

**UNIVERSITY OF PORTSMOUTH**

**WATERMARKED FACE RECOGNITION SCHEME –  
ENHANCING THE SECURITY WHILE MAINTAINING  
THE EFFECTIVENESS OF BIOMETRIC  
AUTHENTICATION SYSTEMS**

**MOHD RIZAL BIN MOHD ISA**

**PhD**

**August 2016**

**UNIVERSITY OF PORTSMOUTH**

**WATERMARKED FACE RECOGNITION SCHEME –  
ENHANCING THE SECURITY WHILE MAINTAINING  
THE EFFECTIVENESS OF BIOMETRIC  
AUTHENTICATION SYSTEMS**

**MOHD RIZAL BIN MOHD ISA**

The thesis is submitted in partial fulfilment  
of the requirements for the award of the degree of

**Doctor of Philosophy  
of  
University of Portsmouth**

**August 2016**

## **ABSTRACT**

Biometric authentication systems provide alternative solutions to traditional methods that are based on knowledge (e.g. password) or physical tokens (e.g., smart card). Many studies now focus on getting high accuracy rates for biometric verification. However, with advances in technology, biometric data (e.g. fingerprint, face, iris) can be captured/sniffed, duplicated, modified, and then resubmitted in the same or in other applications that utilize the same biometric features.

Watermarking techniques can be used effectively to protect the genuine ownership of biometric data, either to accept or reject. This thesis presents a proposal for a suitable and viable combination of a face recognition algorithm and a watermarking technique, namely a Principal Component Analysis (PCA) and Discrete Cosine Transform (DCT) combination, that will ensure the authenticity of the data being transmitted in the face recognition system, which will then increase its level of security. The emphasis is on replay attack, which is recognizing and rejecting captured biometric data resubmitted into the system.

The research begins with an analysis of biometric systems, with an emphasis on face recognition systems, and in particular with reference to the recorded threats on such systems. Biometric watermarking algorithms proposed by previous researchers within the face recognition environment are then studied, noting their proposed solutions to the said threats. This would then give a good idea towards a watermarking scheme to be proposed to enhance the security of face recognition systems, especially in terms of the authenticity of the data being transmitted.

This proposed watermarking face recognition scheme is the main objective, which will be implemented in a PCA—DCT combination, followed by a check on all the 8 vulnerable positions where data may be captured and/or resubmitted. All the results produced are positive, apart from a few situations that will have to be left for future work. Non degradation of the individual PCA and DCT systems due to the combination is also checked and experimented on, again with positive results. Finally, the robustness

of the watermarking scheme is experimented on to evaluate its resilience against attacks.

The contributions from this research constitute a meaningful solution step to security problems associated with biometric techniques. The outcome of the research should also stimulate further research by opening up more research gaps in the area of combining biometric and watermarking techniques.

# **TABLE OF CONTENTS**

## **TABLE OF CONTENTS**

### **AUTHOR'S DECLARATION**

### **ACKNOWLEDGEMENTS**

### **DISSEMINATION**

### **LIST OF TABLES**

### **LIST OF FIGURES**

### **LIST OF ABBREVIATIONS**

<b>CHAPTER ONE: INTRODUCTION</b>	<b>14</b>
1.1 Background	14
1.2 Problem Statement	17
1.3 Research Aim	17
1.4 Objectives	18
1.5 Methodology	18
1.6 Scope	19
1.7 Main Contributions	20
1.8 Chapter by Chapter Summary	20
 <b>CHAPTER TWO: LITERATURE SURVEY</b>	 <b>22</b>
2.1 Introduction	22
2.2 Biometric Authentication Systems Model	22
2.3 Face Recognition	25
2.3.1 Advantages and disadvantages of face recognition	26
2.3.2 Face recognition approaches	27
2.3.3 Face recognition algorithms	29
2.3.4 Principal Component Analysis (PCA)	30
2.4 Biometric Authentication System Threats	35
2.5 Digital Image Watermarking	42
2.5.1 Generic watermarking system	43
2.5.2 Watermarking Properties	44
2.5.3 Watermarking Applications	47

2.5.4 Attacks on watermarks	48
2.5.5 The embedded watermark media in biometric systems	49
2.5.6 Watermarking techniques	50
2.5.6.1 Spatial Domain Techniques	50
2.5.6.2 Frequency domain techniques	51
2.5.6.2.1 Discrete Cosine Transform (DCT)	51
2.5.6.2.2 Discrete Wavelet Transform (DWT)	54
2.5.7 Encryption – Arnold Transformation	55
2.6 Previous Studies on Biometric Watermarking Techniques	56
2.6.1 Work on Biometric Watermarking Techniques	57
2.6.2 Work on the implementation of Watermarking in Face Recognition Systems	62
2.7 Conclusion	66
<b>CHAPTER THREE: PROPOSED WATERMARKED FACE RECOGNITION SCHEME</b>	<b>67</b>
3.1 Introduction	67
3.2 Analysis	
3.2.1 Face Recognition and Watermarking	67
3.2.2 DCT algorithm does not degrade the accuracy of PCA algorithm	70
3.3 Design	
3.3.1 Proposed watermarked face recognition scheme	73
3.4 Conclusion	82
<b>CHAPTER FOUR: IMPLEMENTATION, TEST AND EVALUATION</b>	<b>83</b>
4.1 Introduction	83
4.2 Experiment Set Up	84
4.2.1 Experiment 1 - Determining the frequency band for watermarking	85
4.2.2 Experiment 2 - Non degradation	87
4.2.3 Experiment 3 - System Rejection	89

4.2.4 Experiment 4 - Robustness	93
4.2.5 Experiment 5 -Comparative study of watermarking techniques	94
4.3 Validation - Experiments	94
4.3.1 General Modules	95
4.3.2 Experiment 1 - Determining the frequency band for watermarking	100
4.3.2.1 Implementation	100
4.3.2.2 Results	101
4.3.2.3 Discussion	105
4.3.3 Experiment 2 - Non degradation of PCA and DCT due to the combination	106
4.3.3.1 Implementation	106
4.3.3.2 Results	107
4.3.3.3 Discussion	108
4.3.4 Experiment 3 - Replay attack prevention – system rejection of captured data	109
4.3.4.1 Implementation	109
4.3.4.2 Results	110
4.3.4.3 Discussion	115
4.3.5 Experiment 4 - Robustness of the watermark scheme	115
4.3.5.1 Implementation	115
4.3.5.2 Results	116
4.3.5.3 Discussion	121
4.3.6 Experiment 5 - Comparative study of watermarking techniques	121
4.3.6.1 Implementation	121
4.3.6.2 Results	123
4.3.6.3 Discussion	127
4.4 Conclusion	127
<b>CHAPTER FIVE: CONCLUSIONS AND FUTURE WORK</b>	<b>128</b>
5.1 Summary	128

5.2 Contributions	129
5.3 Future work	131
5.3.1 Complementing current work	131
5.3.2 Future further improvement	132
5.3.3 Applications in other domains	133
5.4 Concluding remarks	133

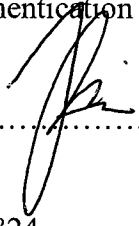
## **REFERENCES**

## **APPENDIX A - List of watermarking techniques on biometrics and their application domains**



## AUTHOR'S DECLARATION

Whilst registered as a candidate for the above degree, I have not been registered for any other research award. The results and the conclusions embodied in this thesis are work of the named candidate and have not been submitted for any other academic award.

Name of Candidate	:	Mohd Rizal Bin Mohd Isa
Candidate I.D. No.	:	630277
Programme	:	PhD in Engineering
Faculty	:	School of Engineering
Thesis Title	:	Watermarked Face Recognition Scheme - Enhancing the security while maintaining the effectiveness of Biometric Authentication Systems
Signature of Candidate	:	 .....
Word Count	:	37, 824
Date	:	August 2016

## **ACKNOWLEDGEMENTS**

I would like to seize this opportunity to pay tribute to all those who have contributed, one way or another, to the completion of this work, which marks another important milestone in my life.

