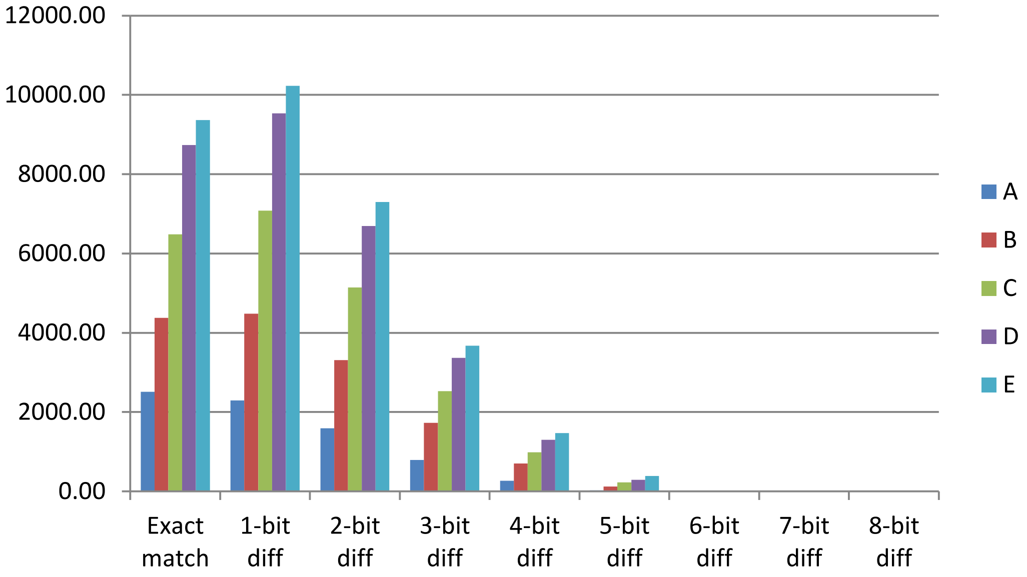


Figure 5.10: M2_8-bits, Number of matched and unmatched patterns

Table 5.6: M2_4-bits, Number of matched and unmatched patterns

Payload	Exact match	1-bit diff	2-bit diff	3-bit diff	4-bit diff	R. of match	R. of change
A	9692.64	2427.57	2625.53	209.48	20.79	0.860	0.140
B	19188.69	4927.61	5073.36	644.16	118.18	0.854	0.146
C	28410.39	7882.02	7504.68	1002.49	128.43	0.853	0.147
D	38481.65	10351.06	9535.04	1360.99	175.26	0.857	0.143
E	41958.81	11037.73	10245.10	1473.18	181.19	0.859	0.141

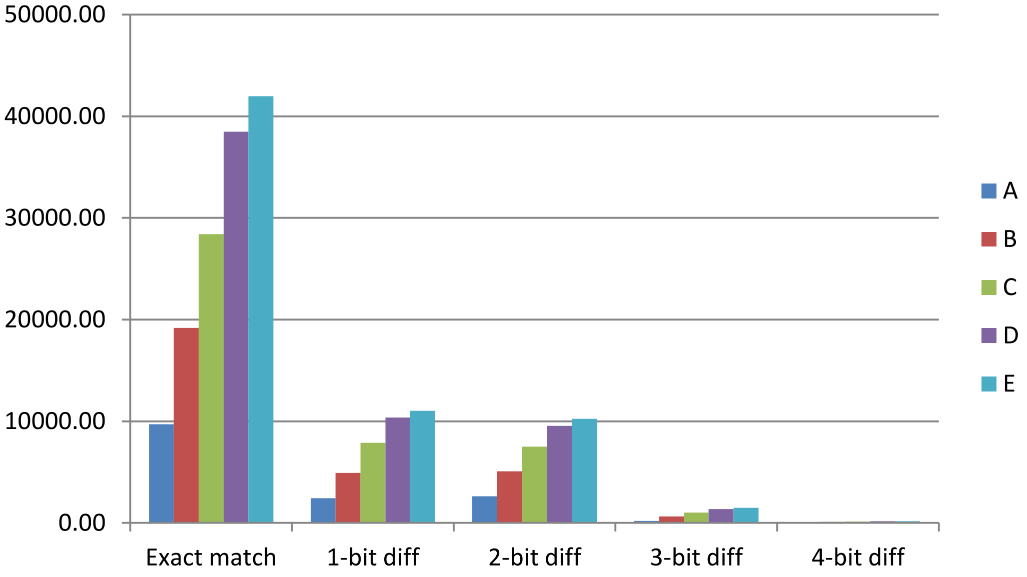


Figure 5.11: M2_4-bits, Number of matched and unmatched patterns

If we compare results obtained using method 1 and method 2 we notice a big enhancement regarding ratio of matching bits especially for using 8-bits patterns. Compared to results of method 1, the change ratio is reduced for the N_8 patterns to between 15.2% and 16.9%, and for the N_4 patterns to 14% to 14.7%. This success in improving the ratio of change in LSB plane, can be seen as a result of the change in embedding strategy between the two methods for embedding the UM set of patterns. Moreover, the distribution of the percentage of the UM set of unmatched secret patterns have changed into a negative exponential distribution over the hamming distances between them and the remaining patterns of the LSB-plane which is why we get the overall ratio of change decreases.

5.3.3 Method 3

Although the last method led to significant improvement regarding decreasing the ratio of change which contributes to smaller change and higher security, the choice of the blocks mapping was not given any serious consideration and the results are based on going for mapping sequentially according to their spatial positions. Noting that using a random mapping certainly improves the security of embedding significantly. In this method, the same procedure of method 2 is used, but we adopt a special block mapping that could possibly improve the change ratios as well as security. Instead of random mapping, we pair each face LBPH patterns block with the LSB-planes block that produces the best matching ratio. Admittedly this would increase the time complexity of the embedding in comparison to the sequential or the random (but unguided) mapping. Assume that we have m LSB cover block and n secret LBPH patterns blocks. Figure (5.12) shows the pseudo code of the mapping block algorithm. In this method the sender needs to inform the receiver the block sequence numbers to be used for extraction process (i.e. to guarantee extracting secret message in the right blocks).

Table 5.7 and figure 5.13 shows the number of matched patterns and unmatched patterns for all five different payloads. The unmatched patterns are arranged according to the hamming distances between LBPH patterns and their corresponding cover LSB patterns in case of using N_8 pattern, while table 5.8 and figure 5.14 shows the same analysis but for N_4 patterns. In both cases we calculate ratio of match and ratio of change after embedding. Again all results are the average results of using 1000 greyscale images as cover.

```
LET Match_Ratio be an nxm matrix of 0's
FOR i=1 to n
    FOR j=1 to m
        Embed the ith LBPH block, in the jth LSB cover image block,

      Match_Ratio(i,j)=(No of match pixels after embedding)/block size
    ENDFOR
ENDFOR
FOR k=1 to n
    Let r and p be the index (i,j) of maximum value in Match_Ratio matrix
    Embed the rth LBPH block in the pth LSB cover image block,
    FOR d=1 to m
         Match_Ratio(r,d) = 0
    ENDFOR
    FOR c=1 to n
        Match_Ratio(c,p) = 0
    ENDFOR
ENDFOR
```

Figure 5.12: Mapping best blocks pseudocode

Table 5.7: M3_8-bits, Number of matched and unmatched patterns

Payload	Exact match	1-bit diff	2-bits diff	3-bits diff	4-bits diff	5-bits diff	6-bits diff	7-bits diff	8-bits diff	R. of match	R. of change
A	2523.8	2317.5	1599.3	772.8	250.7	19.7	2.4	1.4	0.4	0.850	0.150
B	4703.2	4684.0	3349.0	1548.7	544.5	134.7	7.7	3.1	1.1	0.842	0.158
C	6557.2	7181.0	5157.8	2462.7	904.7	190.6	6.5	2.7	1.0	0.836	0.164
D	8856.1	9705.9	6739.9	3247.6	1161.9	228.0	8.1	3.2	1.2	0.838	0.162
E	9503.1	10433.3	7333.5	3526.4	1333.1	304.7	8.8	3.9	1.3	0.836	0.164

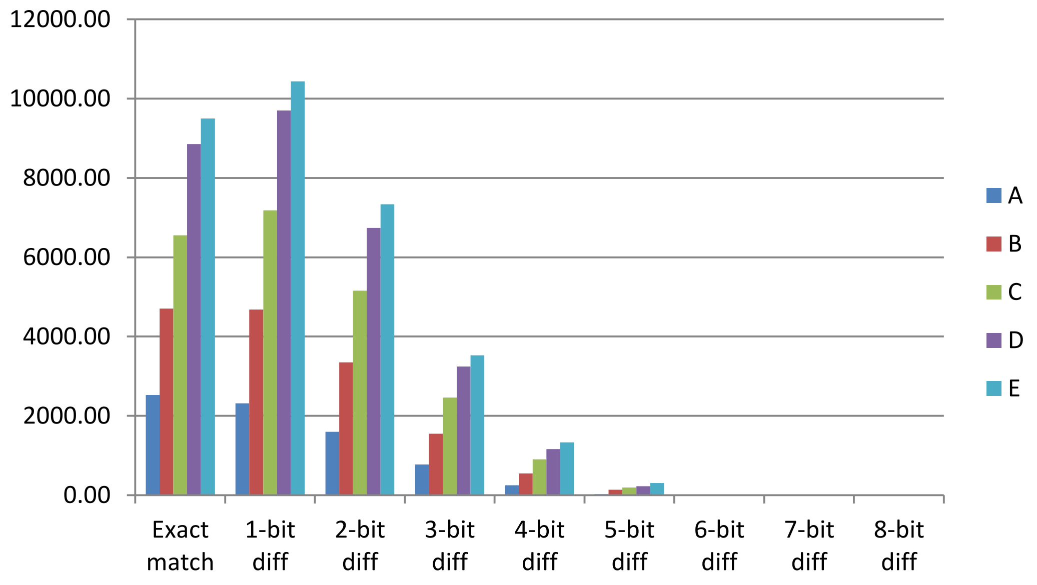


Figure 5.13: M3_8-bits, Number of matched and unmatched patterns

Table 5.8: M3_4-bits, Number of matched and unmatched patterns

Payload	Exact match	1-bit diff	2-bit diff	3-bit diff	4-bit diff	R. of match	R. of change
A	9751.44	2449.81	2612.83	153.69	8.24	0.864	0.136
B	19433.71	5004.54	5053.80	430.15	29.79	0.862	0.138
C	28726.27	7923.78	7574.53	670.34	33.08	0.860	0.140
D	38917.39	10588.50	9453.93	907.08	37.10	0.865	0.135
E	42497.90	11326.73	10081.44	955.24	34.70	0.867	0.133

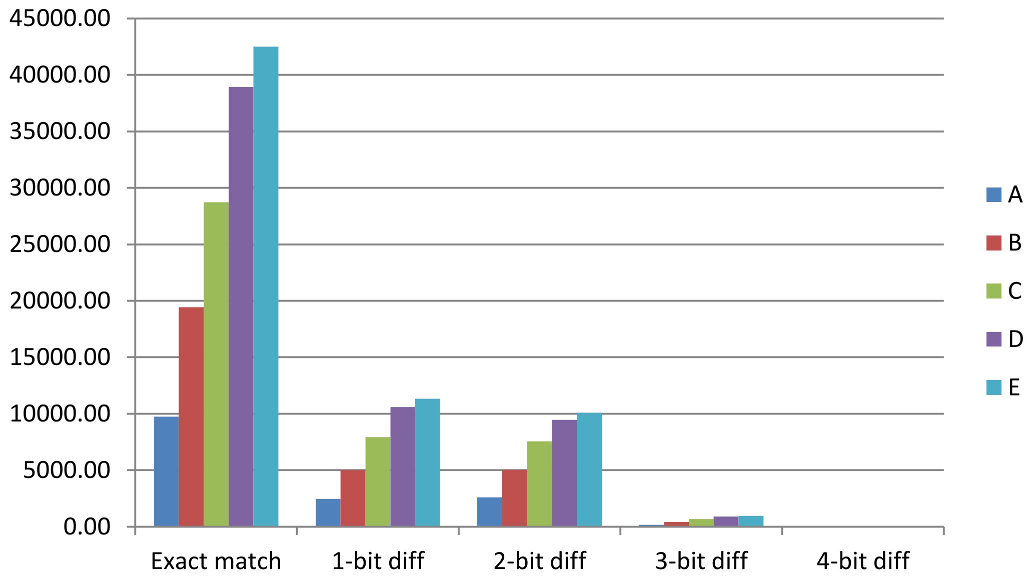


Figure 5.14: M3_4-bits, Number of matched and unmatched patterns

Like method 2, in this method the distribution of the percentage of the UM set of unmatched secret patterns remain in a negative exponential distribution over the hamming distances between secret face LBP blocks and the cover LSB blocks. Moreover, comparing results obtained using method 3 and method 2 we notice that overall a marginal around 0.005 for N_8 and 0.007 for N_4 enhancement was achieved in terms of matching ratio. However, the blocks mapping add an extra layer of the security. The increase in the level of security will be even more significant when the number of cover blocks is greater than the number of secret blocks.

5.4 Why Not Use Other Hiding Scheme for LBPH Patterns?

Reducing the probability of changes during embedding process at a given embedding payload leads to enhanced security. Designers of existing steganographic schemes have endeavoured to improve security and invisibility of their schemes but tested for general random secrets. For example, in Mielikainen (Mielikainen, 2006) modified the well-known least significant bit matching (LSBM) and demonstrated improved security by reducing change rate from 0.5 to 0.375. The question arises as to whether, hiding face LBPH patterns can lead to further improvement and outperform our content-based scheme. This section is an attempt to answer this question by comparing the performance of our content-based scheme in terms of change rate with various other relevant general schemes to hide face LBPH patterns. The comparisons here will be made between the ratios of change when the face LBPH are embedded in cover images using the traditional LSB (TLSB), LSBMR, and S-UNIWARD (see http://dde.binghamton.edu/download/stego_algorithms for the S-UNIWARD code).

We setup a set of new experiments, by (1) extracting LBPH patterns (both N_4 or N_8) from each face image in the Yale face database to be used as a secret message, (2) embedding each secret, using our scheme as well as the above schemes, in the same 1000 cover images obtained from the BOSSbase database that we used above, and (3) calculating change rate between obtained stego-image and cover image. In these experiments we use the same five different payloads that were used in section 5.3.

Table 5.9 and figure 5.15, displays the change rates achieved by each version of 3 implementation methods of our schemes with the 2 different pattern length (8-bits and 4-bits) followed by the rates for each of the 3 other schemes. All results showed here are average values of using 1000 greyscale cover images.

These results demonstrate that none of the existing schemes benefited from the structure of the face LBPH secrets in reducing the pixel change ratio below their known achieved rates for general secrets. Moreover all our schemes outperformed the TLSB and LSBMR schemes. The S-UNIWARD, which outperforms the existing TLSB and the LSBMR, only outperformed our M1 8-bits scheme which we attribute to the fact that M1 8-bits uses traditional LSB for embedding the unmatched patterns which total about 2/3 of the LSB bit-plane patterns and more than 60% of these patterns had hamming distances of 4 or more. In fact, the M1 8-bits scheme only marginally improves the ratio change in comparison to the LSBMR, perhaps for the same reason in the last statement. We notice that our two proposed schemes with 4-bit length patterns (M2 4-bits, and M3 4-bits) out perform all other schemes, the differences between methods with others become clearer with high payloads, while our other three proposed (M1 4-bits, M2 8-bits, and M3 8-bits) are comparable.

Table 5.9: Change rate with different payloads

Payload	M1 8-bit	M1 4-bit	M2 8-bit	M2 4-bit	M3 8-bit	M3 4-bit	TLSB	LSBMR (Mielikainen, 2006)	S-UNIWARD (Holub, et al., 2014)
A	0.0756	0.0384	0.0347	0.0320	0.0342	0.0312	0.1143	0.0857	0.0386
B	0.1570	0.0793	0.0755	0.0667	0.0723	0.0630	0.2250	0.1687	0.0887
C	0.2422	0.1215	0.1149	0.1008	0.1126	0.0962	0.3428	0.2557	0.1483
D	0.3217	0.1590	0.1519	0.1305	0.1480	0.1235	0.4571	0.3363	0.2191
E	0.3500	0.1705	0.1670	0.1399	0.1626	0.1316	0.4951	0.3596	0.2458

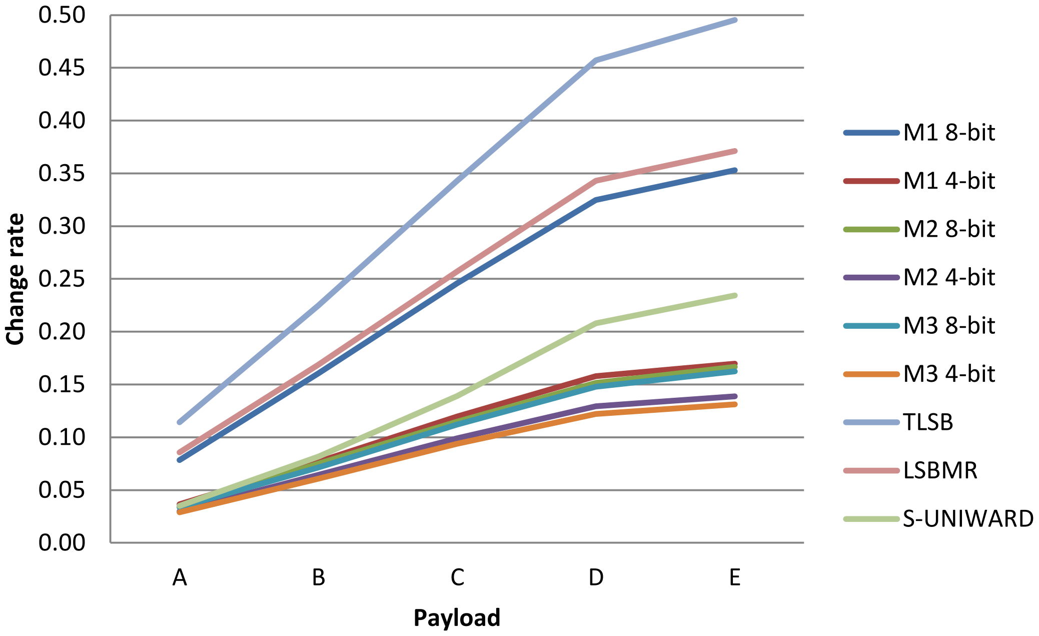


Figure 5.15: Change rate with different payloads

5.5 Conclusions

In this chapter we focused our investigations on the more recent recommendations by leading researcher in the steganography community on the need to moving the steganography aspect from the laboratory condition (theory) into the real world applications. Accordingly we investigated the optimality concept of steganographic schemes which is linked to minimizing distortion of the cover image (consequently maximizing invisibility of embedded secrets) by reducing the change rate while maintain the required payload. Taking into account our specific aim of embedding biometric feature vectors in images for secure remote authentication, we considered the optimality concept in the specific context of content-based steganography by exploiting the knowledge of the structure of the secret message as well as the application objectives in designing optimally efficient hiding schemes. More specifically we designed and tested the optimality of a content-based hiding scheme that aims to embed a human face LBPH patterns into the LSB bit-plane of a natural image. The proposed block based scheme attempts to minimize changes in each image block by aligning the 4 or 8 bits face LBPH patterns with the LSB patterns extracted from 4 or 8 pixels of the cover-image according to ascending order of search hamming distances between the pairs patterns. This "best match" alignment strategy ensures that the changes are minimal for each pair of face and cover images. The embedding first skips all 4 or 8 pixel patterns whose LSBs exactly match the LBPH patterns, then embed the LBPH codes of the set remaining codes (UM) sequentially into the remaining cover block LSB bit strings by embedding the subsets of UM codes that have hamming distance 1 with their aligned LSB patterns followed by those of Hamming distance 2, and so on until all is embedded. The fact that face recognition is based on histogram dissimilarity removes the need for remembering order of pixels into which the secret was embedded.