I would like to express my profound gratitude and great indebtedness to Dr. Salem Aljareh, for his benevolent supervision of my doctorate thesis. I thank him for encouraging and believing in me. His continuous support and constructive criticism, his invaluable advice, guidance, as well as his understanding were of great value to me. But most of all, I thank him for his patience with me through the highs and lows of this research time.

Besides my supervisor, I would like to thank Prof. Dr. Zaharin Yusoff and Dr. Jacey-Lynn Minoi for their encouragement, insightful comments and guidances for the completion of this thesis.

I dedicate this thesis to my wife, Nor Elyana Bte Mohd Salan@Salleh, my supporting pillar, whose continual back-up and loving support was of great value in accomplishing this work. I also dedicate this thesis to my children (Nur Zahra Zuyyin, Muhammad Zihni Zubair and Muhammad Ziqry Zufar); watching you grow is the greatest pleasure in my life and raising you has taught me so much about life and about myself.

Last but not least, I wish to repay the debt of gratitude I owe my beloved parents (Mohd Isa Bin Mohd Samat and Waidah Ally), my mentors and teachers, my idols and my heroes; for years of encouragement and for their strong belief in me. I owe them great appreciation for what I have learned and what I have achieved. They were always there cheering me up and stood by me through the good times and bad.

## DISSEMINATION

### Conference Proceedings:

**Mohd Rizal Mohd Isa** and Salem Aljareh, “Biometric Image Protection Based on Discrete Cosine Transform Watermarking Technique”, *In IEEE Proc. of International Conference on Engineering and Technology (ICET)*, 2012 , pp.1-5.

**Mohd Rizal Mohd Isa**, Salem Aljareh, Zaharin Yusoff, Jacey-Lynn Minoi, “A Watermarking Technique to Improve the Security Level in Face Recognition Systems: An Experiment with Principal Component Analysis (PCA) for Face Recognition and Discrete Cosine Transform (DCT) for Watermarking”, *IEEE International Conference on Information and Communication Technology – 2016 (ICICTM’16)*.

### Journals:

**Mohd Rizal Mohd Isa**, Salem Aljareh, Zaharin Yusoff, “A Watermarking Technique to Improve the Security Level in Face Recognition Systems: An Experiment with Principal Component Analysis (PCA) for Face Recognition and Discrete Cosine Transform (DCT) for Watermarking”, *Springer Journal in Multimedia Tools and Application*, Accepted with minor amendments on 17<sup>th</sup> August 2016.

## LIST OF TABLES

<b>Tables</b>	<b>Title</b>	
Table 2.1	Typical applications of face recognition	25
Table 2.2	The attacks assessment rating on fingerprint recognition	37
Table 2.3	The evaluation factors on attacks with difficulty levels and rating points	38
Table 3.1	The 28 situations which need to be secured and protected	78
Table 4.1	The contents of captured data from position b to position g	89
Table 4.2	The main basis in experiment 4.2.3 - system rejection	90
Table 4.3	Detection rate for different frequency bands	103
Table 4.4	The SSIM index measurements for path 1 and path 2	107
Table 4.5	Rejected status on illegitimate presence of logo (at position a)	110
Table 4.6	Rejected status on timestamp does not tally (at position b)	111
Table 4.7	Rejected status on feature values do not match (at position d)	113
Table 4.8	Rejected status on logo does not exist (at positions a, g)	114
Table 4.9	Detection Rate after Attacks	116
Table 4.10	Face recognition rate comparison for Model 1, Model 2 and Model 3 under various attacks	124
Table 4.11	Watermark detection rate comparison for Model 1, Model 2 and Model 3 under various attacks	125

## LIST OF FIGURES

<b>Figures</b>	<b>Title</b>	
Figure 1.1	Typical components of a biometric system and vulnerable positions for interception and resubmission of data	16
Figure 2.1	Generic biometric authentication system	24
Figure 2.2	Architecture of a face recognition system	27
Figure 2.3	Schematic diagram of the image recognition process	31
Figure 2.4	The process of an image matrix conversion	31
Figure 2.5	The combination of all single vectors to vector matrix T	32
Figure 2.6	Watermark embedding	43
Figure 2.7	Watermark detection	44
Figure 2.8	DCT frequency regions	54
Figure 2.9	2 scale 2D Discrete Wavelet Transform	55
Figure 3.1	Image Processing	68
Figure 3.2	Watermark embedding and decoding processes	69
Figure 3.3	Watermarking and Image Processing	69
Figure 3.4	DCT does not disturb the accuracy of PCA	72
Figure 3.5	DCT and PCA do not degrade the accuracy of each other	72
Figure 3.6	Face recognition process	73
Figure 3.7	Watermarking in face recognition systems	74
Figure 3.8	The proposed watermarked face recognition scheme	75
Figure 4.1	Experiment 2- DCT and PCA do not degrade each other	88
Figure 4.2	Illegitimate presence of logo	91
Figure 4.3	Timestamp is no tally	91
Figure 4.4	Features value does not matched	92
Figure 4.5	Additional rejection - logo does not exist	93
Figure 4.6	Watermark embedding process	96
Figure 4.7	Quantization table recommended in the JPEG specification	97
Figure 4.8	Watermark extraction process	99
Figure 4.9	Face recognition accuracy rate comparison with each DCT frequency band under different strength value	102
Figure 4.10	The quality of the face image for different watermark strength	102

	values	
Figure 4.11	Comparison of face recognition and watermark detection rates for watermarks embedded in the low frequency bands	104
Figure 4.12	Comparison of face recognition and watermark detection rates for watermarks embedded in the middle frequency bands	104
Figure 4.13	Comparison of face recognition and watermark detection rates for watermarks embedded in the high frequency bands	105
Figure 4.14	Detection rate after Median Filter attacks	117
Figure 4.15	Quality of watermark image after Median Filter attacks	117
Figure 4.16	Detection rate after Gaussian Noise attacks	118
Figure 4.17	Quality of watermark image after Gaussian Noise attacks	118
Figure 4.18	Detection rate after Salt and Pepper attacks	119
Figure 4.19	Quality of watermark image after Salt and Pepper attacks	119
Figure 4.20	Detection rate after JPEG compression attacks	120
Figure 4.21	Quality of watermark image after JPEG compression attacks	120
Figure 4.22	Samples of various attacked images	123
Figure 4.23	Face recognition rate comparison with methods of Model 1, Model 2 and Model 3 under various attacks	126
Figure 4.24	Watermark detection rate comparison with methods of Model 1, Model 2 and Model 3 under various attacks	126

## LIST OF ABBREVIATIONS

1-D	One-Dimensional
2-D	Two-Dimensional
AC	Alternating Current
AFRS	Automated Fingerprint Recognition Systems
AT	Arnold Transform
CT	Contourlet Transform
DC	Direct Current
DCT	Discrete Cosine Transform
DE	Different Expansion
DWT	Discrete Wavelet Transform
HVS	Human Visual System
ICA	Independent Component Analysis
IDCT	Inverse Discrete Cosine Transform
JPEG	Joint Photographic Experts Group
LDA	Linear Discriminant Analysis
LSB	Least Significant Bits
MSB	Most Significant Bits
NC	Normalized Correlation
PCA	Principal Component Analysis
PSO	Particle Swarm Optimization
QIM	Quantization Index Modulation
QSWT	Qualified Significant Wavelet Trees
RDWT	Redundant Discrete Wavelet Transform
ROB	Region of Background
ROI	Region of Interest/Salient
SHA-1	Secure Hash Algorithm 1
SS	Spread Spectrum
SVD	Singular Value Decomposition
SVM	Support Vector Machine
TTL	Time to Live
UK	United Kingdom
WM	Watermark