We analysed and evaluated the proposed schemes for calculating change rate for different payloads by embedding LBPH codes for each of the face images in a sufficiently large benchmark face images database into a 1000 cover images of different texture and captured with 8 different cameras. The computed change ratios for this experiment have demonstrated the optimality of the proposed scheme in terms of change ratios. These experiments revealed that significant percentage of matched patterns have been found between the various cover images and the secret messages but in different positions. In fact, on average 83% to 85% of LSB bits match the N_8 patterns (i.e. the probability of changing the cover LSB is 15% to 17%), while 85% to 87 % of LSB bits matched the N_4 patterns (i.e. the probability of changing the cover LSB is 13% to 15% only). Moreover, in terms of pixel value change rate after hiding, this example of a content-based steganography scheme improves the lower bound on optimality ratio of 24% achieved by the state of the art scheme named S-UNIWARD.

Furthermore, we have demonstrated that using existing embedding schemes in hiding LBPH patterns are all outperformed significantly by most of our scheme in terms of change ratios. This is another incentive to recommend the use of content-based steganography.

The proposed content-based steganography scheme differentiates between hiding biometric features and hiding any other secret message (text, image, etc). Therefore, we do not make any claim on the optimality of our scheme except as a content-based embedding. In fact we cannot guarantee the achievement of such excellent lower bounds of change ratio for other types of content-based hiding schemes.

In the next chapter, we shall complement this chapter’s work by investigating the robustness of our content-based scheme against existing targeted as well as Universal steganalysis tools.

Chapter 6
Robustness of the Content-Based Steganography

This chapter continue the investigations into the performance testing of the Content-Based Steganography scheme proposed, in the previous chapter, for embedding face LBPH patterns. Here we are primarily concerned with robustness against steganalysis attacks by targeted as well as universal tools. In particular we shall demonstrate in section 6.1 that our schemes are robust against the 3 most commonly used targeted steganalysers (DIH, RWS, and the calibrated HCF-COM). Expectedly, the SRM does detect the present of our schemes payloads. We shall demonstrate the strength of our scheme by comparing the robustness with 3 existing steganographic schemes when the face LBP features are embedded. In section 6.2 we shall modify our scheme by embedding in selected position but not exactly as done by S-UNIWARD scheme. This modification will be shown to improve performance against the SRM. In section 6.3 we will discuss the stego-image quality of our content-based embedding.

6.1 Strength of Proposed Content-based Steganographic Scheme

We already established that our content-based embedding scheme achieves optimal lower bound of image pixel value change ratio compared to the state of art schemes. Here, we will further discuss the strength of the scheme in terms of robustness against various steganalysers.

The statistical changes that occur in the structure of the cover image after embedding certain amount of secret message may become detectable by steganalysis tools that designed to locate the statistical changes. Our content-based embedding scheme is an LSB-based, therefore we first test its robustness against two well-known targeted steganalysis: the different image histogram (DIH) (Zhang & Ping, 2003) and the revisited weighted stego-image steganalysis (RWS) (Ker & Böhme, 2008). Although our content-based embedding scheme is not based on the LSBM idea but for the purpose of comparison we test its robustness against the calibrated HCF-COM (Ker,

2005) tool that designed specifically for this purpose. Moreover, we shall also test the robustness of our scheme against the universal steganalysis tool named spatial rich models (SRM) that was developed by Jessica Fridrich et al. (Fridrich & Kodovský, 2012), to detect hiding secrets in the spatial or JPEG domain.

The robustness testing of our scheme against above mentioned steganalysis tools will be conducted after embedding the two LBPH pattern versions (i.e. N4 and N8). For the experimental testing we extract both LBPH patterns from each face image in the Yale face database, and embed separately in the same 1000 cover images obtained from the BOSSbase database used in previous chapter. In these experiments we use four different payload capacities 0.1, 0.3, 0.5 and 1. In all cases we use the content-based method 2 scheme and we compare its performance with three different embedding schemes TLSB, LSBM, and S-UNIWARD. In the case of theses 3 benchmark schemes we also embed the same LBPH patterns separately. In fact we are not include the two embedding schemes (LSBM and S-UNIWARD) in the first two steganalysis schemes (DIH and RWS), the reason is that mentioned embedding schemes are based on LSBM embedding strategy, while DIH and RWS steganalysis tools are just designed to detect embedding schemes based on traditional LSB embedding. Therefore robustness of the two embedding schemes (LSBM and S-UNIWARD) compared with our proposed embedding scheme are tested against other two steganalysis tools HCF-COM and SRM. The following subsections show the results obtained after applying corresponding steganalysis tool. In each case we shall briefly review the steganalysis tool.

6.1.1 Robustness against Difference Image Histogram (DIH)

Tao Zhang and Xijian Ping (Zhang & Ping, 2003), proposed the use of the difference image histogram (DIH) method as a classifier for distinguishing between stego-images and cover images. The DIH is designed to detect stego-images obtained by LSB embedding schemes. It uses the measure of weak correlation between the LSB plane and other bit-planes of the image as a result of randomness of the LSB in natural images. The difference image is defined as:

$$D(i,j) = I(i,j) - I(i,j+1) \tag{6.1}$$

Where $I(i,j)$ denotes the value of the image I at the position(i,j). In general the coefficient $D(i,j)$ of the difference image D follows a generalized Gaussian distribution. T.Zhang and X.Ping found that there exists differences between the difference image histograms (DIH) for normal cover image and images obtained after flipping some of the bits of LSB-plane as a result of embedding a secret in a natural image LSB. This fact is utilized to realize the steganalysis technique. Moreover, the scheme models a function to estimate the ratio of embedding as well, i.e. DIH technique not only decides whether the images are stego or not but also obtain embedded message ratio. The DIH tool can be summarized as follows:

Given a test image I, the difference image histogram of I is represented by hi. After flipping all bits of the LSB bits of I, it re-calculate the difference image histogram fi, and create another image by setting all the LSB bits of I to zero and let gi be the DIH of the new image. Based on the relationship between these three differences images histograms, to decide whether the tested image is cover or it is stego. The relationships are defined by a translation scheme between the 3 histograms (hi, fi , and gi) as follows:

$$h_{2i} = a_{2i,2i}g_{2i}, \tag{6.2}$$

$$h_{2i+1} = a_{2i,2i+1}g_{2i} + a_{2(i+1),2i+1}g_{2(i+1)}, \tag{6.3}$$

$$f_{2i+1} = a_{2i,2i-1}g_{2i} + a_{2(i+1),2(i+1)+1}g_{2(i+1)}. \tag{6.4}$$

Where, $a_{2i,2i+j}$ defined as translation coefficient from the histogram gi to hi , and $0 < a_{2i,2i+j} < 1$, for $= 0, 1, -1$, otherwise $a_{2i,2i+j} = 0$, the translation coefficients are assumed to satisfy:

$$a_{2i,2i-1} + a_{2i,2i} + a_{2i,2i+1)} = 1 \tag{6.5}$$

From the symmetry about i=0 of the difference histogram, we get $a_{0,1} \cong a_{0,-1}$. Combining with equations from 6.2 to 6.5, we obtain iterative formula for calculating translation coefficients for all positive i as follows:

$$a_{0,1} = a_{0,-1} = \frac{g_0 - h_0}{2g_0}, \tag{6.6}$$

$$a_{2i,2i} = \frac{h_{2i}}{g_{2i}}, \tag{6.7}$$

$$a_{2i,2i-1} = \frac{h_{2i-1} - a_{2(i-1),2i-1}g_{2(i-1)}}{g_{2i}}, \tag{6.8}$$

$$a_{2i,2i+1} = 1 - a_{2i,2i} - a_{2i,2i-1} . \tag{6.9}$$

The tool then calculates:

$\alpha_i = (a_{2(i+1),2i+1})/(a_{2i,2i+1}), \beta_i = (a_{2(i+1),2(i+1)+1})/(a_{2i,2i-1}), \gamma_i = g_{2i}/g_{2(i+1}.$

It has been shown experimentally that for a given i the value of α_i decreases with the increased secret length, and when the embedding ratio p increases to 100%, α_i approaches 1. The statistical hypothesis of the DIH tool is that for a natural image $\alpha_i = \gamma_i$.

Otherwise, the embedding ratio p is determined by the root of smallest absolute value of a quadratic equation in p whose coefficients are dependent on α_i, β_i, and γ_i. For more details see (Zhang & Ping, 2003).

Figure 6.1 shows the results of applying DIH steganalysis tool on our embedding schemes as well as LSB embedding scheme. The experiments conducted as follows: after LBPH patterns (N4 or N8) are extracted from all faces in the Yale database, the extracted LBPH patterns then embedded using our two proposed embedding (N4 or N8) matching scheme into the 1000 images from the BOSSbase database used in previous chapter. For LSB embedding, we extracted features from the Yale database using N8 LBP scheme and embed the extracted features bit by bit using LSB embedding scheme. Furthermore, to see the robustness of the proposed embedding schemes against DIH steganalysis tool in different payload capacities, we use four different payload capacities 0.1, 0.3, 0.5 and 1. The figure displays on the y-axis the estimates of embedding ratio against different payload capacities (x-axis), proposed schemes compared with TLSB embedding scheme. Comparison with other schemes (LSBM and S-UNIWARD) is not relevant because DIH only detects LSB based schemes. We also tested the original cover image with the steganalysis to see how our embedding scheme far from original covers images.

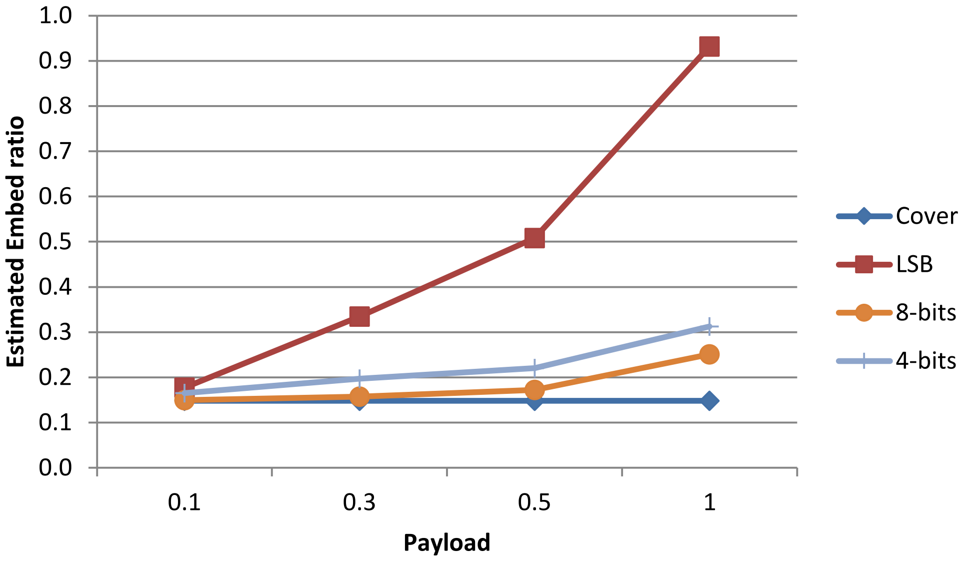


Figure 6.1: Estimation of embedding ratio using DIH

The results demonstrate the robustness of both LBPH pattern lengths (4 and 8) against the DIH steganalysis, because the estimated embedding ratio (especially for the N_8) is not much different than that of natural images until reaching full capacity embedding. Even at the 100% embedding ratio, for our proposed steganographic schemes, the DIH estimate the embedding ratio to be 0.25 and 0.31 for 8-bits and 4-bits patterns, respectively. Note that for natural cover images DIH wrongly estimates the ratio to 0.15. While for TLSB embedding the DIH steganalysis very accurate estimate embedding ratio even for a very small payloads. From the results we also conclude that using 8-bits pattern have better robustness against DIH steganalysis tool.

6.1.2 Robustness against the Revisiting Weighted Steganalysis (RWS)

The RWS steganalysis tool, proposed by Andrew Ker (Ker & Böhme, 2008), is an enhanced version of the scheme that originally proposed by Fridrich and Goljan's (Fridrich & Goljan, 2004). Currently RWS is reported to be one of the best structural steganalysis and most sensitive targeted steganalysis of LSB based steganography since it does not require any training phase and keeps the detection accuracy high (Kodovský & Fridrich, 2013). Like the DIH, RWS not only decides whether the image is cover or stego but also estimate the length of the embedded message by giving the percentage of pixels which may hold data. For the above up mentioned points we choose RWS to see the robustness of our content-based scheme. The technique considers that a proportion of $\mathrm{M}/2\mathrm{N}$ of the cover pixels are flipped when embedding a payload of length M bits, and N is the cover image size. The technique work as follows:

1- Given a test image $I = (i_1, i_2, i_3, \ldots\ldots, i_N)$, and let $\overline{I} = (\bar{i}_1, \bar{i}_2, \bar{i}_3, \ldots\ldots, \bar{i}_N)$ be the image obtained from I after flipping the LSB bits

2- In steganalysis we do not have access to the original cover image, in RWS method the original cover $\hat{C}$ will be predicted by filtering test image I. Filtering I done using a filter that minimize difference between I and $\hat{C}$. The filters are Gaussian-like weighted linear such as:

$$\begin{matrix} 0 & \frac{1}{4} & 0 \\ \frac{1}{4} & 0 & \frac{1}{4} \\ 0 & \frac{1}{4} & 0 \end{matrix} \quad (1) \qquad \begin{matrix} \frac{1}{8} & \frac{1}{8} & \frac{1}{8} \\ \frac{1}{8} & 0 & \frac{1}{8} \\ \frac{1}{8} & \frac{1}{8} & \frac{1}{8} \end{matrix} \quad (2) \qquad \begin{matrix} \frac{-1}{4} & \frac{1}{2} & \frac{-1}{4} \\ \frac{1}{2} & 0 & \frac{1}{2} \\ \frac{-1}{4} & \frac{1}{2} & \frac{-1}{4} \end{matrix} \quad (3)$$

$$\begin{matrix} b & a & b \\ a & 0 & a \\ b & a & b \end{matrix} \quad (4) \qquad \begin{matrix} e & d & c & d & e \\ d & b & a & b & d \\ c & a & 0 & a & c \\ d & b & a & b & d \\ e & d & c & d & e \end{matrix} \quad (5)$$

The weight values that minimize distance between stego and cover image will improves the detector accuracy. In the proposed scheme the weights assigned experimentally as:

$$w_j = \frac{1}{5 + \sigma_j^2} \qquad (6.10)$$

Where, σ_j^2 is the local variance of the stego pixels neighboring in i_j.

To quantify flat pixel bias correction, authors imagine that it is the stego image is fixed and the cover which was generated by randomly flipping proportion p/2 of LSBs. Then the expected flat pixel bias correction is computed using following formula:

$$r = -p \sum_{j=1}^{j=N} w_j (i_j - \bar{i}_j)\,(F * (\bar{i} - i))_j \qquad (6.11)$$

Finally the proportionate payload length $p = \mathrm{M}/\mathrm{N}$ is estimated by calculating the following formula:

$$\hat{p} = r + 2argmin \sum_{j=1}^{j=N} w_j(i_j^{\alpha} - \hat{c}_j)^2 = r + \frac{2}{N} \sum_{j=1}^{j=N} w_j\,(i_j - \hat{c}_j)(i_j - \bar{i}_j) \qquad (6.12)$$

To test robustness of our embedding schemes for the different LBPH patterns (N4 or N8) against RWS steganalysis tool, we repeat the same experiment conducted to test DIH steganalysis tool by first extracting LBPH patterns from all faces in the Yale database, then the extracted LBPH patterns are embedded using our two proposed embedding (N4 or N8) matching scheme into the 1000 images from the BOSSbase database. Again for LSB embedding, we extracted features from the Yale database using N8 LBP scheme and embed the extracted features bit by bit using LSB embedding scheme. Moreover, we use four different payload capacities 0.1, 0.3, 0.5 and 1 to test the robustness. Figure 6.2 show estimation of change rate (y-axis) using RWS steganalysis of our schemes compared with TLSB as well as the natural cover images in four different payload capacities (x-axis). Again comparison with other schemes (LSBM and S-UNIWARD) is not relevant because RWS only detects LSB based schemes.

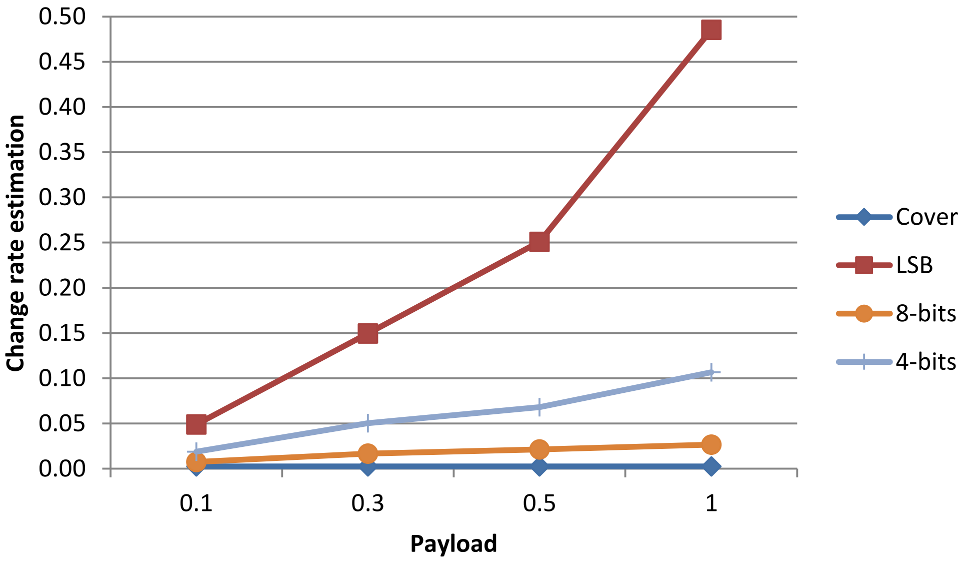


Figure 6.2: Estimation of change rate using RWS steganalysis

The results demonstrate the robustness of both LBPH pattern lengths (4 and 8) against the RWS steganalysis, because the estimated change ratio (especially for the N_8) is very near to that of natural images until reaching full capacity embedding. In fact the pattern of the results is similar to those obtained from the DIH testing. Table 6.1 below, shows the mean and standard deviations of obtained estimated change ratio for our content-based scheme with 8-bits pattern as well as the original cover images.