# **CHAPTER ONE**

## **INTRODUCTION**

### **1.1 BACKGROUND**

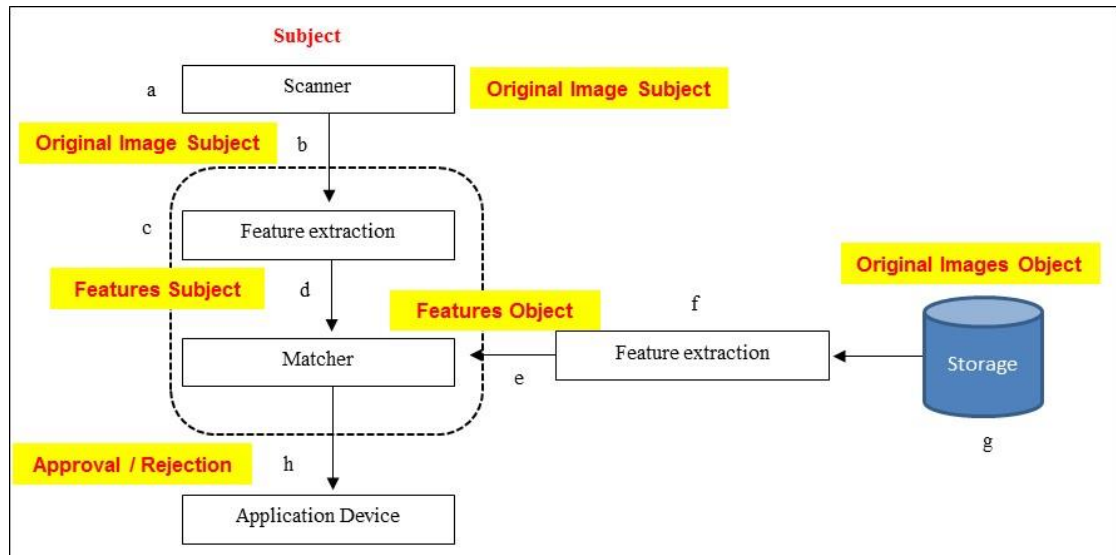
Information technology (IT) has revolutionised the present world and largely influence the way we exchange information. From the low pace and costly books, newspapers and magazines, the discovery of computers and the internet simplifies and speeds up the process of acquisition, publication, as well as the exchange of information for both commercial and non-commercial purposes. What is more, the new era introduces a more flexible and cost effective communication channel using the latest digital transmission technologies. However, the tremendous growth in IT is not without its demons as there are now security issues (Jain et al., 2002; Zhao et al., 2003; Mathivadhani et al., 2010), where the individual's information is now at risk of being illegally accessed by unauthorised users, duplicated and manipulated (Lin, 2000).

Recently, biometric technology in general, and face recognition in particular, has received significant attention. There are a number of reasons for this, the main one being its applicability in a wide range of commercial and law enforcement applications. The second important reason is the availability of possible solutions after almost 3 decades of research in this area, which has led to considerable improvements in the level of maturity of current recognition systems (Zhao et al., 2003). This success extends the variety of applications based on face recognition to include applications such as video games, virtual reality, training programs, human-robot interaction, human-computer interaction, driver's license, entitlement programs, smart card immigration, national ID, passports, voter registration, welfare fraud, TV Parental control, personal device logon, desktop logon, information security system security, database security, network and intranet security, internet access, medical records and law enforcement (e.g. suspect tracking and investigation), to name a few. However, the success of these systems is considered still limited and many applications are still far away from the capabilities of the human perception system.



Biometrics is a relatively new domain in information security technology (Jain et al., 2002). It determines the identity of a person based on his/her biophysical features (e.g. face, fingerprint, palm-print, and iris), or behavior features (e.g. signature, voice, and gaits). Various biometric systems have been developed during the past few decades, such as automated fingerprint recognition systems (AFRS), iris recognition systems, and face recognition systems, have been successfully deployed in a wide range of applications, including access control, attendance control, customs checking and others. Compared with traditional token based security systems, biometric systems are much friendlier and more difficult to cheat because the biometric traits are unique to every person and are permanent throughout his/her life.

Although biometric techniques often offer reliable methods for personal identification, biometric techniques do suffer from several security problems. Ratha et al., (2001) analyzed threats in biometric systems and listed them out into 8 vulnerable positions (refer to Figure 1.1), which will be discussed in more detail in the next chapter. An example of an attack may take place when the scanner captures the biometric traits and sends them to the feature extraction module for further processing. At this location, the transmission channel is vulnerable to several threats, such as eavesdropping attack, replay attack, man in the middle attack, and brute force attack. For example, during the raw data transmission between the said modules, the biometric traits can be intercepted and the attackers can 'replay' the biometric traits directly to the feature extractor and effectively bypass the scanner. Countermeasures to such attacks include transmitting data over encrypted channels, the use of symmetric or asymmetric keys, digital signatures, and Timestamp/Time to Live (TTL) tags.



**Figure 1.1:** Typical components of a biometric system and vulnerable positions for interception and resubmission of data

Figure 1.1 depicts the components of a typical biometric system, where the biometrics data of the subject captured by a scanner/sensor is to be matched with one of the authorized objects stored in a database. The core component is made up of a feature extraction module and a matcher that compares the features extracted from the subject and those from an object. A match will result in an approval status sent to the application device, else a rejection.

According to Ratha et al. (2001), there are attacks on a biometric system where data can be intercepted, manipulated, and then resubmitted into the system to achieve approval. In the case of a face recognition system, the sensor device is a scanner, and the object database is a facial database. More importantly, the figure 1.1 above identifies the vulnerable positions where data may be intercepted as well as resubmitted, namely the 8 positions a, b, c, d, e, f, g, h. The figure also shows the possible types of data that can be intercepted and/or resubmitted. Measures to increase the level of security of biometric systems will have to secure these 8 positions, both in terms of blocking entry, as well as to ensure the authenticity of the data being transmitted.

Indeed, in order to attain a more widespread utilization of biometric techniques, an increased level of security of biometric data is necessary (Ratha et al., 2001). Cryptography and watermarking are among the possible techniques to achieve this. Watermarking involves embedding information into the host data itself, so it can provide security even after detection (the watermark attached to the host data), in particular against tampering (Sridhar, Sattar and Mohan, 2014).

Recently, researchers have proposed algorithms based on image watermarking techniques to protect biometric data (Ratha et al., 2000; Gunsell et al., 2002; Jain et al., 2002; Jain and Uludag., 2003; Vatsa et al., 2004a; Kim et al., 2006; Salah et al., 2008; Rajibul Islam et al., 2008; Sabu and Ann., 2011; Bahsal et al., 2012; Isa and Aljareh., 2012; Kekre et al., 2015; Abdullah et al., 2015; Isa et al., 2016). In biometric watermarking, a certain amount of information, referred to as a watermark, is embedded into the original cover image using a secret key, such that the contents of the cover image are not altered. Some of these methods perform watermarking in the spatial domain (Gunsell et al., 2002; Jain et al., 2002; Jain and Uludag, 2003; Kim et al., 2006; Hoang et al., 2008; Yadav et al., 2011; Sabu and Ann, 2011; Zutao Zhang, 2011; Bahsal et al., 2012), while other methods embed the biometric watermark in the frequency domain (Ratha et al., 2000; Vatsa et al., 2004a; Vatsa et al., 2007; Rajibul Islam et al., 2008; Salah et al., 2008; Yan and Liu, 2010; Isa and Aljareh, 2012; Bedi et al., 2012; Behera and Govindan, 2013; Inamdar and Rege, 2014; Kekre et al., 2015; Abdullah et al., 2015; Isa et al., 2016).