Table 6.1: Mean and standard deviation of content-based with N_8

Payload	0 (cover)	0.1	0.3	0.5	1
Mean	0.002	0.007	0.017	0.021	0.027
Std.	0.007	0.009	0.013	0.013	0.010

Consideration of the standard deviation of the estimated ratios for each payload, reveal that the RWS response for large number of images could be missed by RWS as being a natural image. Note that in all cases the standard deviation values are relative high compared to the corresponding means. In fact, these statistics indicate that there noticeable number of stego images with 0.3 payload that are would return values within ½ standard deviation of the mean of the natural images. Even for the 100% embedding ratio, for our proposed steganographic schemes, the RWS estimate the change ratio to be 0.027 (i.e. estimated embedding payload is about 5.4%) and 0.107 (i.e. estimated embedding payload is about 21.4%) for 8-bits and 4-bits patterns, respectively. On the other hand, for TLSB embedding the RWS steganalysis estimate correctly the change ratio even for a very small payload.

6.1.3 Robustness against the LSBM Steganalysis

Harmsen and Pearlman (Harmsen & Pearlman, 2003) showed that embedding technique works as a low-pass filter on the histogram of the cover image; this means that the histogram of the stego-image contains fewer number of high-frequency components compared with the histogram of its cover version. By exploiting this property, the authors introduced a detector using the centre of mass (COM) of the histogram characteristic function (HCF) and they named HCF-COM. That work was tested on colour images, but is not applicable to greyscale images. In (Ker, 2005) Andrew Ker showed and proved that the original HCF-COM method does not work well on grayscale images. Therefore, Ker proposed a new version of HCF-COM based on the calibration (down-sampling) technique which applicable on greyscale images. The proposed work as follows:

1- Let I be a greyscale image that need to be tested, and h be the histogram of I. The histogram characteristic function (HCF) of I is defined as the Discrete Fourier Transform (DFT) $\widehat{h}$ of h.

2- The Centre of mass of the HCF (HCF-COM) is defined as :

$$C(I) = \frac{\sum_{k=0}^{N/2} k \left|\hat{h}(k)\right|}{\sum_{k=0}^{N/2}\left|\hat{h}(k)\right|} \qquad (N = 256) \tag{6.13}$$

3- Let $\hat{I}$ be a down-sampled version image of I by factor 2 in both dimensions:

$$\hat{I}(i,j) = \left\lfloor \sum_{u=0}^{1} \sum_{v=0}^{1} \frac{I(2i+u, 2j+v)}{4} \right\rfloor \tag{6.14}$$

4- Compute the HCF-COM for $\hat{I}$ and noted it by $C(\widehat{I})$.

The proposed steganalysis tool is based on the fact that for natural images the 2 calculated HCF-COMs (before and after down-sampling) are approximately equal (i.e. $C(I) \approx C(\hat{I})$). On the other hand, although the embedding process does introduce the noise into the down-sampled image, nevertheless it reduce the value of HCF-COM, but to a lesser extent than in full-sized image (i.e. $C(I) < C(\hat{I})$ in most stego images).

Although our embedding scheme is not based on LSBM idea, but to see how our content-based scheme robust against specific LSBM steganalysis tools, we repeated the same experiment above on our embedding scheme for the different LBPH patterns. Results obtained are compared with other embedding schemes such as TLSB, LSBM and S-UNIWARD. Figure 6.3 shows the probability of detection for different payload capacities for tested schemes as well as for original cover images. In the latest two embedding schemes (LSBM and S-UNIWARD), the strategies of embedding are based on the least significant bit matching idea and the mentioned steganalysis is designed to catch such kind of embedding strategies.

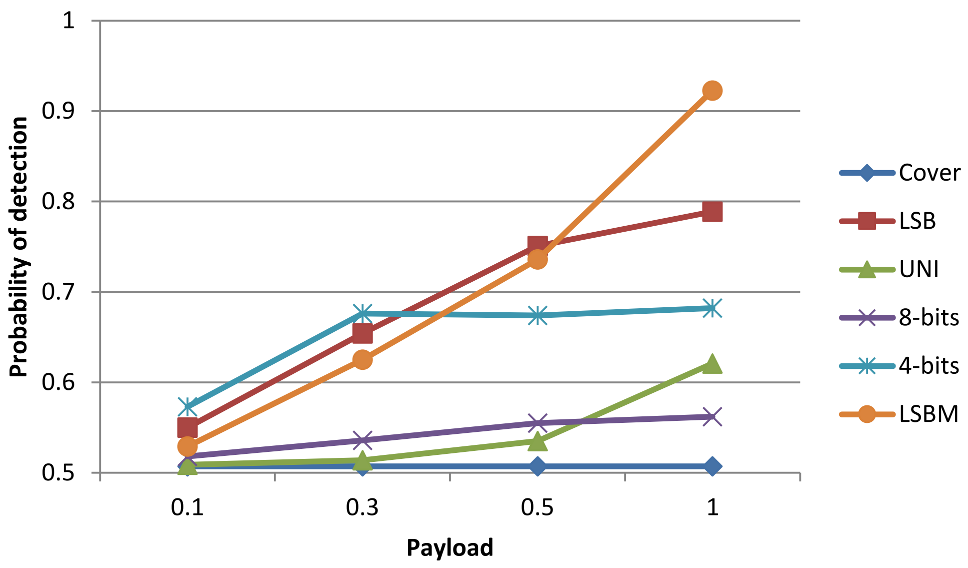


Figure 6.3: Probability of detection using steganalysis proposed in (Ker, 2005)

From these results it is clear that the LSBM is defeated by this tool especially when payload is high, for example the probability of detection is about 92% (i.e. the error rate is only around 8%) in case of full payload capacity while this error rate is around 22% of using TLSB. On the other hand, the S-UNIWARD is robust against this steganalysis technique at low payload, but for fully embedding payload the reported error rate is only 38% (i.e. 62% of cases are correctly classified as stego-images). As we mention before although our embedding schemes is not based on LSBM idea but at full payload the N_8 scheme is more robust against this tool than the S-UNIWARD with an error rate of 43.8% (i.e. 56.2% of cases are correctly classified as stego-images) . For our N_4 scheme, the error rate remains around 33% for all payloads >= 0.3.

6.1.4 Robustness against the SRM Steganalysis

This is the most powerful universal steganalysis tool that is designed to detect the presence of hidden secrets in spatial domain as well as JPEG images. It is called the spatial rich models (SRM) and was proposed by Jessica Fridrich et al. (Fridrich & Kodovský, 2012). It is primarily used by steganographers to test robustness of their embedding scheme and have to provide their algorithms. This tool is based on computing a very large number of different types of dependencies among neighbouring pixels (also referred to as distortion features) to enable the detection of a wide range of embedding algorithms on the bases of the fact that any embedding scheme will create few local distortions at different scales. The dependencies are modelled as noise residuals.

1- Let I_{ij} be the pixel located at position (i,j) of the test image I, N_{ij} be a local neighborhood of pixel I_{ij} , $\theta(N_{ij})$ be a predictor of I_{ij} defined on N_{ij}, the noise residuals R computed using the following form:

$$R_{ij} = \theta\left(N_{ij}\right) - I_{ij} \tag{6.15}$$

Different pixel predictors are implemented as locally supported linear filters and can be expressed as the convolutions of *I* and a kernel matrix. A total of 39 kernels are used. For example, the two kernels:

$$K_3 = \frac{1}{4}\begin{pmatrix} -1 & 2 & -1 \\ 2 & 0 & 2 \\ -1 & 2 & -1 \end{pmatrix}$$

$$K_5 = \frac{1}{12}\begin{pmatrix} -1 & 2 & -2 & 2 & 1 \\ 2 & -6 & 8 & -6 & 2 \\ -2 & 8 & 0 & 8 & -2 \\ 2 & -6 & 8 & -6 & 2 \\ -1 & 2 & -2 & 2 & -1 \end{pmatrix}$$

Other kernels involve pixels arranged only in horizontal or vertical direction and derived from constant, linear and quadratic models of local image block.

2- Different quantized and truncated versions of each residual are calculated:

$$R_{ij} \leftarrow trunc_T\left(round\left(\frac{R_{ij}}{q}\right)\right) \tag{6.16}$$

Where, T is a truncation threshold and q is a quantization step.

3- After the quantized residuals are obtained, the SRM submodels will be constructed from their horizontal and vertical 4th order co-occurrences. The 4th order horizontal and vertical co-occurrence matrix of residual R_{ij} is defined as the normalized number of the groups of four neighboring residual samples (d1, d2, d3, d4). Some post procedures are followed by leveraging symmetries of natural images. When all the resulting submodels are put together, their combined dimensionality is 34671 features. (for detail see in (Fridrich & Kodovský, 2012))

4- Due to very large dimensionality of the features, its classification process is done using an ensemble classifier machine learning tool which consists of number of base learners. Each base learner is trained on a set of cover images together with stego images obtained by embedding different payload with a variety of hiding schemes. The ensemble reaches its decision by fusing all individual decisions obtained from each base learners using majority voting. The accuracy of the system is evaluated using the ensemble's estimate of the testing error known as the 'out-of-bag' error (EOOB). (for detail see in (Kodovský, et al., 2012)) Matlab codes for SRM steganalysis feature extractor as well as the ensemble classifier are downloaded from the (http://dde.binghamton.edu/download/) website.

To test the robustness of our embedding scheme for the different LBPH patterns (4-bits and 8-bits) compared with TLSB, MLSB, and S-UNIWARD we conduct experiments as follows: we embedding the LBPH patterns in the 1000 images from BOSSbase database, then train the SRM with 500 of the obtained stego-images together with their cover versions while remain 500 images are used for testing. Figure 6.4 shows obtained EOOB of tested schemes over different payload capacities.

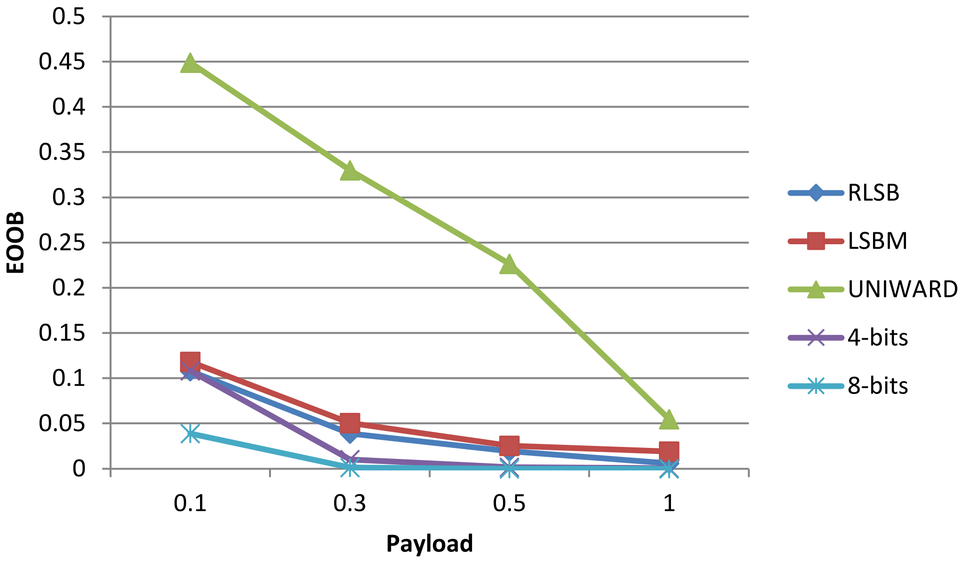


Figure 6.4: Detection error of Out-of-Bag (EOOB) using SRM steganalysis.

From the results we notice that our proposed embedding schemes as well as TLSB and MLSB are not robust against this kind of steganalysis if compared with the S-UNIWARD embedding scheme. However, the S-UNIWARD will lose its robustness after a specific (0.4) payloads embedded (Holub, et al., 2014).

Further analysis of these results require an understanding of the way the S-UNIWARD embedding technique works to enable it avoiding detection at low embedding rates. The S-UNIWARD embedding technique was specially designed to find the best locations for embedding in terms of a special distortion function and then embed only in those positions for which less distortion can be detected. Our proposed method, on the other hand, embeds the secret everywhere without consideration of impact on local features. In the next section, we shall modify our content-based scheme by embedding in selected locations and test robustness against SRM.

6.2 Enhanced Content-based Steganography Scheme

The S-UNIWARD embedding technique was specifically designed to withstand SRM steganalysis and to some extent it is successful at low embedding rates only. Our intended application of embedding LBPH pattern of face images for remote authentication, the embedding rate is particularly low due to the small size of the LBPH secret. In the above experiments we were embedding multiple copies for the same or different faces to enable comparison of robustness with other embedding schemes at different payloads. Therefore, in practice there is no need to embed the LBPH secret everywhere in the cover image.

To attempt improving the robustness of our content-based hiding scheme in general but more importantly against SRM at low embedding rate, we use a similar strategy to that used by S-UNIWARD and incorporate a position selection process into our content-based schemes. From the literature review, we learnt that hiding in the “noisy areas” of cover images such as edges and textures are less detectible than embedding in smooth areas. However, we also learnt that when secret bits are embedded in edge positions, these edge pixels may not remain as such, i.e. the act of embedding changes the list of edge pixels. If this is to happen then we cannot guarantee the exact extraction of the secret message in the receiver side. To guarantee the availability for embedding of the same number and positions of edges in a cover image, Kathryn Hempstalk (Hempstalk, 2006) proposed a method which calculates and determines the edge pixels positions using the r most significant bit of the pixel, while embedding is advised to be made in the t least significant bits where $r = 8 - t$, (here we are assuming that cover images are 256 greyscale images). Doing so enables the retrieval of the secret bits from the same pixels that used for embedding because the bits used in finding edges are not changed during embedding process. Authors of (Hempstalk, 2006) called this process of excluding t bit-plane from edge detection process as the FilterFirst process.

Here we use a modified version of the FilterFirst idea in order that the LSB plane is used for the embedding purpose and other bit-planes for edge detection. The number of pixels labelled as edge positions is different from one image to another, and it depends on the structure of the image content or texture. Hence, we employ adaptive labelling of edges pixels, by using a threshold for finding edge positions that depends on the length of the secret. This adaptive approach assigns greater values for the threshold parameter to get less number of edges while smaller threshold values results higher number of edges. Figure 6.5 shows the relation between number of edge pixels and threshold values. Threshold values are real numbers between 0 and 1, and the results are the average calculated when we tested the same 1000 cover images that we used before in all experiments.

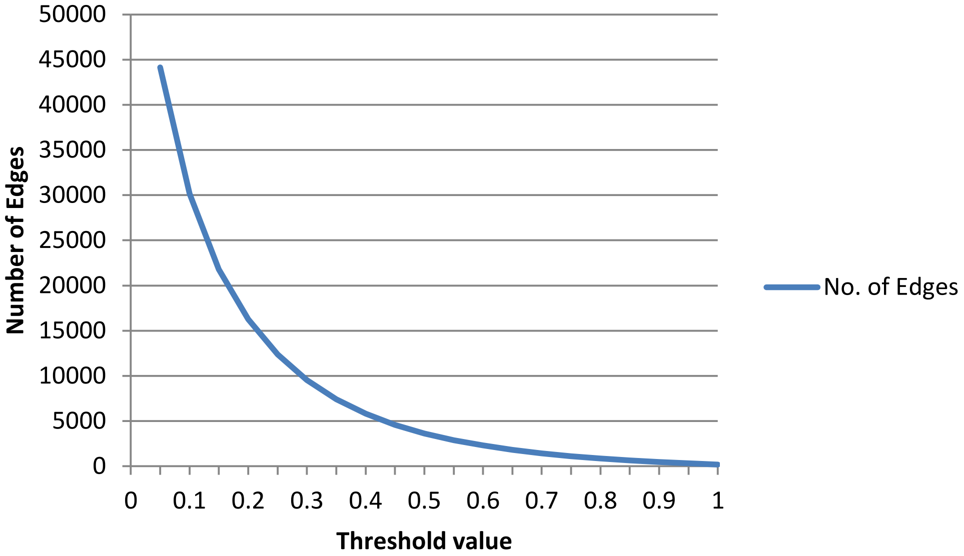
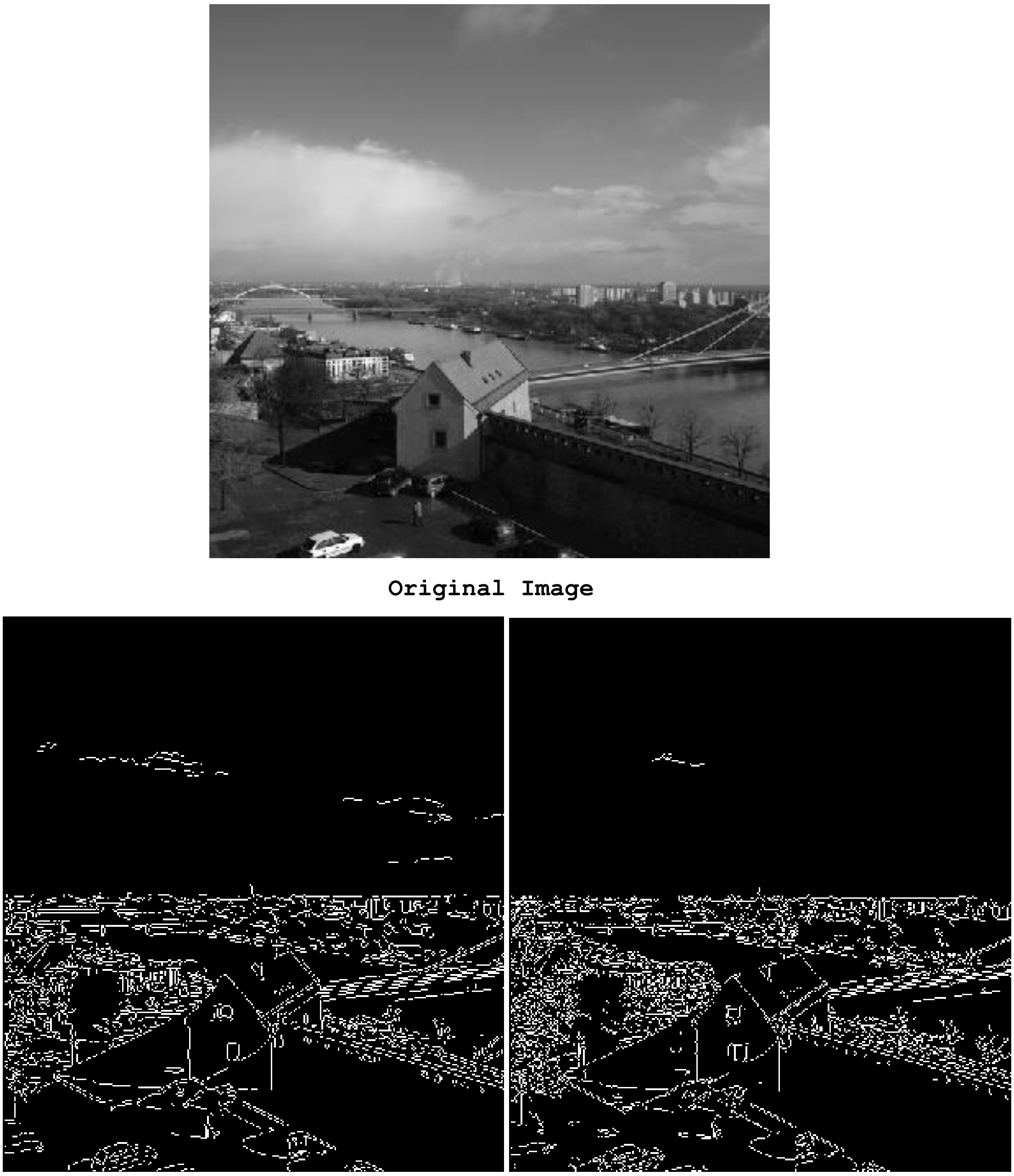


Figure 6.5: **Relation between edge numbers and threshold value**

By doing so we choose for each image a different threshold (i.e. will be selected adaptively depending on how textured the cover image is), this threshold value can be used as a key shared between sender and receiver.

To achieve higher number of edges we used “canny” edge detector. Edge are defined to be clean are edges in less densely textured regions, which are not suitable for embedding. Edge cleanness can be determined by the “sigma” parameter of the “canny” edge detector. Assigning small values to “sigma” helps avoid clean edges, but increase the number of selected pixel positions in dense regions. See figure 6.6 as an example to differentiate between using low and high value of sigma parameter for detecting edge positions using canny edge detector with the same threshold value. Again this sigma value can be used as a key shared between sender and receiver before any session of communication.



Original Image

```
can = edge(Cover,'canny',0.1,0.8);      can = edge(Cover,'canny',0.1,0.2);
```

Figure 6.6: Effect of the sigma value to detect edge positions

Furthermore, assigning small value to ‘sigma’ parameter for the same threshold value, will gave larger number of edges especially when small value of threshold used for detecting edge areas. See figure 6.7 which explain number of edges detected using different value of threshold with using two different ‘sigma’ values 0.2 and 0.8. From the figure we can conclude that assigning low value to ‘sigma’ parameter not only mark pixels as an edge position in dense area but also will increase number of pixels that marked as edge positions.

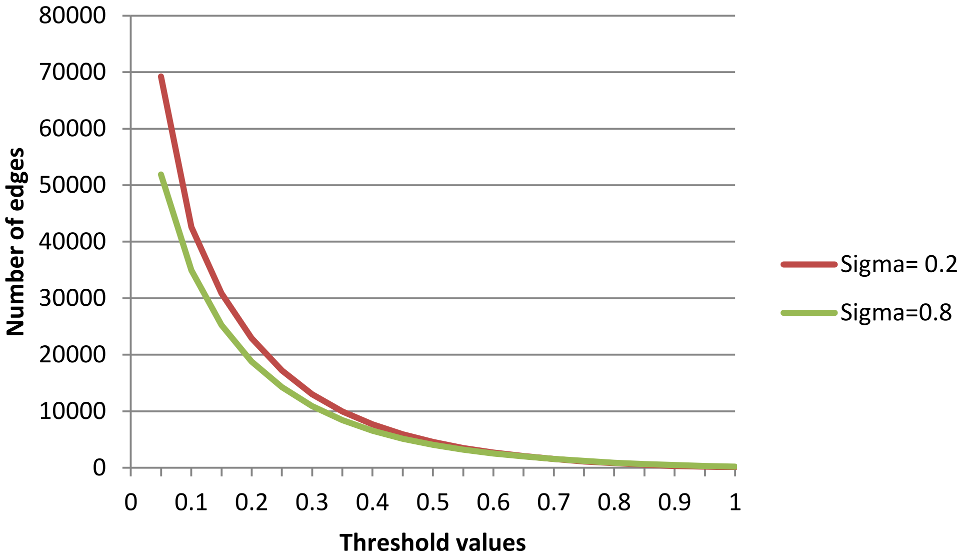


Figure 6.7: Edge numbers vs. 'Sigma' value

To evaluate the new proposed content-based we use three low payload capacities which they are 0.05, 0.1, and 0.2. These payloads are sufficient for embedding both LBPH patterns extracted from a single face image. For larger than these payload we need to exclude significant number of images in the experimental BossBase image set because we cannot guarantee enough number of edges even when we assign smallest value to the threshold parameter during finding edge positions, e.g. payload 0.3 cannot be achieved by 135 images out of the 1000 used (i.e. not having enough number of edges). For an image to pass this test, it is not necessary to have the image edges distributed uniformly over different blocks or regions. Therefore, in these experiments we must use the cover image as one block and this would mean that the secret LBP code are also extracted from the secret image without dividing into blocks.

Figure 6.8 shows EOOB of our new proposed position selection based technique fused with previously proposed content-based scheme M2 with different pattern sizes (4-bit and 8-bits), for simplicity we named FF_4 and FF_8 respectively, results are compared with S-UNIWARD.

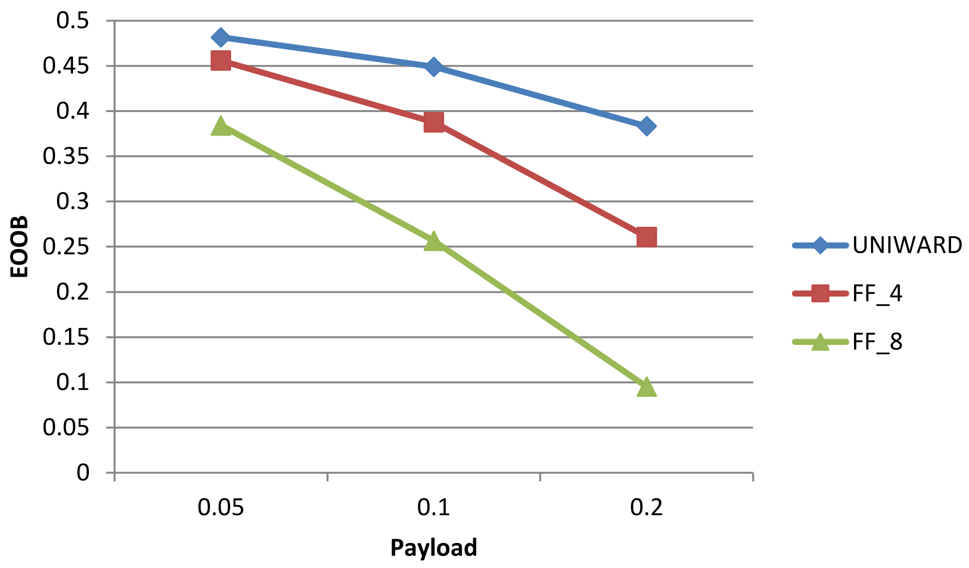


Figure 6.8: Detection error of Out-of-Bag (EOOB) using SRM steganalysis

It is very clear from results shown in figure 6.8 that our proposed schemes have significantly improved robustness against SRM steganalysis if compared with the results shown in figure 6.4. We also notice that using 4-bits pattern have significant improvement over using 8-bits patterns. These results demonstrate that selecting positions for embedding will highly affect the robustness of the embedding system. The choice of the above position selection is by no means the only possible way of improving robustness against SRM. In fact, our content-based steganography schemes can be used with any position selection procedure to improve its robustness.

Finally, these robustness results and consideration of ratio of change, all point that our content based scheme, as well as any other steganographic schemes, can greatly benefit from selecting suitable cover images to meet certain criteria. Much work in steganography has focused on how to improve the performance of embedding techniques by modifying the manner of embedding but little is done on choosing the cover image as the signal carrier. Such work can now benefit from improved chance to easily generate digital media with almost any desired property.

6.3 Invisibility (Image Quality)

Finally, we complement the results of robustness and security of our content-based embedding schemes by demonstrating the invisibility of the embedded secret LBPH patterns using the commonly used image quality measure of peak-signal-to-noise ratio (PSNR) calculated between cover and stego-image. Though the literature in image processing offer many sophisticated quality measures, but the PSNR provide a measure of the amount of distortion or noise presence in an image post processing or manipulation. Table 6.2 and figure 6.9 shows the average value of PSNR (dB) obtained from using the same 1000 greyscale cover images used in previous experiments. The table or figure also include results obtained for using all our 3 different content-based methods, explained in previous chapter, for embedding the different LBPH patterns size (4 or 8) at 5 different payload percentages (0.2285, 0.45, 0.6855, 0.9141, and 0.9902). For comparison, the table or figure also include PSNR values obtained when we used the 3 other embedding schemes TLSB, LSBMR, and S-UNIWARD for embedding the same set of LBPH patterns.

The results of comparison demonstrate that the stego-images created by all our steganographic methods have better quality if compared with TLSB and LSBMR. All our proposed methods except proposed M1 with 8-bits have higher invisibility and quality if compared with S-UNIWARD embedding scheme, the differences become clearer when high payloads embedded. In summary these experiments add more evidences to support the already demonstrated security and efficiency in terms of amount of change in cover pixel values.

Table 6.2: PSNR between cover and stego-images

Payload	M1 8-bit	M1 4-bit	M2 8-bit	M2 4-bit	M3 8-bit	M3 4-bit	TLSB	LSBMR (Mielikainen, 2006)	S-UNIWARD (Holub, et al., 2014)
A	59.357	62.336	62.788	63.164	62.849	63.289	57.551	58.800	62.282
B	56.176	59.163	59.372	59.928	59.575	60.180	54.610	55.858	58.664
C	54.292	57.299	57.540	58.118	57.630	58.326	52.780	54.059	56.427
D	53.058	56.125	56.323	56.989	56.436	57.234	51.531	52.875	54.730
E	52.691	55.822	55.910	56.686	56.027	56.952	51.184	52.592	54.230

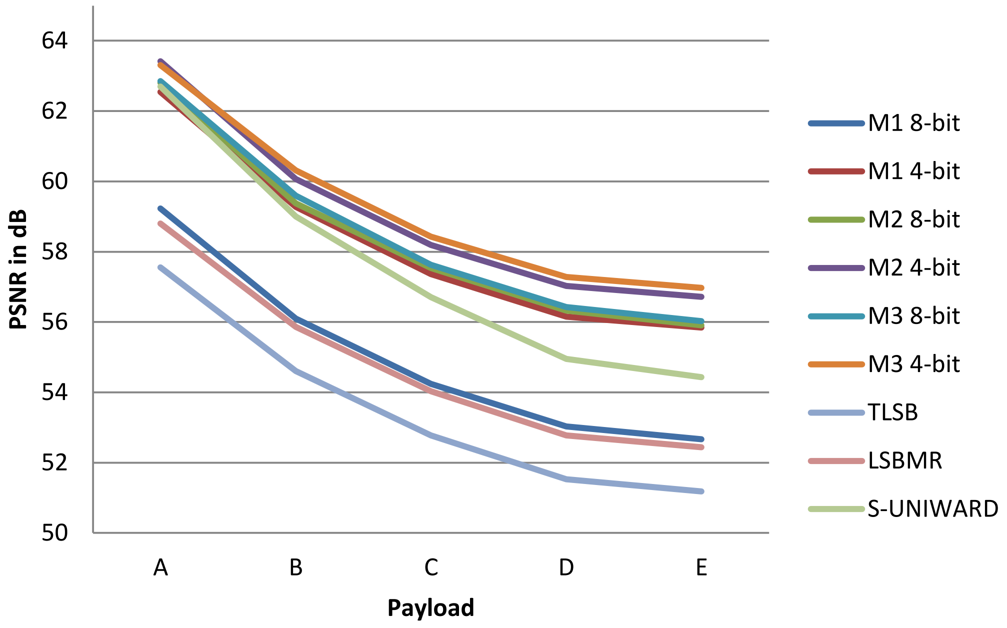


Figure 6.9: PSNR between cover and stego-images

6.4 Conclusions

In this chapter, we investigated the robustness of our content-based steganographic scheme, designed for hiding face biometric LBPH patterns, against targeted and universal steganalysis tools. We conducted several experiments for this purpose using all faces in the Yale database for embedding into 1000 greyscale images from BOSSbase database at different embedding ratios. The experiments also included comparisons of robustness of 3 existing steganographic schemes.

The results of the experiments demonstrated that the content-based scheme is robust against all the 3 targeted steganalysis tools. This remained true for all payloads; although at the full payload the steganalyis tools were reporting a very low ratio which may reflect the margin of error in the report of these tools.

Unfortunately, the scheme was not as successful in avoiding detection by the universal SRM tool. In this set of experiments we also checked the robustness of the S-UNIWARD scheme and found that it has much better robustness than our scheme at low embedding ratios. By analysing the way the S-UNIWARD to achieve this kind of performance, we found that this due to the fact it is designed specifically to withstand SRM attack by embedding in certain locations that cannot generate certain types of distortions that are related to the training features or filters in the SRM. Since, face LBPH pattern generate a small payload, we modified our scheme by embedding in edge regions. The retesting of the modified content-based scheme we achieved robustness against SRM at low payload that is comparable to that of S-UNIWARD.

Finally, measuring the invisibility of the secrets that are embedded by our content-based scheme, in terms of PSNR, has shown that our schemes outperforms all other tested schemes but only marginally when compared with S-UNIWARD.

Chapter 7
Conclusions and Future Works

7.1 Conclusions

This thesis was devoted to investigate the problem related to the secure transfer of biometric data between entities, for remote authentication or identification, while protecting privacy. These investigations were motivated by the widely accepted knowledge that encrypting the biometric data can only protect the data during transmission. Although in recent years the use of homomorphic ciphers have been promoted for privacy preserving solution, but efficiency seem to be a major obstacle that require more research. Steganography, being the obvious other alternative security mechanism that may provide an appropriate solution, has become the focus of this thesis investigations. Initial investigations revealed that for this solution to be practical, secure and privacy preserving certain properties must be satisfied by the biometric data as well as the hiding scheme. Consequently, our first task was to determine these properties before developing specific schemes. The main challenging requirements in the steganography field that are not restricted to their use for transmitting biometrics data include capacity, invisibility, and robustness against targeted as well as universal steganalysis tools.

Due to the fact that the face is the most acceptable public identity of a person, and could be easily recorded using cameras embedded on personal mobile devices that most people possess, face biometrics was our obvious choice. The main aims of this thesis was then to study and understand the properties of steganography as well as face biometric features that could be exploited and integrated within an innovative robust embedding techniques to transfer face biometric data securely within a privacy preserving environment. The most important criterion for selecting the suitable face biometric scheme is that the embedding process does not adversely impact the recognition accuracy. The first part of the thesis focused on investigating the variety of face feature extraction schemes, for their suitability to be binarised and hidden in natural image to be used for remote authentication without losing accuracy. Another steganography-related condition to be imposed on the choice of face feature vector relates to the secret data size for its impact on payload and stego image quality. The privacy preserving requirement adds another restriction on the choice of the binarised face feature vector. Here we link this to the infeasibility of recovering the originally capture face image from the feature vector.

Having reviewed a variety of face recognition schemes, we have come to realise that the LBP based scheme provides many of the requirements. In its simplest spatial domain form it works like a filter that replaces each pixel value with an 8-bit code that reflect the order relation between each pixel and that of its 8 neighbours. Face recognition is based on testing similarity of a special type of histograms of 59 bins for the frequency of the LBP codes, known as LBPH features. LBP codes provide image-dependent binarization, face LBPH features are known to yield excellent recognition rate, and more importantly it is privacy preserving in that it is not feasible to retrieve the original image from the LBPH. For embedding purpose, we only need to embed the size of the 59 bins in a certain order. However, due to size of the face image the bins have different unknown sizes which for recovery needs to be sent as side information. Dividing the secret face image into block may reduce, but not eliminate, the chance of this happening. Normalising the size of the bins have been shown to solve the problem but with some loss in accuracy. Using LBPH in the wavelet domain, extracted from blocks of each of the wavelet sub-bands has led to the elimination of the problem while preserving accuracy. This success together with the interest in reducing payload for embedding, has motivated the modification of the LBP codes by computing them using only 4 neighbours. This led to 2 different types of 4-bit patterns depending on whether we take Horizontal-Vertical or Diagonal neighbours. These investigations generated a variety of face recognition schemes that use each of these 3 different LBPH patterns or a combination of them, and led to improved accuracy. As a result using only 4 neighbours the number of LBPH bins was reduced to 16 leading to significant reduction in embedding payload capacity. The experimental results have demonstrated that the proposed methods can reduce the number of features by 22% to 72% of the original features (see Chapter 4). By testing the performance of the various schemes that require less number of LBPH features, we find that there is a trade-off between numbers of reduced features and recognition accuracy. One important benefit from using LBPH representations of face images is the fact that all these representations generate very small payload relative to most cover image sizes. In fact, the above schemes generate payloads in the range 0.08% to 22% of cover image size 512x512. However, for comparison reason the experiments will cover full capacity by embedding multiple face LBPH features.

Our investigation into suitable steganographic schemes started with reviewing existing embedding scheme with focus on their known properties of invisibility, capacity and robustness against known steganalysis tool. The trend in the more recently proposed spatial domain hiding schemes is based on sophisticated ways of manipulating or replacing one or more bit-planes (LSB or 2LSB) of the cover image with the aim of achieving high invisibility, high capacity and robustness against some LSB targeted steganalysis tools. There were various levels of success but what was clear that achieving success for all the 3 criteria remains a challenge.

Our first attempt was aimed at developing a scheme that could achieve robustness against all LSB-targeted steganalysis tools with a good compromise on the other 2 criteria. The developed LSB-witness scheme modifies the 2nd LSB as a witness for the presence of the secret bits in the 1st LSB. This approach guarantees no change in 1st LSB plane, and thereby robustness against all the LSB-targeted steganalysis tools for all and up to 100% payload without introducing significant visual distortion to the cover image obtained. However, due to the fact that the LSB-witness scheme was change the 2nd LSB which seem to have resulted in cover image quality which was lower than that achieved by RLSB, especially at high embedding payloads. Nevertheless, the experiments has demonstrated beyond any doubts the viability of using steganography for remote biometric-based recognition and the biometric feature vectors can be binarised, without leaking information on the freshly recorded biometric sample.

Although, the fact that in the specific application we know that we do not generally need high capacity embedding, we recognised that more work is needed to be done to achieve adequately high invisibility. Noting that almost all existing schemes including the LSB-witness are general-purpose in that the secret message is a random bit-stream. Recognising the fact that unencrypted biometric data are far from being represented by a random secret bit-stream, has motivated the work in the 2nd part of the thesis to investigate, develop and test performance of a new scheme that could achieve a good compromise for embedding face LBP code features. In such a scheme, the embedding must exploit the structure or content of the secret to improve quality, which we called *content-based* steganography. This is a rather different type of steganography from the traditional schemes, could also benefit many steganography applications which deal with structured secrets. Developing such general schemes, require an understanding of the structure of the secrets, but this is outside the scope of this thesis.