A survey of the previous work listed has also shown that not all of the the 8 vulnerable positions of biometric systems have been thoroughly covered or secured, and as such there is still research to be done in some areas, especially in securing the data transmitted against replay attack. This will be discussed in more detail in Chapter Two.

## **1.2 PROBLEM STATEMENT**

The main problem is to find a suitable combination of a face recognition algorithm and a watermarking technique, ensuring that the combination will not degrade the performance of the individual systems, with the main objective being to increase the level of security of the face recognition system at the 8 vulnerable positions where data may be intercepted and/or resubmitted, in particular in terms of the authenticity of the data being transmitted.

## **1.3 RESEARCH AIM**

The aim of this research is to propose a watermarked face recognition system that is well-protected at the 8 vulnerable positions, especially against replay attacks, while at the same time maintain the face recognition rate and robustness against watermarking attacks (Median filter, Gaussian noise, JPEG compression and Salt & Pepper).

## **1.4 OBJECTIVES**

The problem statement leads to the following three research objectives, which will also define the main deliverables of this study:

- 1) To propose a suitable combination of a face recognition algorithm and a watermarking technique, and that the combination will not degrade the performance of the individual systems.
- 2) To propose a watermarked face recognition scheme that will ensure the authenticity of the data being transmitted in the face recognition system, in particular at the 8 vulnerable positions where data may be intercepted and/or resubmitted, and in doing so will increase the level of security of the face recognition system,
- 3) To propose a watermarked face recognition scheme that is robust against watermarking attacks (mainly signal processing attacks) especially Median filter, Gaussian noise, JPEG compression and Salt & Pepper attacks to ensure that the watermark cannot be easily removed.

## **1.5 METHODOLOGY**

This research begins with an analysis of biometric systems, with an emphasis on face recognition systems, and in particular with reference to the 8 threats that have been listed out by Ratha et al. (2001), Next, biometric watermarking techniques proposed by previous researchers within the face recognition environment are studied and classified according to their proposed solutions to the said threats.

The literature survey would then give a good idea towards a watermarked face recognition scheme to be proposed to enhance the security of face recognition systems, especially in terms of the authenticity of the data being transmitted. This proposed watermarked face recognition scheme is a major target.

Towards an implementation for validating the proposed watermarked face recognition scheme, the PCA (Principal Component Analysis) method, a holistic approach for face recognition, is chosen. For the watermarking system, the Least Significant Bits (LSB), Discrete Cosine Transform (DCT), and Discrete Wavelet Transform (DWT) techniques,

being representative of their respective approaches, are looked at to complement the PCA to enhance the level of security. An analysis is then carried out to show that the DCT performs the best, and a further analysis is carried out to ensure that the PCA—DCT combination will not degrade the performance of the individual systems.

The proposed watermarked face recognition scheme is then worked into the PCA—DCT combination, followed by a verification on the 8 vulnerable positions (of Figure 1.1) where data may be intercepted and/or resubmitted to ensure the authenticity of the transmitted data. From the 8 vulnerable positions, there are the 64 (8x8) possible situations, and it is found that some may not be relevant at all, many will be shown to be resolved (fully-protected), while the (few) remaining ones will have to be left for future work. The robustness of the proposed watermarked face recognition scheme will also be experimented on to evaluate its resilience against attacks.

As an experiment for the validation of the proposal, the three combinations of PCA—LSB, PCA—DCT, and PCA—DWT are implemented and compared, and the results are analyzed and discussed.

## **1.6 SCOPE**

In this study, only one face recognition algorithm is selected to combine with one of three watermarking techniques. Although this may seem quite limited, the algorithm and techniques chosen are considered representative of their respective approaches (being the most cited and considered the best), and it would at least set a new benchmark and reference for other implementations to follow.

PCA is one of the most used algorithms and has proven to be very effective for information compression in face recognition system. Furthermore, researchers have shown that PCA performs well in recognition when the training data set is small (which is the case in this thesis), and is very stable with different training sets (Jafri and Arabnia, 2009).

For the watermarking techniques, LSB, DCT and DWT are representative of their specific approaches. LSB is based on the Spatial Domain while DCT and DWT are both based on the Frequency/Transform Domain. In the frequency domain, coefficients are only slightly adjusted, which makes it more robust against geometric attacks such as

noise, scaling and others (Manoharan et al., 2010) as well as unnoticeable in terms of changes to the original image.

## **1.7 MAIN CONTRIBUTIONS**

The focus of the thesis is on complementing face recognition biometric systems with watermarking systems to increase the level of security. In doing so, it must be ensured that the combination of the two systems does not degrade the performance of either one, and that the level of security is indeed improved at all 8 vulnerable positions especially in maintaining the authenticity of the transmitted data against replay attack.

## **1.8 CHAPTER BY CHAPTER SUMMARY**

This research focusses on proposing a suitable combination of a face recognition algorithm and a watermarking technique as watermarked face recognition scheme that will ensure the authenticity of the data being transmitted in the face recognition system, which will then increase its level of security.

Chapter One introduces the problem domain leading to the advantages of complementing face recognition algorithm with watermarking technique to increase the level of security. The problem statement is derived from the presented arguments which then translates into the research objectives and defines the main contributions of the thesis. An outline of the methodology is provided as well as the scope.

Chapter Two outlines the literature on previous research in the problem area, with a brief review of face recognition systems and the security problems that may still arise. Watermarking systems are then explored as a means to increase the level of security, which will not only be in terms of the algorithms proposed, but also the watermarking techniques deployed in order to ensure the authenticity of the data transmitted within the face recognition systems. This will then highlight the main contributions of the thesis.

Chapter Three presents the core of the research, which gives the details of the proposed watermarked face recognition scheme in section 1.5 Methodology. The chapter proposes the PCA—DCT system as a suitable and viable combination of a face recognition algorithm and a watermarking technique, with minimal degradation in the performance of the individual systems. The chapter also details a watermarking technique using DCT that will ensure the authenticity of the data being transmitted in

the PCA face recognition system, in particular at the 8 vulnerable positions where data may be intercepted and/or resubmitted, thus increasing the level of security of the PCA face recognition system.

Chapter Four begins with a description of **the** experiment set up, followed by **an** explanation on the implementation of the experiments. The results for each experiment will be presented, analyzed and discussed. The five experiments for the validation of the proposal **are**: (1) Determining the frequency band for watermarking; (2) Non degradation of PCA and DCT due to the combination; (3) Replay attack prevention – system rejection of captured data; (4) Robustness of the watermark scheme; (5) Comparative study of watermarking techniques.

The main contributions and conclusions from this research will be summarized in Chapter Five. Possible future work will also be discussed either based on the constraints arising from this research or on improvements and extensions of the proposed approach.

# **CHAPTER TWO**

## **LITERATURE SURVEY**

### **2.1 INTRODUCTION**

In preparation to achieve the three objectives given in section 1.3, this chapter begins with an exploration of biometric systems, with an emphasis on face recognition systems, and in particular with reference to the 8 threats that have been listed out by Ratha et al., (2001). In addition, the most popular holistic approach for face recognition, namely the PCA, is singled out due its advantages over the others.

Biometric watermarking techniques proposed by previous researchers within the face recognition environment are studied and classified according to their proposed solutions to the said threats. The Least Significant Bits (LSB), Discrete Cosine Transform (DCT), and Discrete Wavelet Transform (DWT) techniques, being representative of their respective approaches, are looked at to complement the PCA to enhance its level of security. Particular emphasis is given to the DCT, as it is reported (Weilong, Meng and Shiqian, 2005) that it would probably perform the best.

The literature survey would then give a very good idea towards proposing a suitable combination of a face recognition algorithm and a watermarking technique as watermarked face recognition scheme to enhance the security of face recognition systems, especially in terms of the authenticity of the data being transmitted. These will be presented in Chapter Three, together with all the other components to meet the three main objectives listed earlier in Chapter One.