Our developed content-based hiding scheme differs from that of the LSB-witness scheme in that instead of embedding the LBPH frequencies, we embed the LBPH patterns themselves. It exploits similarities between these LBPH patterns and the structure of the cover image bit-planes by first organise these as 8-bit or 4-bit patterns. We investigated various block-based embedding where our secret image (or its wavelet subband) is divided into blocks and the cover image into blocks whose LSB bit plane is the same size of the LBPH block bit-stream. The embedding of the LBPH patterns is done in the ascending order of 1's in the pattern, by searching through the LSB-cover image block for the next unused pattern that matches it or has the smallest hamming distance from it. We tested the performance of several versions of this scheme, depending on blocking strategy and pairing blocks of the LBPH patterns to a block of the partitioned cover image blocks. The block pairing strategy can be used as a key shared between sender and receiver as a second layer of security.

Our tests covered the optimality concept which is aimed to minimize distortion of the cover image and maximize the invisibility of the secret message by reducing the pixel value change rate during embedding the required payload. In terms of pixel change rate after hiding, our scheme achieved the ratio of change of 13% which is a significant improvement of the lower bound on optimality ratio of 24% that was achieved by the state of the art S-UNIWARD scheme.

The performance of the content-based schemes was also tested by checking the robustness of the scheme against the targeted steganalysers (DIH, RWS, and the calibrated HCF-COM) and the universal steganalysis tool (SRM). Results demonstrated that none of the 3 targeted steganalysis tools can detect and estimate the embedding ratio of embedding correctly for our schemes. Unfortunately, the SRM detect the present of our schemes as we expected. However, when we incorporates a position selection (edges and noisy regions) process into our schemes, robustness against SRM improved significantly at low embedding rate.

7.2 Future works

The works reported in this thesis was aimed to enhance the security of embedding schemes for a specific type of secrets. In particular, we were interested in the security of embedding face biometric features for remote authentication. To our knowledge our developed content-based embedding scheme is the first embedding scheme that differentiate between embedding face biometric data and other secret or sensitive data such as (text, image, etc.). In order to promote this exciting direction in steganography, the following is a list of potential research projects that extend our work in the future.

Extending Content-based steganography for other biometric traits. The success of our work in developing a specific embedding scheme that exploit certain carefully selected face feature vector for use in privacy preserving remote biometric authentication, is a strong motivation to extend our investigations by testing the viability of embedding other biometrics (fingerprint, Iris) for remote authentication. Such investigations will depend on understanding the non-random patterns of feature vectors for such biometrics that could be exploited appropriately for other content based steganographic schemes.

Natural cover image selection. In the literature, much works in the steganography has focused on how to improve the performance of embedding schemes, and although cover selection is recognised as an important factor little is done on choosing the suitable cover image as the secrete carrier. For content-based steganography, this becomes an essential component in the success of such schemes and the selection would also need to be compatible with the structure and organisation of the embedded secret. This will apart of our future plans.

Robustness of content-based schemes against universal Steganalysis tools. In this thesis we investigate several types of steganalysis tools (targeted and universal), while our main content-based scheme was robust against all known targeted steganalysis tools, for robustness against the universal SRM scheme could have only been improved for low embedding ratios by selecting best positions for embedding. More investigations need to be done to improve robustness of general content-based schemes at high embedding ratios against SRM and other steganalysis tools. In particular, we need to investigate positions where certain known local dependencies (i.e. feature distortion models) where embedding related changes to pixel values lead to less distortion of the cover image and more robust against this kind of steganalysis for higher payload capacities. This will also be closely related to cover selection question. Moreover, our work in the future must address recovery post active attacks. We shall investigate the solutions in case of loss or bits are missed by active attacks. One obvious solution will be the incorporation of error correction code (ECC).

REFERENCES

- Abboud, A. J., 2011. *Quality Aware Adaptive Biometric Systems,* Buckingham,UK: Thesis for the degree of Doctor of Philosophy in computer science in the University of Buckingham..

- Abdulla, A. A., Jassim, S. A. & Sellahewa, H., 2013. *Secure Steganography Technique Based on Bitplane Indexes.* California, USA, IEEE International Symposium on Multimedia.

- Agrawal, N. & Savvides, M., 2009. *Biometric Data Hiding: A 3 Factor Authentication Approach to Verify Identity with a Single Image Using Steganography, Encryption and Matching.* Miami, FL , IEEE Conference on Computer Vision and Pattern Recognition, pp. 85-92.

- Ahonen, T., Hadid, A. & Pietikainen, M., 2004. *Face Recognition with Local Binary Patterns.* Czech Republic, Proceedings of the 8th european conference on computer vision, pp. 469-481.

- Ahonen, T., Hadid, A. & Pietikainen, M., 2006. Face Description with Local Binary Patterns: Application to Face Recognition. *IEEE Transactions on Pattern Analysis and Machine Intelligence,* 28(12), pp. 2037-2041.

- Al-Assam, H., 2013. *Entropy Evaluation and Security Measures for Reliable Single/Multi–Factor Biometric Authentication and Biometric Keys,* Buckingham: Thesis for the degree of Doctor of Philosophy in computer science in the University of Buckingham.

- AL-Assam, H., Rashid, R. & Jassim, S., 2013. *Combining Steganography and Biometric Cryptosystems for Secure Mutual Authentication and Key Exchange.* London/UK, The 8th International Conference for Internet Technology and Secured Transactions (ICITST-2013).

- Al-Jawed, N., 2009. *Exploiting Statistical Properties of Wavelet Coefficient for Image/ Video Processing and Analysis Tasks,* Buckingham/UK: Thesis for the degree of Doctor of Philosophy in computer science in the University of Buckingham.

- Amirtharajan, R., Akila, R. & Deepikachowdavarapu, P., 2010. A Comparative Analysis of Image Steganography. *International Journal of Computer Applications,* May, 2(3), pp. 41-47.
- Avcibas, I., Memon, N. & Sankur, B., 2001. *Steganalysis Using Image Quality Metrics.* San Jose, CA, SPIE/ Security and Watermarking Multimedia Contents.
- Bailey, K. & Curran, K., 2006. An Evaluation of Image based Steganography Methods Using Visual Inspection and Automated Detection Techniques. *Springer, Multimed Tools Appl,* Volume 30, pp. 55-88.
- Bas, P., Filler, T. & Pevný, T., 2011. *Break Our Steganographic System – the ins and outs of organizing BOSS.* Prague, Czech Republic, Information Hiding , 13th International Workshop.
- Belhumeur, P. N., Hespanha, J. P. & Kriegman, D. J., 1997. Eigenfaces vs. Fisherfaces: Recognition Using Class Specific Linear Projection. *IEEE Transactions on Pattern Analysis and Machine Intelligence,* JULY , 19(7), pp. 711-720.
- Bera, S. & Sharma, M., 2010. Steganalysis of Real Time Image by Statistical Attacks. *International Journal of Engineering Science and Technology,* 2(9), pp. 4396-4405.
- Chan, C.-K. & Cheng, L., 2004. Hiding Data in Images by Simple LSB Substitution. *Pattern Recognition,* Volume 37, pp. 469-474.
- Chan, C. H., 2008. *Multi-scale Local Binary Pattern Histogram for Face Recognition,* Guildford, Surrey, U.K.: PhD. Thesis in University of Surrey.
- Chen, W.-J., Chang, C.-C. & Ngan Le, T. H., 2010. High Payload Steganography Mechanism Using Hybrid Edge Detector. *Expert Systems with Applications,* Volume 37, pp. 3292-3301.
- Chien, J.-T. & Wu, C.-C., 2002. Discriminant Wavelet Faces and Nearest Feature Classifiers for Face Recognition. *IEEE Transaction on Pattern Analysis and Machine Intelligence,* 24(12), p. 1644–1649.
- Dc, W. & Tsai, W., 2003. A Steganographic Method for Images by Pixel-Value Differencing. *Pattern Recognition,* pp. 1613-1626.

- Dickman, S. D., 2007. *An Overview of Steganography,* Virginia: James Madison University Infosec Techreport.
- Dong, J. & Tan, T., 2009. *Security Enhancement of Biometrics, Cryptography and Data Hiding by Their Combinations.* Xian China, Visual Information Engineering, 5th International Conference, pp. 239-244.
- Farid, H., 2002. *Detecting Hidden Messages Using Higher-Order Statistical Models.* Rochester, NY, Proc. IEEE International Conference in Image Processing.
- Filler, T. & Fridrich, J., 2010. Gibbs Construction in Steganography. *IEEE Transactions on Information Forensics Security,* 5(4), p. 705–720.
- Fridrich, J., Du, R. & Long, M., 2000. Steganalysis of LSB Encoding in Color Images. *ICME,* July.
- Fridrich, J. & Goljan, M., 2002. *Practical Steganalysis of Digital Images – State of the Art.* San Jose, CA, Proceeding of SPIE photonics imaging, security and watermarking of multimedia contents, pp. 1-13.
- Fridrich, J. & Goljan, M., 2004. *On Estimation of Secret Message Length in LSB Steganography in Spatial Domain.* San Jose, CA, Security, Steganography, and Watermarking of Multimedia Contents, SPIE 5306, p. 23–34..
- Fridrich, J., Goljan, M. & Du, R., 2001. *Reliable Detection of LSB Steganography in Color and Grayscale Images.* Ottawa, Proceedings of ACM Workshop on Multimedia and Security, pp. 27-30.
- Fridrich, J., Goljan, M. & Hogea, D., 2003. *New Methodology for Breaking Steganographic Techniques for JPEGs.* Santa Clara, California, International Society for Optical Engineering, pp. 143-155.
- Fridrich, J. & Kodovský, J., 2012. Rich Models for Steganalysis of Digital Images. *IEEE Transactions of Information Forensics Security,* 7(3), p. 868–882.
- Fridrich, J. & Soukal, D., 2006. *Matrix Embedding for Large Payloads.* SUNY Binghamton (United States), Proc. of SPIE Electronic Imaging,Photonics West.
- Geng, C. & Jiang, X., 2009. *Face Recognition Using SIFT Features.* Cairo, 16th IEEE International Conference on Image Processing (ICIP).

- Gentry, C., 2009. *A Fully Homomorphic Encryption Scheme PhD thesis,* CA, United States: Stanford University.

- Gentry, C. & Halevi, S., 2011. *Fully Homomorphic Encryption without Squashing Using Depth-3 Arithmetic Circuits.* Washington, DC, USA, IEEE Computer Society.

- Gentry, C. & Halevi, S., 2011. Implementing Gentry’s Fully Homomorphic Encryption Scheme. In: K. G. Paterson, ed. *Advances in Cryptology – EUROCRYPT 2011.* Estonia: Springer Berlin Heidelberg, pp. 129-148.

- Georghiades, A., Belhumeur, P. N. & Kriegman, D. J., 2001. From Few to Many:Generative Models for Recognition under Variable Pose and Illumination. *IEEE Transactions on Pattern Analysis and Machine Intelligence,* 23(6), pp. 643-660.

- Gonzales, R. C. & Woods, R. E., 2002. *Digital Image Processing.* Second eddition ed. New Jersey: Tom Robbins.

- Guo, G. et al., 2003. KNN Model-Based Approach in Classification. *Lecture Notes in Computer Science,* Volume 2888, p. 986 – 996.

- Guo, Z., Zhang, L., Zhang, D. & Mou, X., 2010. *Hierarchical Multiscale LBP for Face and Palmprint Recognition.* Hong Kong, IEEE 17th International Conference on Image Processing, pp. 4521-4524.

- Harmsen, J. J. & Pearlman, W. A., 2003. *Higher-Order Statistical Steganalysis of Palette Images.* Santa Clara, CA, Proc. SPIE Security Watermarking Multimedia Contents.

- Hempstalk, K., 2006. *Hiding Behind Corners: Using Edges in Images for Better Steganography.* Hamilton, New Zealand, Computing Women's Congress.

- Holub, V. & Fridrich, J., 2012. *Designing Steganographic Distortion Using Directional Filters.* Tenerife, Fourth IEEE International Workshop on Information Forensics and Security.

- Holub, V., Fridrich, J. & Denemark, T., 2014. Universal Distortion Function for Steganography in an Arbitrary Domain. *EURASIP Journal on Information Security,* 2014(1).

- Hussam, U.-D., Ihmaidi, A., Al-Jaber, A. & Hudaib, A., 2006. *Securing Online Shopping Using Biometric Perdonal Authentication and Steganography.* s.l., Information and Communication Technologies ICTTA.

- Islam, S., Modi, M. R. & Gupta, P., 2014. Edge-based Image Steganography. *EURASIP Journal on Information Security,* 2014(8).

- Jain, A. K., Flynn, P. & Ross, A. A., 2008. *Handbook of Biometrics.* 1 ed. US: springer.

- Jain, A. K., Ross, A. & Uludag, U., 2005. *Biometric Templete Security: Challenges and Solutions.* Antalya,Turkey, European Signal Processing Conference.

- Jain, A. K. & Uludag, U., 2003. Hiding Biometric Data. *IEEE Transactions on Pattern Analysis and Machine Intelligence,* NOVEMBER, 25(11), pp. 1494-1498.

- Johnson, N. F. & Jajodia, S., 1998. Exploring Steganography: Seeing the Unseen. *Computer Jornal,* pp. 26-34.

- Johnson, N. F. & Jajodia, S., 1998. *Steganalysis: The Investigation of Hidden Information.* New York, USA, IEEE Information Technology Conference, pp. 113-116.

- Kapczynski, A. & Banasik, A., 2011. *Biometric Logical Access Control Enhanced by Use of Steganography Over Secured Transmission Channel.* Prague, Czech republic, The 6th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and applications.

- Kathuria, M., 2010. Performance Enhancement of Identification System using Vein Biometric with Modified Run Length Encoding,Stegnography and Cryptography. *International Journal of Computer Applications,* December, 12(8), pp. 1-5.

- Katzenbeisser, S. & Petitcolas, F. A., 2000. *Information Hiding Techniques for Steganography and Digital Watermarking.* Boston, London: Artech House Computer Security Series.

- Ker, A. D., 2004. *Improved Detection of LSB Steganography in Grayscale Images.* s.l., Proc. Information Hiding Workshop, Lecture Notes in Computer Science vol. 3200, Springer, pp. 97–115..

- Ker, A. D., 2004. *Quantitative Evaluation of Pairs and RS Steganalysis.* San Jose,CA, Proc. of, SPIE, Security, Steganography, Watermarking of Multimedia Contents..

- Ker, A. D., 2005. Steganalysis of LSB Matching in Grayscale Images. *IEEE Signal Processing Letters,* JUNE , VOL. 12(NO. 6), pp. 441-444.

- Ker, A. D., 2007. Steganalysis of Embedding in Two Least-Significant Bits. *IEEE Transactions on Information Forensics and Security,* MARCH , 2(1), pp. 46-54.

- Ker, A. D. et al., 2013. *Moving Steganography and Steganalysis from the Laboratory into the Real World.* Montpellier, France, Proceedings of the first ACM workshop on Information hiding and multimedia security (IHMMSec2013), pp. 45-58.

- Ker, A. D. & Böhme, R., 2008. *Revisiting Weighted Stego-image Steganalysis.* San Jose, CA, Proceedings SPIE, Electronic Imaging, Security, Forensics, Steganography, and Watermarking of Multimedia Contents.

- Kodovský, J. & Fridrich, J., 2013. *Quantitative Steganalysis Using Rich Models.* Burlingame, California, USA, Proceding of SPIE 8665, Media Watermarking, Security, and Forensics 2013, 86650O.

- Kodovský, J., Fridrich, J. & Holub, V., 2012. Ensemble Classifiers for Steganalysis of Digital Media. *IEEE Transaction of Information Forensics Security,* 7(2), p. 432–444.

- Križaj, J., Štruc, V. & Pavešić, N., 2010. Adaptation of SIFT Features for Robust Face Recognition. *LNCS on image analysis and recognition,* Volume 6111, pp. 394-404.

- Lafferty, P. & Ahmed, F., 2004. *Texture based Steganalysis: Results for Color Images.* Bellingham, WA, Proc. SPIE Mathematics of Data/Image Coding, Compression, and Encryption VII with Applications.

- Li, B., He, J. & Huang, J., April, 2011. A Survey on Image Steganography and Steganalysis. *Information Hiding and Multimedia Signal Processing,* 2(2).

- Lin, E. T. & Delp, E. J., 2001. *A Review of Data Hiding in Digital Images,* West Lafayette: Purdue University.

- Liu, X., Du, M. & Jin, L., 2010. *Face Features Extraction Based on Multi-scale LBP.* Dalian , 2nd International Conference on Signal Processing Systems (ICSPS), pp. V2-438-V2-441.
- Li, X., Qi, Z., Yang, Z. & Kong, J., 2009. *A Novel Hidden Transmission of Biometric Images base on Chaos and Image Content.* Wuhan, Hubei , First International Workshop on Education Technology and Computer Science.
- Luo, W., Huang, F. & Huang, J., 2011. A More Secure Steganography based on Adaptive Pixel-Value Differencing Scheme. *Springer Multimed Tools Appl,* Volume 52, pp. 407-430.
- Lu, Y. et al., 2008. *Lossless and Content-based Hidden Transmission for Biometric Verificaion.* Shanghai , IEEE Second International Symposium on Intelligent Information Technology Application.
- Lyu, S. & Farid, H., 2002. *Detecting Hidden Messages Using Higher-Order Statistics and Support Vector Machines.* Noordwijkerhout, The Netherlands, 5th International Workshop on Information Hiding.
- Lyu, S. & Farid, H., 2004. *Steganalysis Using Color Wavelet Statistics and One-Class Vector Support Machines.* San Jose, CA, Procedings of SPIE, Security, Steganography, Watermarking of Multimedia Contents, p. 35–45.
- Lyu, S. & Farid, H., 2006. Steganalysis Using Higher-Order Image Statistics. *IEEE Transactions on Information Forensics and Security,* 1(1), pp. 111-119.
- Mallat, S. G., 1989. A Theory for Multiresolution Signal Decomposition: The Wavelet Representation. *IEEE Transactions on Pattern Analysis and Machine Intelligence,* 11(7), pp. 674 - 693.
- Meng, J. & Gao, Y., 2010. *Face Recognition based on Local Binary Patterns with Threshold.* San Jose, CA , IEEE International Conference on Granular Computing.
- Mielikainen, J., 2006. LSB Matching Revisited. *IEEE Signal Processing Letters,* May , 13(5), pp. 285-287.
- Morkel, T., Eloff, J. & Olivier, M., 2005. *An Overview of Image Steganography.* Sandton, South Africa, Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005).

- Murugesh, R., 2012. *Advanced Biometric ATM Machine With AES 256 and Steganography Implemintation.* Anna University, Chennai, IEEE- Fourth International Conference on Advanced Computing, ICoAC 2012 MIT.

- Na, W., Chiya, Z., Xia, L. & Yunjin, W., 2010. *Enhancing Iris-Feature Security with Steganography.* Taichung , IEEE conference on Industrial Electronics and Applications, pp. 2233-2237.

- Ntalianis, K., Tsapatsoulis, N. & Drigas, A., 2011. Video-Object Oriented Biometrics Hiding for User Authentication under Error-Prone Transmissions. *EURASIP Journal on Information Security,* Volume 2011, p. 12.

- Ojala, T., Pietikäinen, M. & Harwood, D., 1996. A Comparative Study of Texture Measures with Classification based on Featured Distributions. *Pattern Recognition,* January, 29(1), pp. 51-59.

- Ojala, T., Pietikäinen, M. & Mäenpää, T., 2002. Multiresolution Gray Scale and Rotation Invariant Texture Classification with Local Binary Patterns. *IEEE Transactions on Pattern Analysis and Machine Intelligence,* July, 24 (7), pp. 971-987.

- Penev, P. S. & Atick, J. J., 1996. Local Feature Analysis: A General Statistical Theory for Object Representation. *Network: computation in neural systems,* 7(3), pp. 477-500.

- Pevný, T., Filler, T. & Bas, P., 2010. *Using High-Dimensional Image Models to Perform Highly Undetectable Steganography.* Calgary,Canada, 12th International Conference of Information Hiding.

- Rashid, R. D., Jassim, S. A. & Sellahewa, H., 2013. *Covert Exchange of Face Biometric Data using Steganography.* University of Essex, Colchester, UK, IEEE Fifth Computer Science and Electronic Engineering Conference (CEEC 2013).

- Rashid, R. D., Jassim, S. A. & Sellahewa, H., 2013. *LBP based on Multi Wavelet Sub-bands Feature Extraction Used for Face Recognition.* SOUTHAMPTON, UK, IEEE International Workshop on Machine Learning for Signal Processing.

- Rashid, R. D., Sellahewa, H. & Jassim, S. A., 2013. *Biometric Feature Embedding Using Robust Steganography Technique.* Baltimore,USA, Proceeding of SPIE 8755, Mobile Multimedia/Image Processing, Security, and Applications.

- Ratha, N., Connell, J. & Bolle, R., 2001. Enhancing Security and Privacy in Biometrics-based Authentication Systems. *IBM SYSTEMS JOURNAL*, 40(3), pp. 614-634.
- Ratha, N. K., Connell, J. H. & Bolle, R. M., 2001. *An Analysis of Minutiae Matching Strength.* Halmstad, Sweden, Proc. of Third International Conference on Audio- and Video-Based Biometric Person Authentication.
- Samaria, F. S. & Harter, A. C., 1994. *Parameterisation of a Stochastic Model for Human Face Identification.* Sarasota (Florida), Proceedings of the 2nd IEEE Workshop on Applications of Computer Vision.
- Sellahewa, H., 2006. *Wavelet-based Automatic Face Recognition for Constrained Devices,* University of Buckingham, Buckingham, UK: Dphil thesis.
- Sellahewa, H. & Jassim, S., 2010. Image Quality-based Adaptive Face Recognition. *IEEE Transactions on Instrumentation and Measurement,* April, 59(4), pp. 805-813.
- Sellahewa, H. & Jassim, S. A., 2008. *Illumination and Expression Invariant Face Recognition: Toward Sample Quality-based Adaptive Fusion.* Arlington, VA, 2nd IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS 2008).
- Shan, C., Gong, S. & McOwan, P., 2009. Facial Expression Recognition based on Local Binary Patterns: A Comprehensive Study. *Image and Vision Computing,* Volume 27, pp. 803-816.
- Shaozhang, N., Qi, Z., Baojiang, C. & Linna, Z., 2009. Detecting LSB Steganography Based on Noise Function. *Chinese Jornal of Electronics,* April, 18(2), pp. 343-346.
- Sharp, T., 2001. *An Implementation of Key-based Digital Signal Steganography.* Pittsburgh, PA, USA, 4th International Workshop on Information hiding , pp. 13-26.
- Shiva Kumar, K. B., Raja, K. B. & Pattnaik, S., 2011. Hybrid Domain in LSB Steganography. *International Journal of Computer Applications,* April, 19(7), pp. 35-40.

- Singh, K. M., Singh, L. S., Singh, A. B. & Devi, K. S., 2007. *Hiding Secret Message in Edges of the Image.* Dhaka, Bangladesh, International Conference on Information and Communication Technology, pp. 238-241.
- Smart, N. P. & Vercauteren, F., 2014. Fully Homomorphic SIMD Operations. *Designs, Codes and Cryptography,* 71(1), pp. 57-81.
- Sonsare, P. M. & Sapkal, S., 2011. *Stegano-Crypto System for Enhancing Biometric-Feature Security with RSA.* Singapore, International Conference on Information and Network Technology, pp. 196-200.
- Stehlé, D. & Steinfeld, R., 2010. Faster Fully Homomorphic Encryption. In: M. Abe, ed. *Advances in Cryptology - ASIACRYPT 2010.* Singapore: Springer Berlin Heidelberg, pp. 377-394.
- Sur, A., Goel, P. & Mukhopadhyay, J., 2008. *A Spatial Domain Steganographic Scheme for Reducing Embedding Noise.* Malta, Turkey, EEE International Symposium on Communications, Control and Signal Processing (ISCCSP 2008).
- Tang, H., Sun, Y., Yin, B. & Ge, Y., 2010. *Face Recognition based on Haar LBP Histogram.* Chengdu , 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), pp. V6-235-V6-238.
- Turk, M. A. & Pentland, A. P., 1991. *Face Recognition Using Eigenfaces.* s.l., IEEE Conference on Computer Vision and Pattern Recognition.
- Umamaheswari, M., Sivasubramanian, S. & Pandiarajan, S., 2010. Analysis of Different Steganographic Algorithms for Secured Data Hiding. *IJCSNS International Jornal of Computer Science and Network Security,* August, 10(8), pp. 154-160.
- Unnikrishnan, R., 2011. *Analysis of Modern Steganographic Techniques.* New Delhi, Computing For Nation Development.
- Venkatraman, S., Abraham, A. & Paprzycki, M., 2004. *Significance of Steganography on Data Security.* s.l., International Conference on Information Technology: Coding and Computing (ITCC'04).
- Wang, C. et al., 2010. *A Content-Adaptive Approach For Reducing Embedding Impact In Steganography.* Dallas,Texas,USA, IEEE International Conference on Acoustics, Speech and Signal Processing.

- Wang, W., Chen, W. & Xu, D., 2011. *Pyramid-based Multi-scale LBP Features for Face Recognition.* Guilin, Guangxi , IEEE International Conference on Multimedia and Signal Processing, pp. 151-155.
- Wang, Y., Yan, Q. & Li, K., 2011. *Hand Vein Recognition based on Multi-scale LBP and Wavelet.* Guilin, Proceedings of the 2011 International Conference on Wavelet Analysis and Pattern Recognition, pp. 214-218.
- Westfeld, A. & Pfitzmann, A., 1999. *Attacks on Steganographic Systems Breaking the Steganographic Utilities EzStego, Jsteg,Steganos, and S-Tools—and Some Lessons Learned.* Dresden, Germany, 3rd Information Hiding Workshop, pp. 61-75.
- Whitelam, C., Osia, N. & Bour, T., 2013. *Securing Multimodal Biometric Data through Watermarking and Steganography.* Waltham, MA, IEEE International Conference on Technologies for Homeland Security (HST), pp. 61 - 66.
- Wu, H.-C., Wu, N.-I., Tsai, C.-S. & Hwang, M.-S., 2005. Image Steganographic Scheme based on Pixel-Value Differencing and LSB Replacement Methods. *IEE Proc. Image Signal Process,* October, 152(5), pp. 611-615.
- Xuan, G. et al., 2005. Steganalysis Based on Multiple Features Formed by Statistical Moments of Wavelet Characteristic Functions. *Lecture Notesin Computer Science, Springer-Verlag Berlin Heidelberg,* Volume 3727, pp. 262-277.
- Xu, J., Sung, A. H., Shi, P. & Liu, Q., 2004. *JPEG Compression Immune Steganography Using Wavelet Transform.* s.l., IEEE International Conference of Information Technology.
- Yang, C.-H., Weng, C.-Y., Wang, S.-J. & Sun, H.-M., 2008. Adaptive Data Hiding in Edge Areas of Images With Spatial LSB Domain Systems. *IEEE Transactions on Information Forensics and Security,* September, 3(3), pp. 488-497.
- Zebbiche, K., Ghouti, L., Khelifi, F. & Bouridane, A., 2006. *Protecting Fingerprint Data Using Watermarking.* Istanbul , IEEE Proceedings of the First NASA/ESA Conference on Adaptive Hardware and Systems (AHS'06).
- Zhang, J., Cox, I. J. & Doerr, G., 2007. *Steganalysis for LSB Matching in Images With High-Frequency Noise.* Crete, Proceedings of the IEEE Workshop on Multimedia Signal Processing, p. 385–388.

- Zhang, T. & Ping, X., 2003. *Reliable Detection of LSB Steganography based on the Difference Image Histogram.* s.l., IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP '03), III 545-548.
- Zhi, L., Ai Fen, S. & Yi Xian, Y., 2003. *A LSB Steganography Detection Algorithm.* s.l., 14th IEEE Proceedings on Personal, Indoor and Mobile Radio Communications.

LIST OF PUBLICATIONS

During the life of this research programme, the following papers were published with fellow researchers within the department of Applied Computing at The University of Buckingham. For more details about individual papers see references.

- Hisham Al-Assam, **Rasber D. Rashid**, and Sabah Jassim, “**Combining Steganography and Biometric Cryptosystems for Secure Mutual Authentication and Key Exchange**”, 8th International Conference for Internet Technology and Secured Transactions (ICITST-2013), December 9-12, 2013, London, United Kingdom. (AL-Assam, et al., 2013)

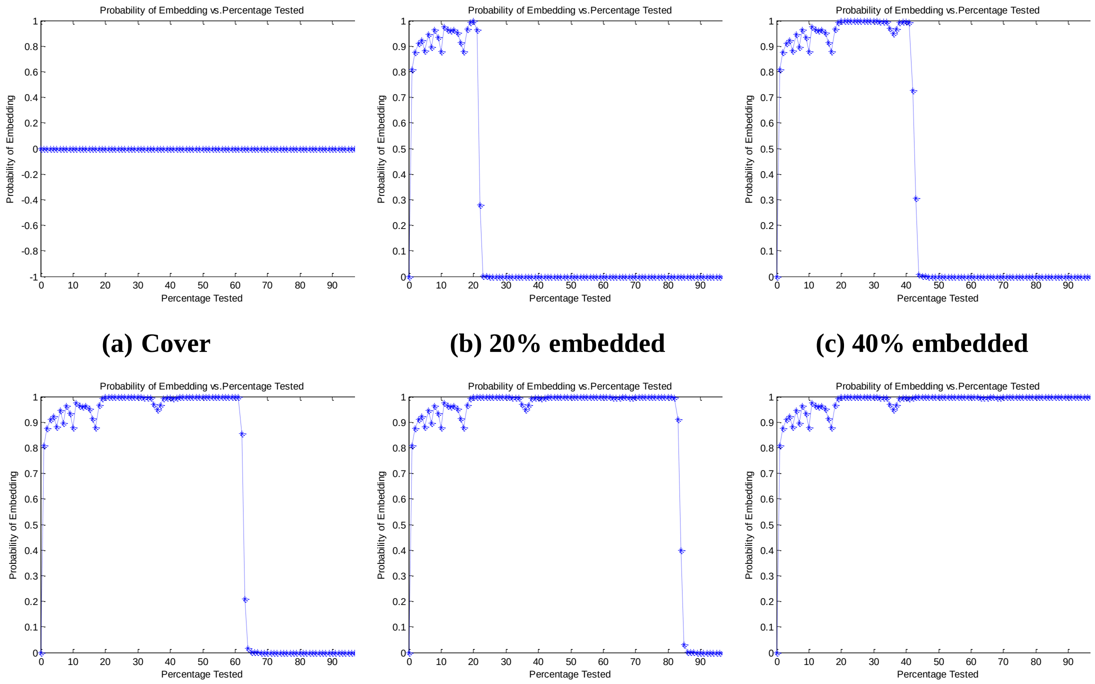
- **Rasber D. Rashid** , Sabah A. Jassim and Harin Sellahewa,”**LBP based on Multi Wavelet Sub-bands Feature Extraction used for Face Recognition**“ , IEEE International Workshop on Machine Learning for Signal Processing (MLSP) , September 22-25, 2013 Southampton, United Kingdom. (Rashid, et al., 2013)

- **Rasber D. Rashid** , Sabah A. Jassim and Harin Sellahewa, “**Covert Exchange of Face Biometric Data using Steganography**“, Fifth Computer Science and Electronic Engineering Conference (CEEC 2013), September 17-18, 2013, University of Essex, Colchester, United Kingdom. (Rashid, et al., 2013)

- **Rasber D. Rashid** , Harin Sellahewa and Sabah A. Jassim,”**Biometric feature embedding using robust steganography technique**“, In proceedings of SPIE 8755, Mobile Multimedia/Image Processing, Security, and Applications, Baltimore/USA,(May , 2013). (Rashid, et al., 2013)

APPENDIX

A: Robustness against Pairs of Value (PoV) Steganalysis Tool



(a) Cover

(b) 20% embedded

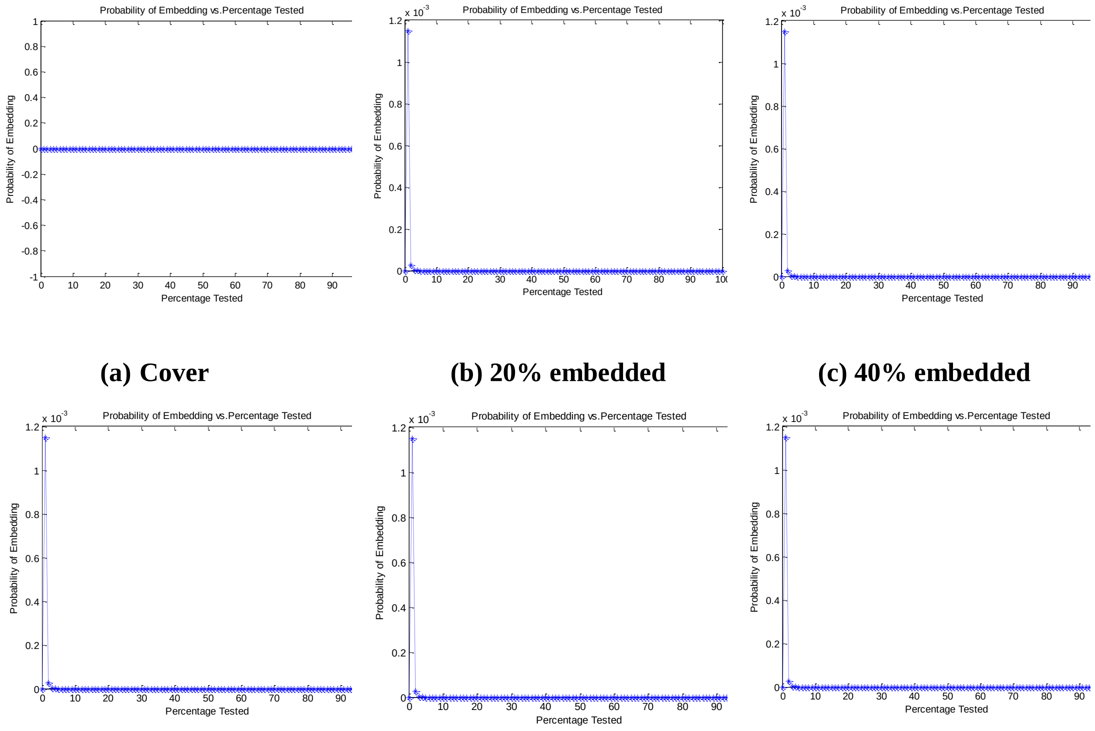
(c) 40% embedded

(d) 60% embedded

(e) 80% embedded

(f) 100% embedded

Figure A.1: SLSB detection using PoV steganalysis for different payload for Living room image



(a) Cover

(b) 20% embedded

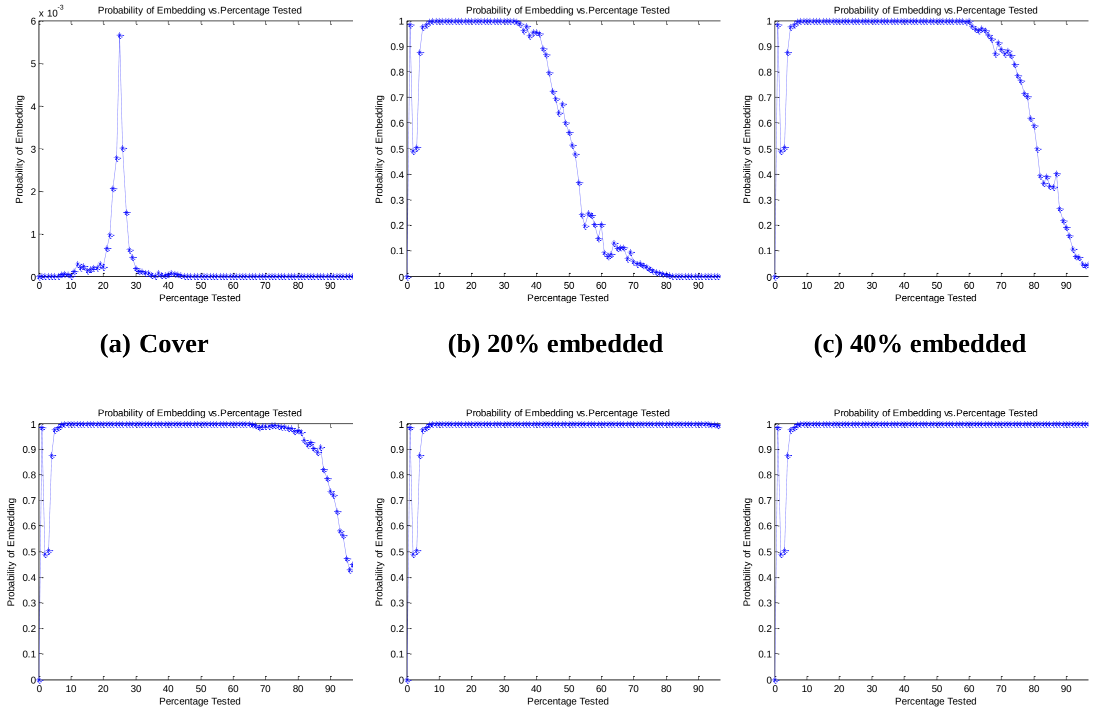
(c) 40% embedded

(d) 60% embedded

(e) 80% embedded

(f) 100% embedded

Figure A.2: SLSB-Witness detection using PoV steganalysis for different payload for Living room image