### **2.2 BIOMETRIC AUTHENTICATION SYSTEMS MODEL**

Biometric authentication systems have several advantages over traditional authentication mechanisms that are based on passwords or tokens (e.g. smart cards). Biometric technologies rely on the statistical analysis measurement from an individual's biometric traits to determine his or her identity. Since biometric authentication systems use individual biometric traits (fingerprints, iris, face, palm print, hand geometry, voice and others) that are essentially permanent to an individual as a means of authentication,

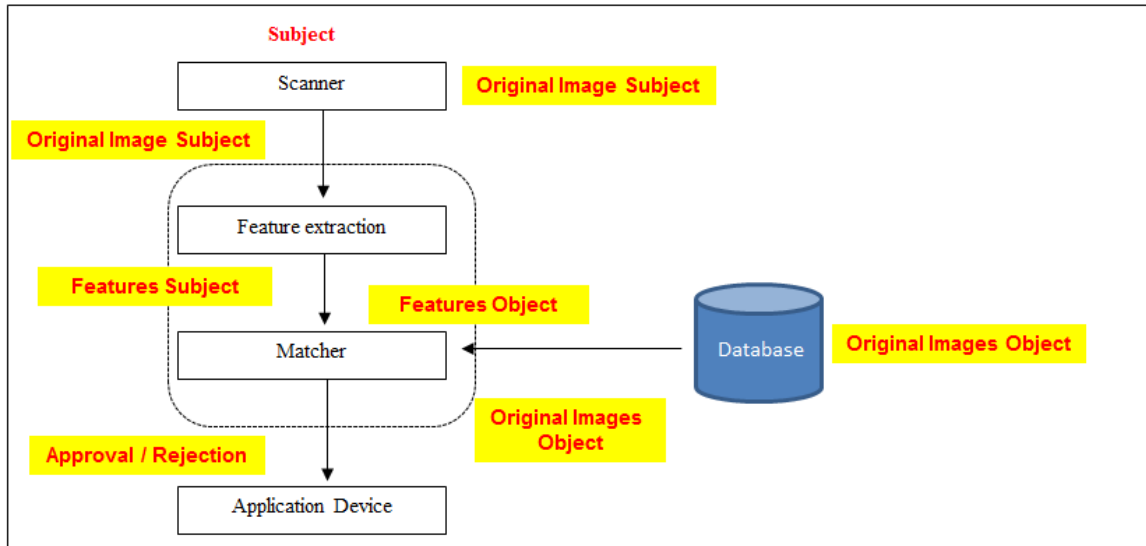


the systems provide a more reliable and much stronger factor of authentication compared to tokens and passwords.

A password (knowledge) is something a user (or a group of users) knows and supposedly no one else. The main drawback of passwords is the necessity to memorize the suitable combination of characters made up from uppercase and lowercase letters, numbers and symbols of at least eight characters long (SANS Institute, 2014). The password must be different for every system the user is registered for. Even though the number of possible passwords can be generated from eight characters, people tend to use easily guessed ones that are easier to memorize, such as the date of birth ('041180') or 'qwerty'. A poorly constructed password can be easily hacked by deploying brute force or dictionary attacks. Single sign-on services are now being offered to reduce the memorization load, but this is at the expense of trusting a single entity to provide strong security and respect your privacy.

A token (key) is something a user (or a group of users) has and again supposedly no one else. The basic principle of this factor/type is equivalent to requiring a key to unlock the door. It may refer to a physical device for authorized users of the service to facilitate authentication. The limitation of a token is that it may be lost or captured, with which attackers would easily be able to access the system without any knowledge of the authorized user or the system itself. On the other hand, should the token be lost or captured, the user would be physically aware of the missing token, thus the necessary procedures can be carried out to block the token from the authorized access list.

Biometric authentication systems do not have the disadvantages of the password or token system, as the authorization 'keys' are essentially derived from the biometric traits of the authorized user. In general, a generic biometric authentication system consists of five main modules: sensor, feature extraction, matcher, face database, and application device, as shown in Figure 2.1 and are discussed below.



**Figure 2.1:** Generic biometric authentication system

The scanner module is for capturing of the raw biometric data of the individual seeking to be authorized, which is in the form of an image, video or audio using a scanning or sensing device. Scanning/sensor devices vary for each biometric trait to be captured. There are also multimodal biometric systems, where two or more biometric traits are captured. For instance, a camera is used to capture the face image and subsequently a fingerprint device is used to scan the fingerprint of the person. The biometric samples will then be pre-processed in a controlled environment to remove noise, for image adjustments, and for sharpening due to variations from illumination effects. The treated biometric samples are handed over to the feature extraction module for further processing.

The feature extraction module extracts the salient features of the pre-processed images to obtain the relevant information using feature extraction methods designed for the selected biometric traits and specific applications. The resulting features are then sent to the matching module for further processing.

The matching module matches the extracted features of the person seeking authorization against a database of features of authorized users, referred to as biometric templates. The authorized users are pre-enrolled, where at the time of enrolment the same process as the above would be carried out and the extracted features are stored in the database alongside the user's identity to form the biometric template. At runtime, the matching module calculates a matching/similarity score to determine or verify the

identity of the user. A score above a certain threshold will result in an acceptance, else a rejection. This result is then sent to the last module, which is the application device (e.g. a door, a safe deposit box).

In the past 15 years, research on biometric systems has seen a very significant increase because of its high demand, and this is assisted with the availability of higher processing power due to advances in computer and communication technology. Researchers have developed advanced algorithms for recognition, such as for face, iris, fingerprint, voice, amongst others (Morizet et al., 2007). The focus in this thesis is on face recognition, although much of the results should also be applicable in other biometric systems.

## 2.3 FACE RECOGNITION

Face recognition systems are used for identifying individuals, and they have very much grown in demand due to the wide range of commercial use and for law enforcement, supported with the availability of more feasible technologies after 30 years of research (Zhao et al., 2003). Some applications include those listed in Table 2.1.

**Table 2.1:** Typical applications of face recognition

Areas	Specific Applications
Entertainment	Video games, virtual reality, training programs
	Human-robot-interaction, human-computer-interaction
Smart cards	Driver's license, entitlement programs
	Immigration, national ID, passports, voter registration
	Welfare fraud
Information security	TV parental control, personal device log on, desktop log on
	Application security, database security, file encryption
	Intranet security, internet access, medical records
	Secure trading terminals

Law enforcement and surveillance	Advanced video surveillance, CCTV control
	Portal control, post event analysis
	Shoplifting, suspect tracking and investigation

### 2.3.1 Advantages and disadvantages of face recognition

Face recognition offers several advantages over other biometric methods, such as:

- a) User involvement - face recognition can be done passively without the needs of users to stand in front of the camera, since recognition can be made from a distance with a long zoom range and an image stabilizer camera. However, the user needs to scan his thumb on a fingerprint device for fingerprint recognition, place his palm on a hand rest for hand geometry detection, or stand in a fixed position for iris or retina identification. The evasion of non-cooperation involvement from the user is beneficial for security and surveillance purposes.
- b) Data acquisition - extracted biometric data from hands and fingers can be considered useless if the skin tissue is damaged (e.g. bruised, cracked), iris and retina identification needs expensive equipment and is much too sensitive to body motion, signatures can be forged or modified, voice recognition can be disturbed by surrounding noises and others. On the other hand, facial images can be easily obtained through a simple setup and using inexpensive fixed cameras. Furthermore, there are also good face recognition algorithms with appropriate pre-processing techniques to tackle problems due to noise and slight variations in orientation, scale and illumination.
- c) Physical interaction – there are technologies that require multiple individuals to interact with each other (e.g. touching) or using the same device for capturing their biometric data, which would expose the individuals to transmissions of germs or viruses. Face recognition does not require any such interaction.

On the other hand, there are also drawbacks to face recognition. For example, the image acquired in an outdoor environment still remains one of the major difficulties due to changes of light illumination or the pose of the person (Zhao et al., 2003). It is quite clear that the current perceptibility of face recognition systems is still far inferior to human perceptibility for recognizing face images. Facial expressions also pose major problems, where even a big smile can make the recognition system become less

effective. As a result, Canada, for example, only allows for images with a neutral expression in passports (Passport Canada, 2012).

### 2.3.2 Face recognition approaches

According to Zhao et al., (2003), a generic face recognition process begins with the insertion of input images, through face detection, feature extraction, face recognition, and finally to verification, as shown in Figure 2.2.



**Figure 2.2:** Architecture of a face recognition system

The face image is first captured using a scanning device such as a camera. The captured face image is then put through the face detection process where it involves the separation of the face image into two regions, the salient region, which is the face area, and the background region. The goal of face detection process is to determine the existence of any face(s) in the image, and if found, to return the face area within the bounding box (Hatem, 2015). The face area is then pre-processed, where unwanted noise is removed and it is also normalized. After that, the feature extraction process extracts the important features of the face image, where the distinctive facial features are identified and extracted, possibly with the help of data compression techniques (which will be discussed more later on). Finally, the face recognition process gives the results of the recognition based on the matching status.

There are methods and techniques for each of the modules given in Figure 2.2, but for the moment the methods tend to depend on the underlying applications. For instance, image database investigations may require static sharp and clean images taken by a standard camera and the recognition would require a certain set of techniques, while video images would obviously require a different device and certainly a different set of techniques. As this research deals with static biometric data and not videos, the focus will be on face recognition methods for intensity images. The methods for this situation fall into two main categories: feature-based and holistic approaches (Brunelli and Poggio, 1993; Grudin, 2000; Heisele et al., 2003; Gottumukkal and Asari, 2004;

Jian et al., 2004; Ahonen et al., 2006; Neerja and Walia, 2008; Kumar et al., 2011; Fernandes and Bala, 2013; Kim et al., 2013; Jangid et al., 2015).

#### i) Feature-based approaches

Early work carried out on automated face recognition was mostly using featured based approaches. In essence, the first process is to identify and extract distinctive facial features from the image of the subject, such as the eyes, mouth, nose and others, and then the geometric relationship among those facial points are computed and converted into a vector of geometric features. Using these measurements, standard statistical pattern recognition techniques are then employed to match faces. Kanade (1973) was one of the earliest recorded attempts using such techniques. The author adapted simple image processing methods to capture a vector of 16 facial parameters made up of ratios of distances, areas and angles. He then used a simple Euclidean distance measurement for the matching module. Another well-known feature based approach was proposed by Wiskott et al., (1997) using an elastic bunch graph matching method, adopting Dynamic Link Structures (Lades et al., 1993) as part of the technique. Although this method was among the best performing ones in the FERET evaluation (Philips et al., 1996; Philips et al., 1997), it had quite serious drawbacks so much so that for the first 70 faces the graph placement had to be positioned manually before the elastic graph matching would become adequately dependable (Sukthankar, 2000). Other methods are based on the grayscales difference of unimportant components and important components, by using feature blocks, set of Haar-like feature block in the Adaboost method (Jones and Viola, 2003) to change the grayscales distribution into the feature. In the Local Binary Patterns (LBP) method (Shu et al., 2006), every face image is divided into blocks, where each block has its corresponding central pixel. Then the neighbouring pixels are examined. Based on the grayscales value of the central, a given pixel changes its neighbour's value to 0 or 1. Then a histogram is built for every region and the histograms are subsequently combined into a feature vector for the face image. Another technique is using the Gabor wavelets transform as feature extraction (Lim et al., 2009). The advantages of these methods are their concentration on important components of the face, such as

eyes, nose and mouth, but the drawback is that they do not represent the global structure of the face and its texture.

## ii) Holistic approaches

Holistic approaches use global information on face images rather than local features. These approaches can be subdivided into two groups: statistical and Artificial Intelligent (AI) approaches.

In statistical approaches, the image is represented as a 2D array of intensity values and the recognition is measured by comparing the input face and all the other faces in the database using direct correlation computation. Although this approach is simple to carry out, it only works under limited and controlled environments, such as equal illumination, scale, pose and others. The Principal Component Analysis (PCA) method and Linear Discriminant Analysis method are examples of statistical holistic approaches of face recognition.

Neural network and machine learning techniques are the use of some tools from AI to recognize faces. These would include the use of fuzzy logic backed by knowledge bases, or the use of neural networks, genetic algorithms, Hidden Markov models and others.

Our research is focused on protecting the face image against replay attacks within a holistic approach specifically for the PCA algorithm, which will be discussed further in the next section.

### **2.3.3 Face recognition algorithms**

Within the face recognition techniques, there are also various algorithms proposed for the various modules described earlier, namely for the pre-processing, feature extraction, and matching modules. Within these, according to Lu et al., (2003), two issues are central to all such algorithms, which are feature extraction for face representation, and classification of new face images based on the chosen feature representation.

Due to the abundance of research on face recognition algorithms (Jafri and Arabnia, 2009), this research will look at mainly the feature extraction component, and in particular, where the main objective is the representation for matching – and to look at

techniques that can introduce low-dimensional feature representation with enhanced discriminatory power for face objects. This is essentially because the main objective of the research is enhance security within face recognitions systems by embedding watermarks, and such embedding will have a major impact in the representation.

Within feature extraction, the Principal Component Analysis (PCA) and Linear Discriminant Analysis (LDA) are considered as two classic tools in appearance-based approaches for data reduction and feature extraction. According to Lu et al., (2003), LDA outperforms PCA as LDA focusses more on the most discriminant feature extraction. However, LDA may suffer “small sample size problem” (SSS) that occur in high dimensional pattern recognition.

#### **2.3.4 Principal Component Analysis (PCA)**

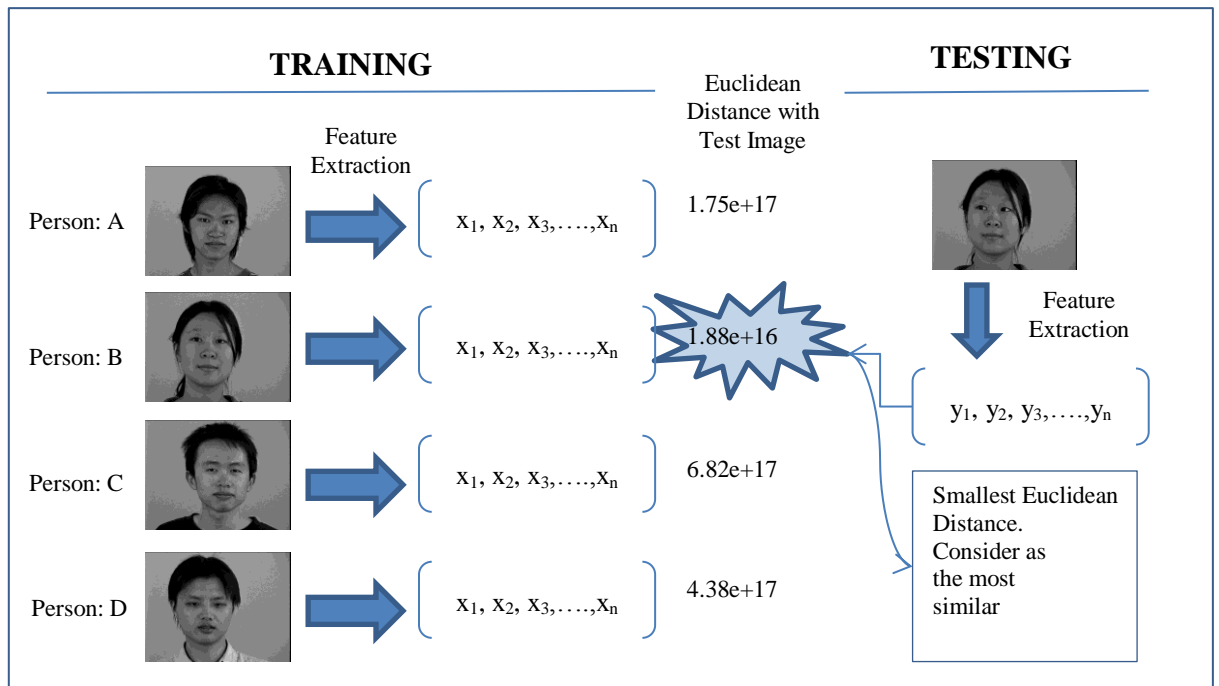
PCA is one the most successful techniques that have been used in image recognition and compression. PCA was first introduced in 1901 by Karl Pearson, and rapidly became a regularly used tool for data analysis exploration. It is a statistical method that uses factor analysis to reduce the dimensionality of the data space to a significantly smaller dimensionality of feature space. PCA is the basis of many techniques in data mining and information retrieval (Halko et al., 2010).