(a) Cover

(b) 20% embedded

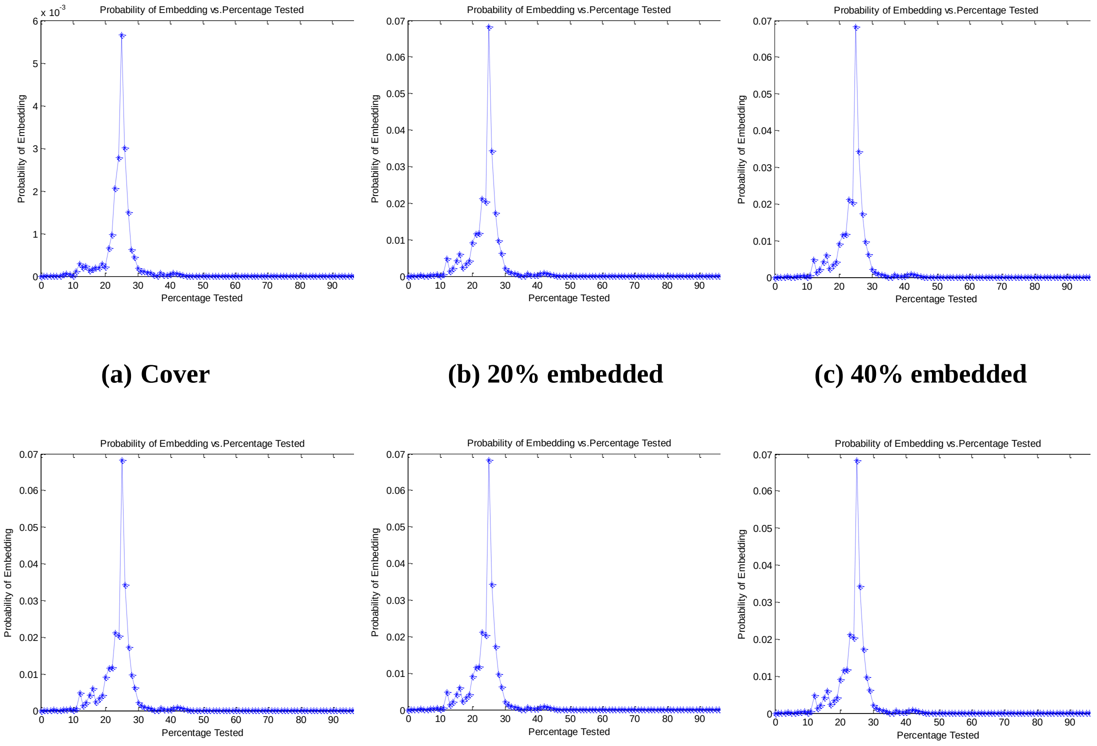
(c) 40% embedded

(d) 60% embedded

(e) 80% embedded

(f) 100% embedded

Figure A.3: SLSB detection using PoV steganalysis for different payload for Lena image



(a) Cover

(b) 20% embedded

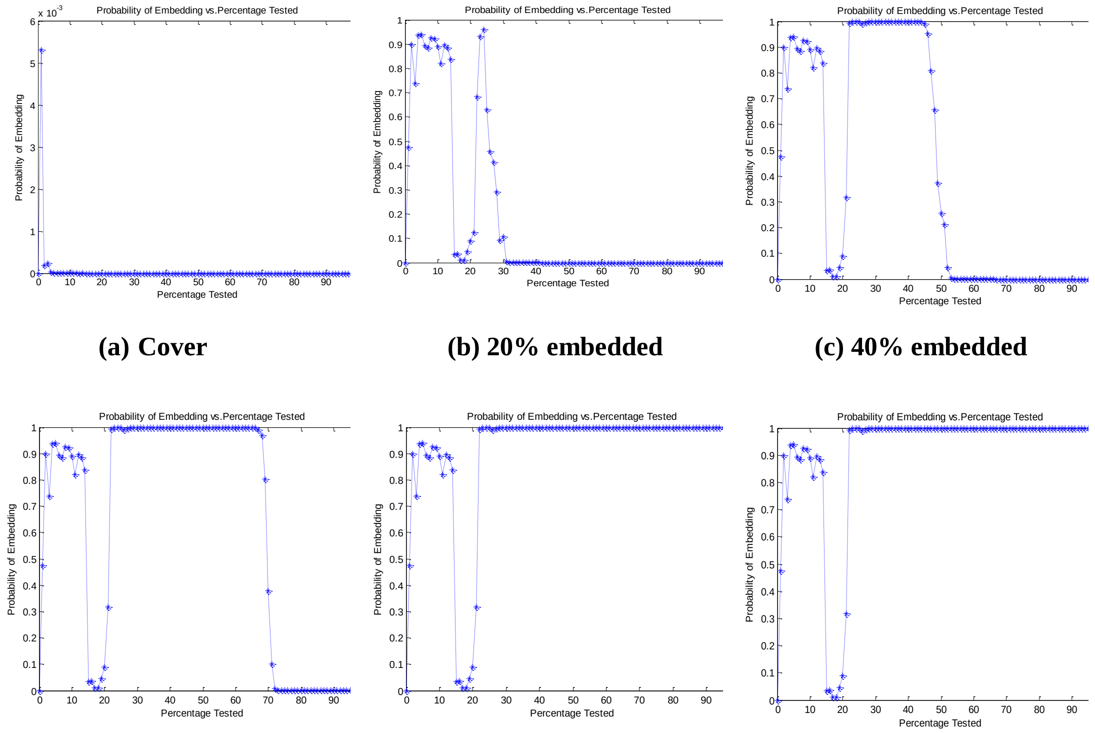
(c) 40% embedded

(d) 60% embedded

(e) 80% embedded

(f) 100% embedded

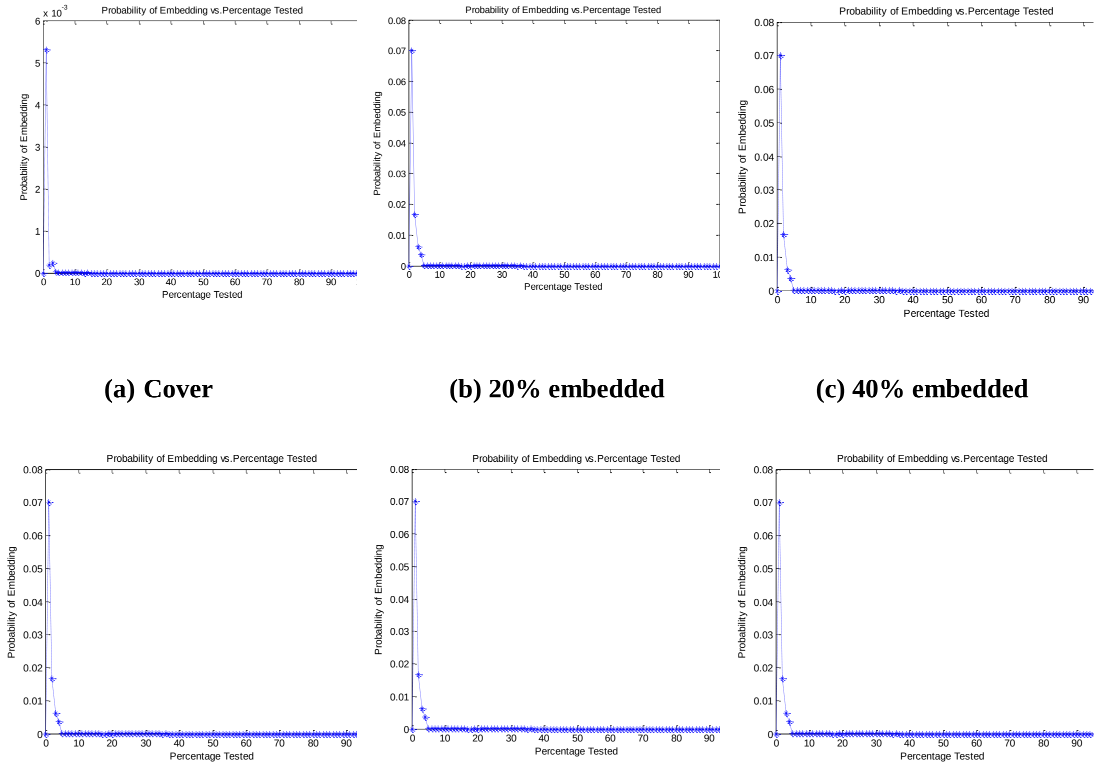
Figure A.4: SLSB-Witness detection using PoV steganalysis for different payload for Lena image



(a) Cover **(b) 20% embedded** **(c) 40% embedded**

(d) 60% embedded **(e) 80% embedded** **(f) 100% embedded**

Figure A.5: SLSB detection using PoV steganalysis for different payload for Camera man image

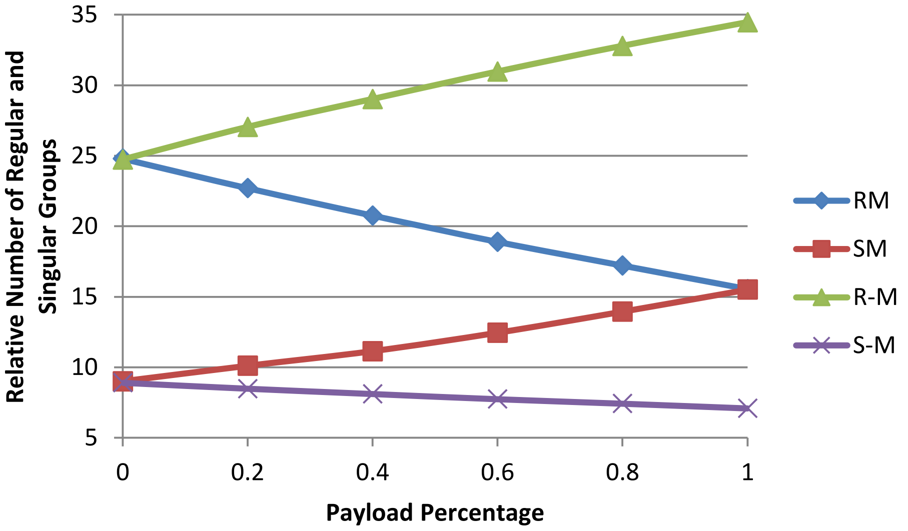


(a) Cover **(b) 20% embedded** **(c) 40% embedded**

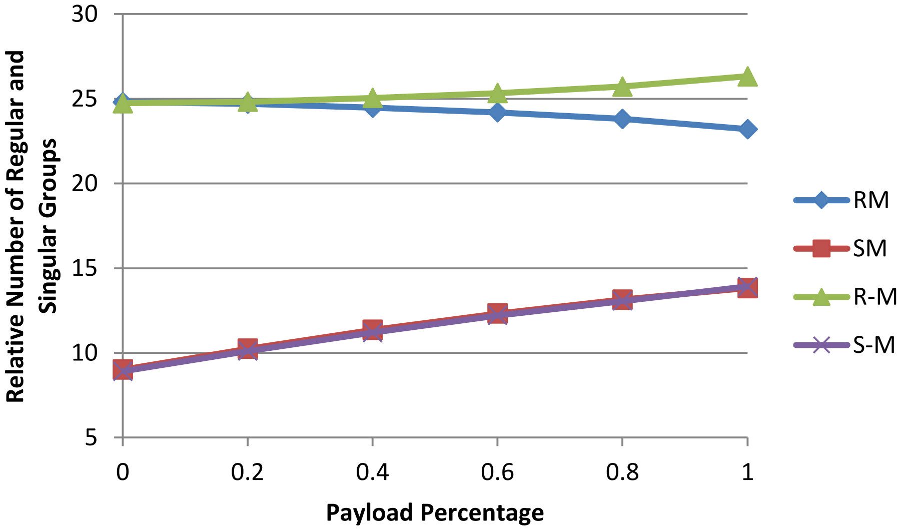
(d) 60% embedded **(e) 80% embedded** **(f) 100% embedded**

Figure A.6: SLSB-Witness detection using PoV steganalysis for different payload for Camera man image

B: Robustness against Regular and Singular (RS) Steganalysis Tool

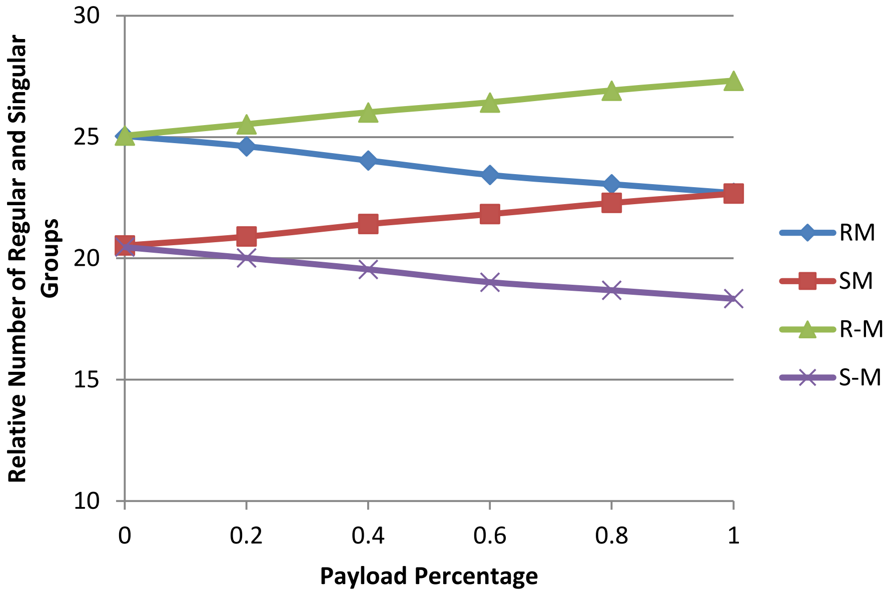


(a) Random LSB

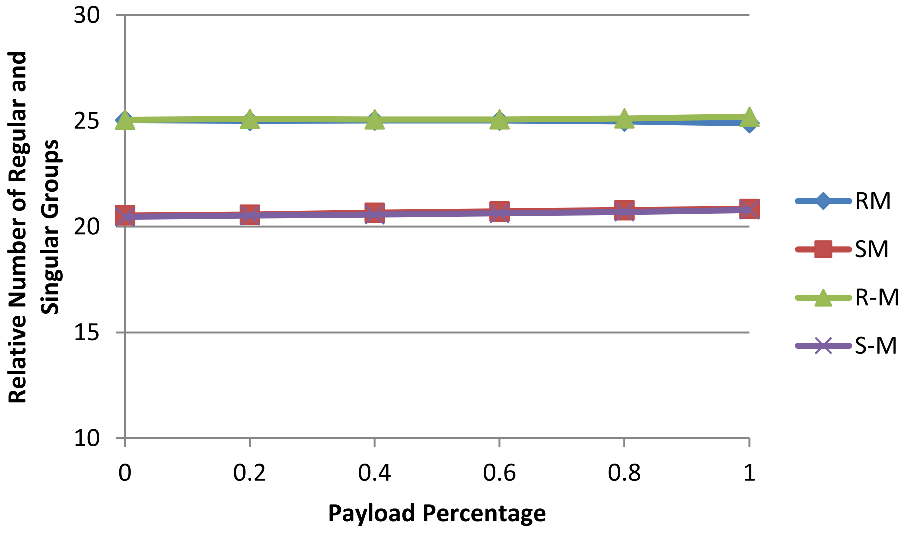


(b) Random LSB-Witness

Figure B.1: RS-diagram for different payload, Camera man image used

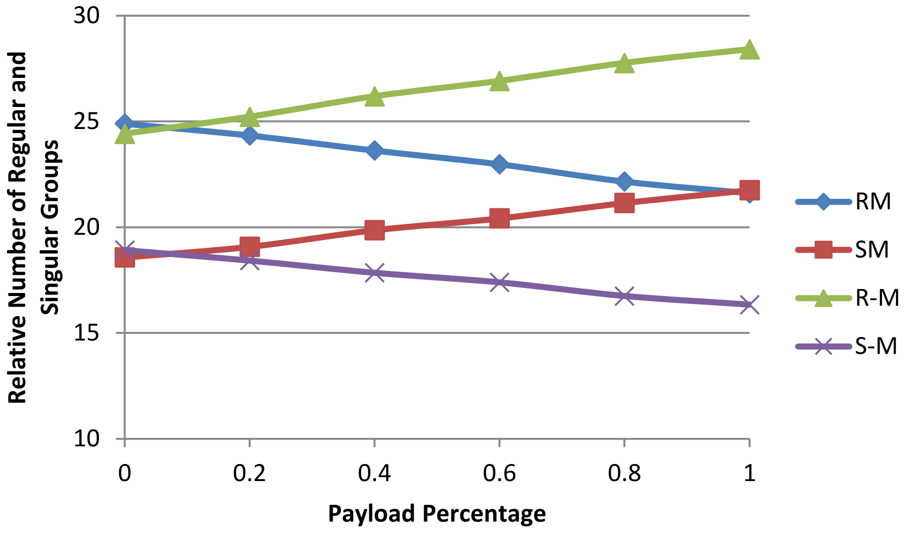


(a) Random LSB

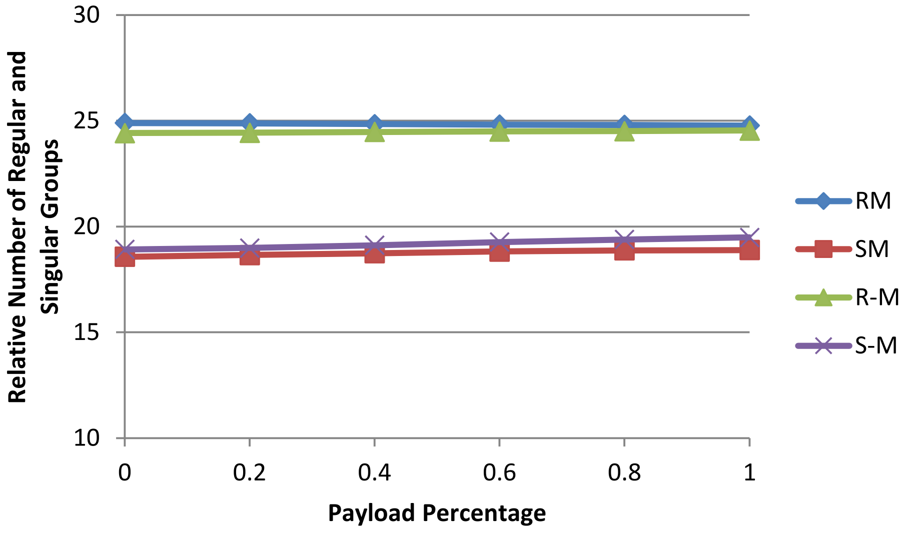


(b) Random LSB-Witness

Figure B.2: RS-diagram for different payload, Baboon image used



(a) Random LSB



(b) Random LSB-Witness

Figure B.3: RS-diagram for different payload, Living room image used

C: Face Recognition accuracy of 5 LBPH schemes compared with N8 scheme using 3 different protocols, 2 different databases (Yale and ORL), and 2 different wavelet subband blocking (3x3 and 5x5).