The PCA in face recognition consists of methods for calculating the mean, deviation, covariance, eigenvalue, eigenvector, eigenfaces and projection of the face space. There are three essential steps in PCA face recognition:

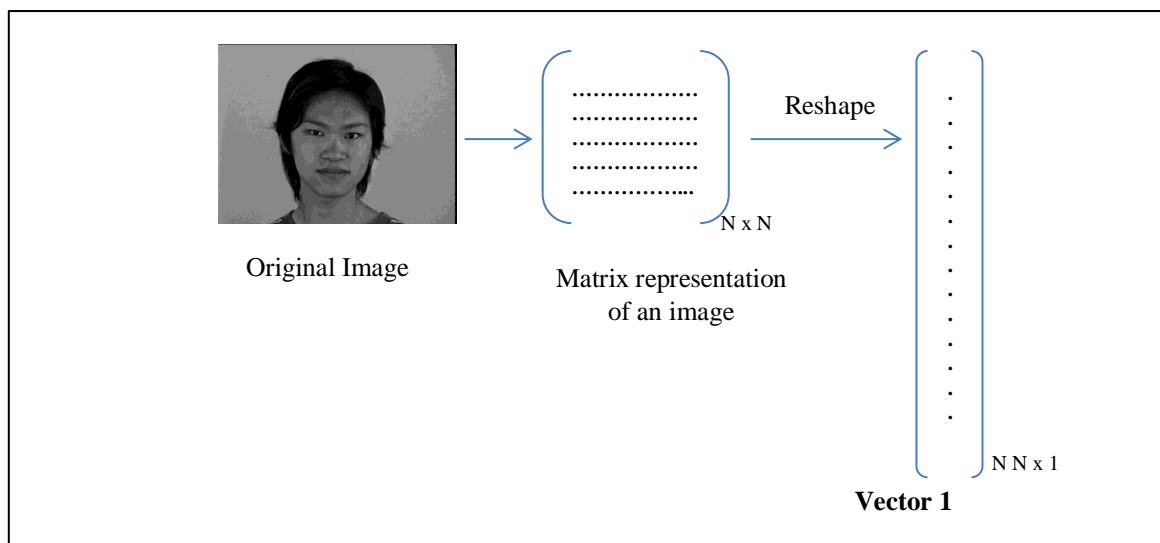
- a) Preparation of the database of authorized persons (Training phase)
- b) Preparation of a fresh image to be authenticated (Testing phase)
- c) Matching of (b) with an element of (a)

For (a), the following three figures illustrate the process, Figure 2.3 giving the overall picture. For each captured 2D image of an authorised person, the picture will be converted to a grayscale image, which is essentially a 2D matrix of pixels. The 2D matrix ( $N$ =rows,  $N$ =columns) will then be transformed into 1D vector matrix by reading column-by-column. Then all the resulting 1D matrices will be combined to become a large set of data (database).

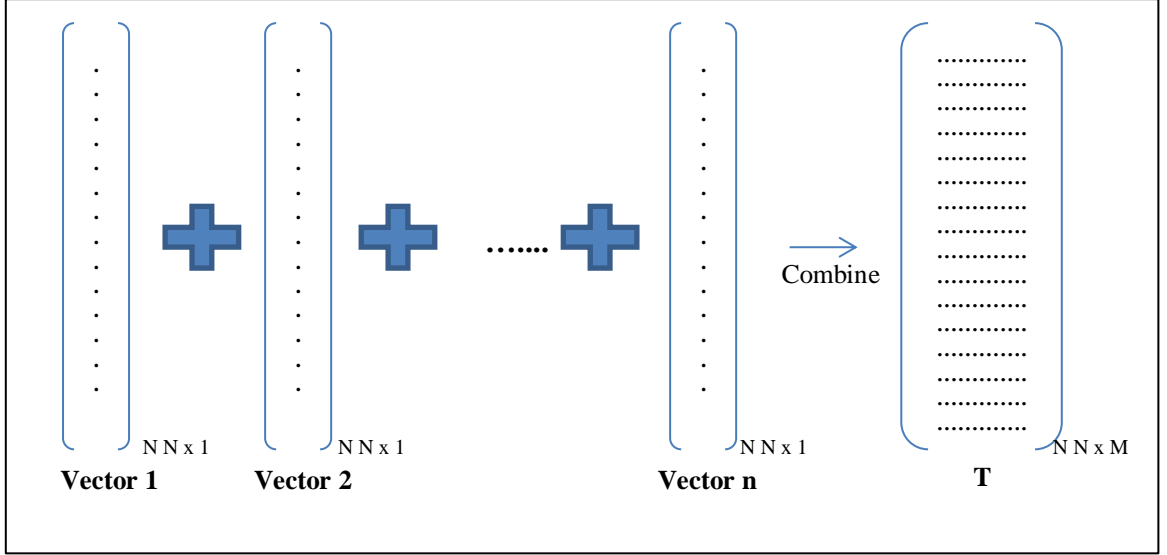




**Figure 2.3:** Schematic diagram of the image recognition process



**Figure 2.4:** The process of an image matrix conversion



**Figure 2.5:** The combination of all single vectors to vector matrix T

Suppose the total number of images =  $M$ , with each image  $i$  being represented by a vector  $\Gamma_i$ . The mean for each row is calculated and tabulated in a 1D vector  $\Psi$ :

$$\Psi = \frac{1}{n} \sum_{i=1}^n \Gamma_i \quad (1)$$

To get a set of vectors  $\Phi_i$ , subtract the mean face vector  $\Gamma_i$  minus  $\Psi$ :

$$\Phi_i = \Gamma_i - \Psi \quad (2)$$

The purpose of subtracting the mean image from each image vector is to be left with only the distinguishing features from each face and “removing” in a way information that is common to both. All the values of  $\Phi_i$  will be assigned to a new matrix  $A$ :

$$A = [\Phi_1 \Phi_2 \Phi_3, \dots, \Phi_n] \quad (3)$$

Then the covariance of the matrix  $A$  is computed using

$$C = AA^T \quad (4)$$

Note that the Covariance matrix has simply been made by putting one modified image vector obtained in one column each. Also note that  $C$  is a  $N^2 \times N^2$  matrix and  $A$  is a  $N^2 \times M$  matrix.

We now need to calculate the Eigenvectors  $\mu_i$  of  $C$ . However, note that  $C$  is a  $N^2 \times N^2$  matrix, and it would return  $N^2$  Eigenvectors, each being  $N^2$  dimensional. As this number is HUGE, the computations required would easily make the system run out of memory.