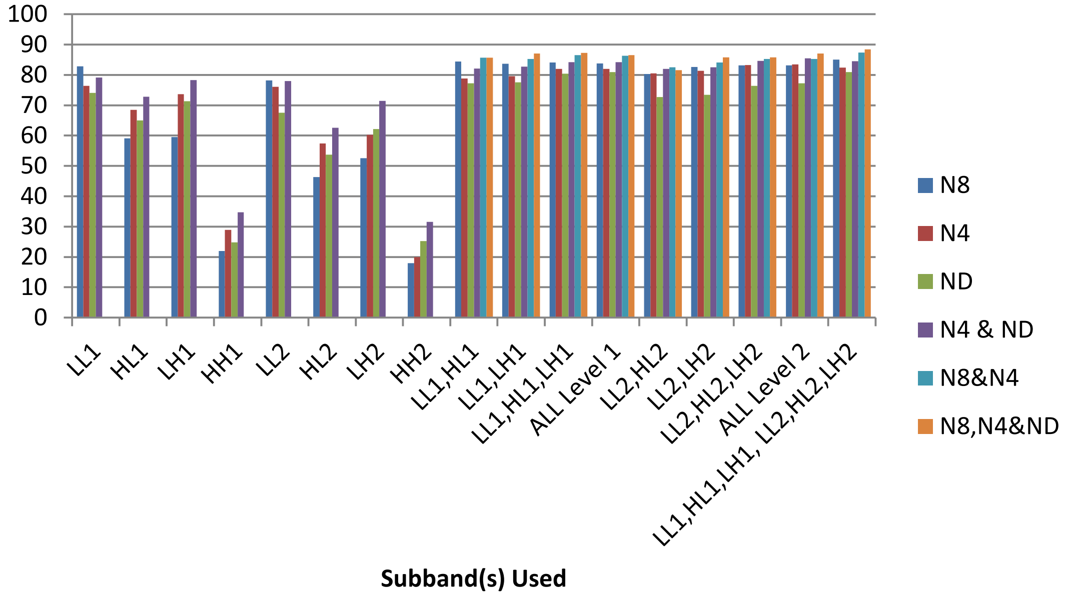


Figure C.1: Recognition rates (%) of Yale database for one training protocol and 5×5 blocking strategy

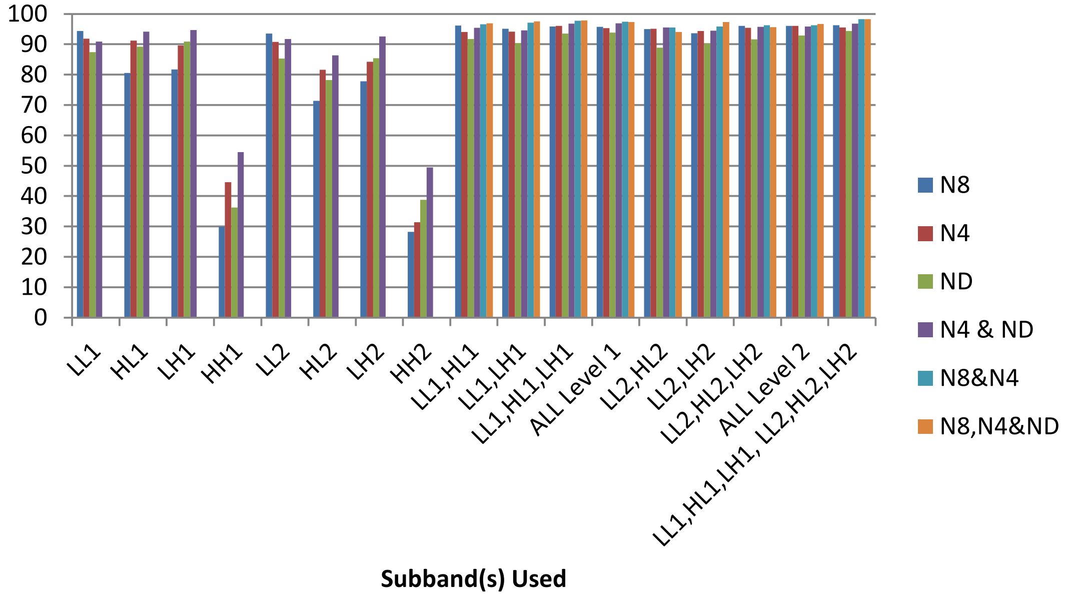


Figure C.2: Recognition rates (%) of Yale database for 50% training protocol and 5×5 blocking strategy

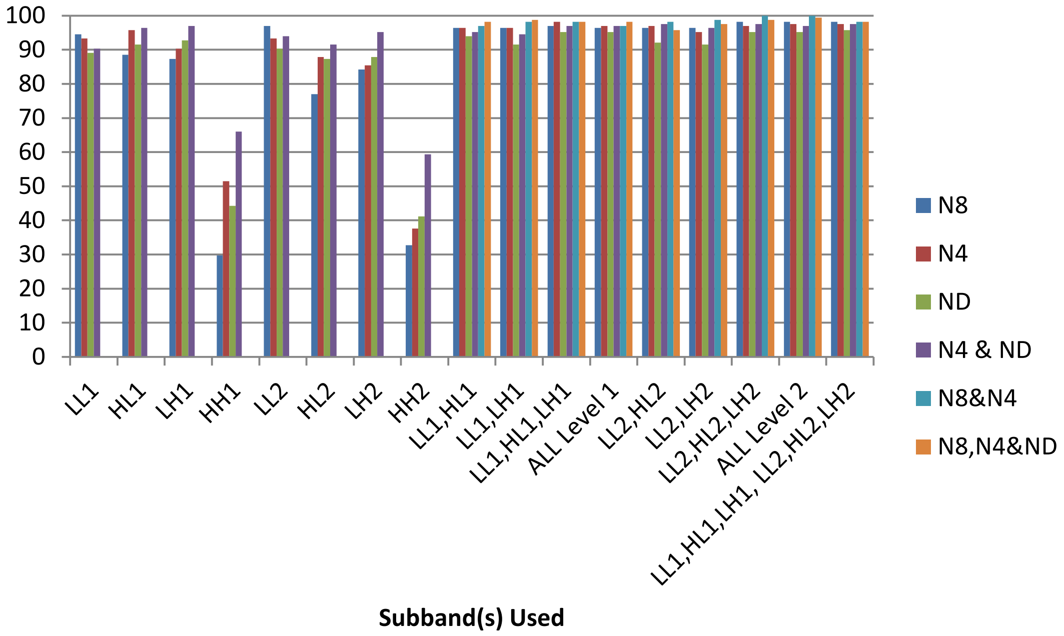


Figure C.3: Recognition rates (%) of Yale database for leave one out protocol and 5×5 blocking strategy

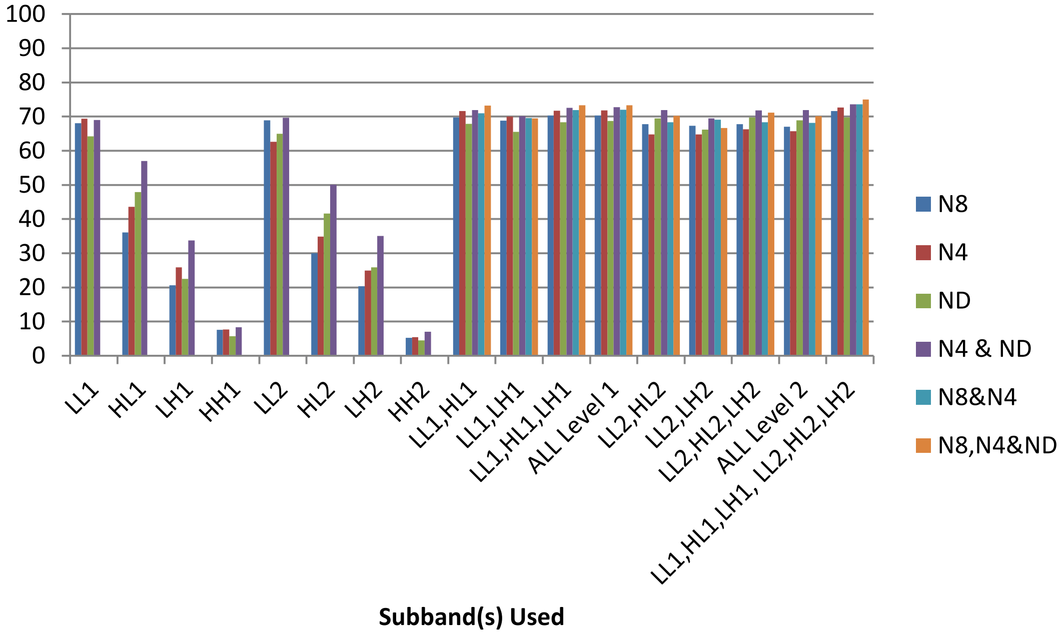


Figure C.4: Recognition rates (%) of ORL database for one training protocol and 3×3 blocking strategy

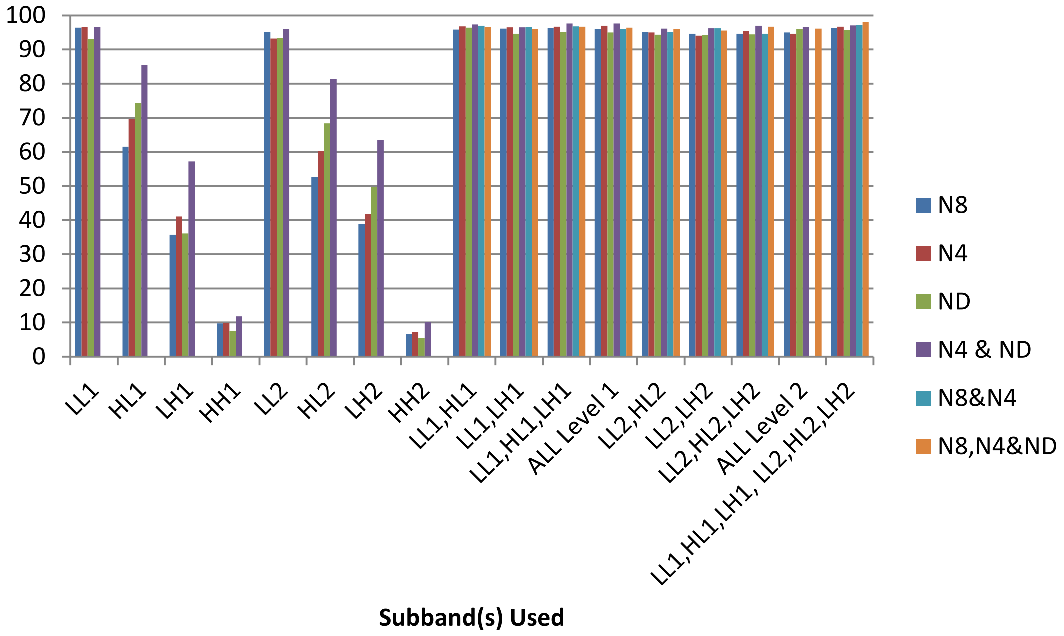


Figure C.5: Recognition rates (%) of ORL database for 50% training protocol and 3×3 blocking strategy

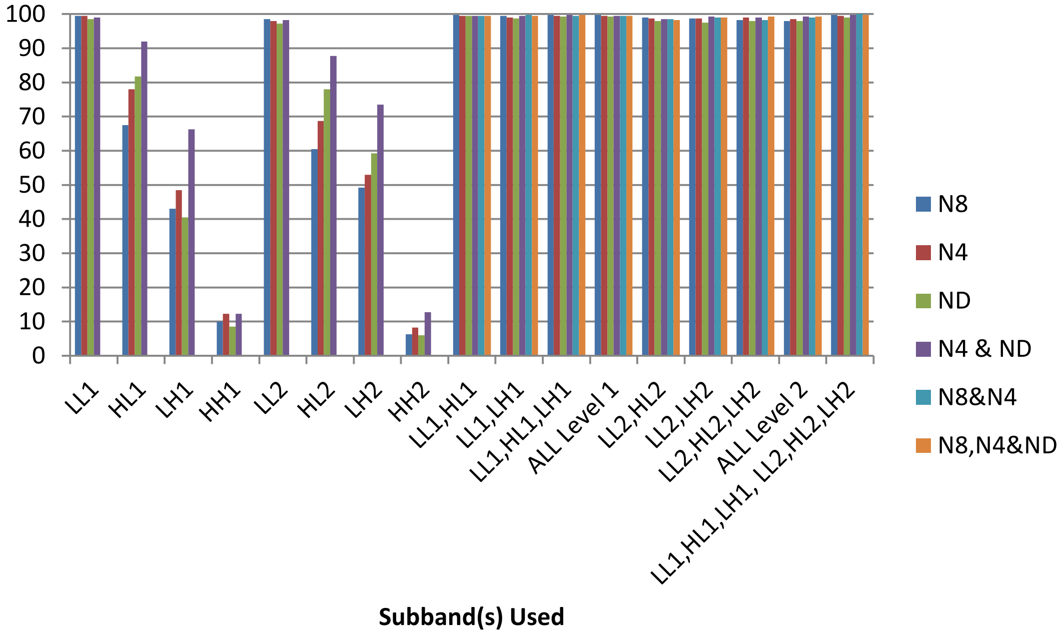


Figure C.6: Recognition rates (%) of ORL database for leave one out protocol and 3×3 blocking strategy

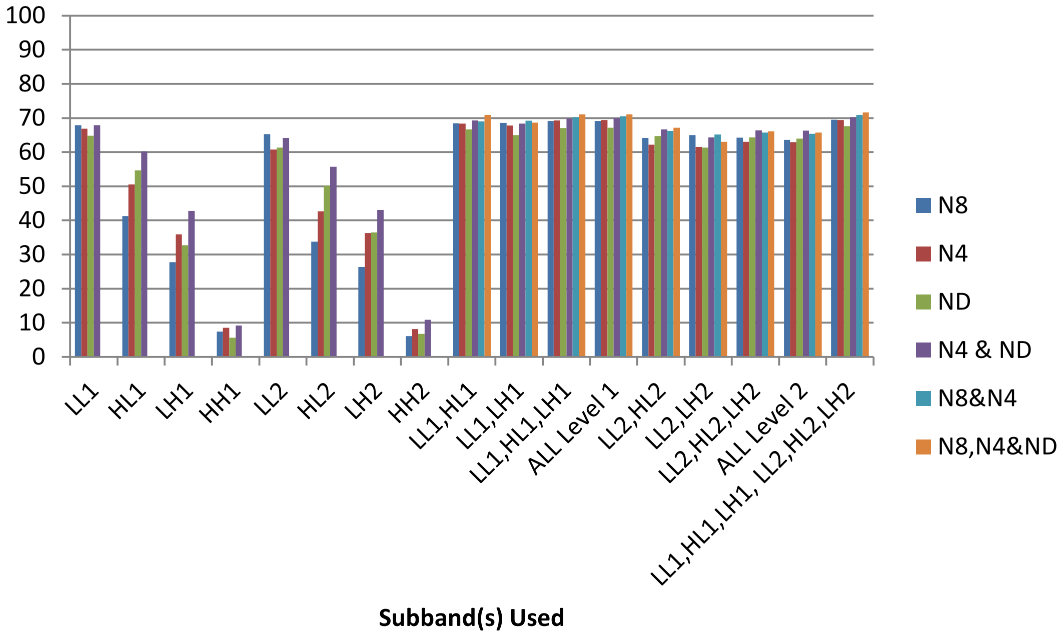


Figure C.7: Recognition rates (%) of ORL database for one training protocol and 5×5 blocking strategy

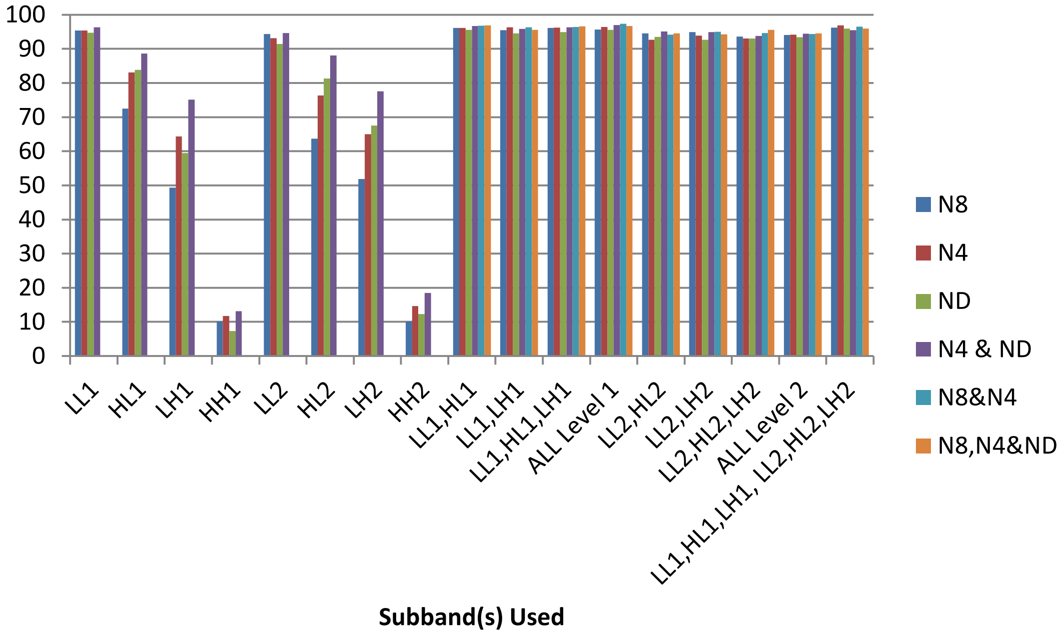


Figure C.8: Recognition rates (%) of ORL database for 50% training protocol and 5×5 blocking strategy

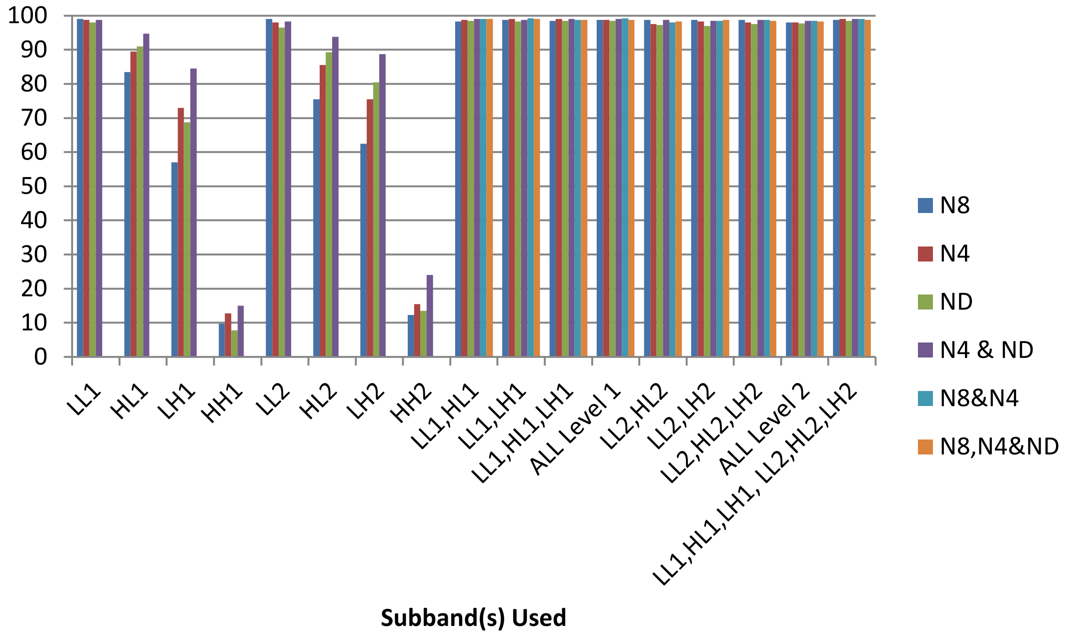


Figure C.9: Recognition rates (%) of ORL database for leave one out protocol and 5×5 blocking strategy