As such, instead of  $AA^T$ , consider the matrix  $A^T A$ . Recall that  $A$  is a  $N^2 \times M$  matrix, thus  $A^T A$  is a  $M \times M$  matrix. If we find the Eigenvectors of this matrix, it would return  $M$  Eigenvectors, each of Dimension  $M \times 1$ , which we call Eigenvectors  $v_i$ .

Now, from some properties of matrices, it follows that:  $\mu_i = Av_i$ . We had found  $v_i$  earlier. This implies that using  $v_i$  we can calculate the  $M$  largest Eigenvectors  $AA^T$ . Then recall that  $M \ll N^2$ , as  $M$  is simply the number of training images.

Find the best  $M$  Eigenvectors of  $C = AA^T$  by using the relation discussed above, namely:  $\mu_i = Av_i$ . Also keep in mind that  $\|\mu_i\| = 1$ .

Select the  $K$  Eigenvectors, where the selection is done heuristically. Now each face in the training set (minus the mean),  $\Phi_i$  can be represented as a linear combination of these Eigenvectors  $\mu_i$ :

$$\Phi_i = \sum_{j=1}^K w_j u_j, \text{ where } u_j \text{ are Eigenfaces.}$$

These weights can be calculated as:

$$w_j = u_j^T \Phi_i \tag{5}$$

Each normalized training image is represented in this basis as a vector.

$$\Omega_i = [\omega_1, \omega_2, \dots, \omega_k] \tag{6}$$

where  $i = 1, 2, \dots, M$ . This means that we have to calculate such a vector corresponding to every image in the training set and store them as templates.

We have thus found the Eigenfaces for the training images, their associated weights after selecting a set of the most relevant Eigenfaces, and have stored those vectors corresponding to each training image.

If an unknown probe face  $\Gamma$  is to be recognized, then:

1. We normalize the incoming probe  $\Gamma$  as  $\Phi = \Gamma - \Psi$ .
2. We then project this normalized probe onto the Eigenspace (the collection of Eigenvectors/faces) and find out the weights.

$$\omega_i = u_i^T \Phi$$

3. The normalized probe  $\Phi$  can then simply be represented as:

$$\Omega = [\omega_1, \omega_2, \dots, \omega_k]$$

After the feature vector (weight vector) for the probe has been found, we simply need to classify it. For the classification task we could simply use some distance measures. In the case where we use distance measures, the classification is done as follows:

Find  $c_r = \min \|\Omega - \Omega_i\|$ . This means that we take the weight vector of the probe we had just computed and find its distance with the weight vectors associated with each of the training image.

If  $c_r < \theta$ , where  $\theta$  is a threshold chosen heuristically, then we can say that the probe image is recognized as the image with which it gives the lowest score.

If however  $c_r > \theta$ , then the probe does not belong to the database.

The Euclidean Distance is probably the most widely used distance metric (Sharma and Vashisht, 2012).

$$\|x - y\|_e = \sqrt{|x_i - y_i|^2}$$

(7)

## **2.4 BIOMETRIC AUTHENTICATION SYSTEM THREATS**

In today's highly technical world, the mechanisms for determining the identity of an individual are vitally important in commercial as well as non-commercial applications. The implementation of biometric authentication systems could solve such problems with the use of user individual physiological (e.g., fingerprint, face, iris) or behavioral (e.g., body language, handwriting) as identification. However, there are still major challenges in biometric systems, which can be divided into two categories: external and internal factors.

External factors have the disadvantage of the lack of secrecy, such as face images which can be found literally anywhere on the internet, and fingerprints can be traced out on left objects. The privacy of biometric data can also be a concern in cross application usage, where the biometric data used in one system (e.g. company) may be used in another system (e.g. bank). As for internal factors, the vulnerabilities could come from the biometric system itself, where data may be intercepted, manipulated and then resubmitted back into the system to obtain approval. One main problem with external factors is that biometric authentication systems cannot guarantee that the biometric data in the authentication phase is coming from the same legitimate user as the one at the time of enrolment. The main issue for internal factors is somewhat similar as the systems cannot guarantee that the current data in the system (e.g. transmission between modules in a database) is from genuine users. This thesis focusses on internal factors, where the solution would be in protecting the biometric data throughout the system.

As explained earlier, biometric authentication systems offer many advantages in enhancing user convenience and robust security over traditional authentication schemes (tokens and passwords). However, they are still susceptible to various types of threats. Ratha et al. (2001) analysed these threats and listed them out into 8 vulnerable positions (refer to Figure 1.1).

### **a) Attacks at the scanner (position a)**

At this position, intruders may trick the system by presenting to the sensor a fake or dummy biometric trait, such as an artificial finger made from silicon to bypass fingerprint recognition systems, a face mask to deceive face recognition systems, or a

fake iris contact lens to cheat iris recognition systems. These types of attacks fall under the category spoofing attack.

Previous researchers have noted the success of identification using fake biometrics. Much work has been done on spoofing attacks using fingerprint traits (Putte and Keuning, 2000; Henniger et al., 2010), and surprisingly such attacks do not require any knowledge of the system, such as on the applied feature extraction algorithm, the matching algorithm, and even the user identity is not necessary. This type of attack is also often referred to as ‘zero effort attack’, and for that reason its frequency is rather high compared to others.

Putte and Keuning (2000) have done a thorough comparative study between the fake/dummy and real live fingers presented at the sensor for commercial fingerprint recognition systems. Experiments were carried out for two different approaches of capturing the fingerprint, of the real owner, with and without owner assistance. The authors used a plaster cast on the owner’s finger and then the cast is filled with silicone rubber to create a wafer thin silicon dummy. The dummy fingerprint can be easily glued to an attacker’s finger without being noticed by human eyes. In the second approach, the fingerprint was captured using a glass or a surface. As expected, the quality of the fingerprint dummy is much better without owner assistance. The experiment results showed that both dummy fingerprints can be accepted as a real finger.

Henniger et al., (2010) assessed potential attacks on fingerprint recognition. The authors used an attack tree for keeping track of the multitude of potential vulnerabilities. They noted that only a few fingerprint recognition products have achieved a security certificate level and even then only on a low Evaluation Assurance Level EAL2 (Canadian Communications Security Establishment, 2001; Australian Defense Signals Directorate, 2003; TÜViT, 2005; German Federal Office for Information Security, 2008; German Federal Office for Information Security, 2008), despite the fact that numerous guidelines on security evaluations have been developed, published and distributed (Common Criteria Biometric Evaluation Methodology Working Group, 2002; International Standard ISO/IEC 19792) and protection profiles (UK CESG, 2001; U.S. Information Assurance Directorate, 2007; U.S. Information Assurance Directorate, 2007; German Federal Office for Information Security, 2008; German Federal Office for Information Security, 2010; German Federal Office for Information Security, 2010).

As such, the authors conclude that efforts on evaluation towards security issues in biometric systems are still relevant for investigation. The evaluation is based on the following factors (International Standard ISO/IEC 18045):

- (i) Duration for an attacker to identify vulnerability, develop an attack method, and execute the attack;
- (ii) Technical expertise required;
- (iii) Knowledge of the target systems required;
- (iv) Tools required for identifying and exploiting the vulnerability;
- (v) Window of opportunity for the attack.

The authors evaluated a number of potential attacks using different methods. Table 2.2 presents the attacks carried out together with the corresponding evaluation rating based on the aspects given in Table 2.3 (International Standard ISO/IEC 18045).

**Table 2.2:** The attacks assessment rating on fingerprint recognition (source: Henniger, 2010)

Attacks	Time taken	Expertise	Knowledge of target system	Window of opportunity	Tools	Required attack potential	
						Sum	Rating
Construct a dummy from a given fingerprint image	1	3	0	0	4	8	Basic
By pass liveness detection	4	6	7	1	4	22	High
Capture a latent fingerprint from the touched surfaces	0	3	0	10	1	14	Moderate
Zero effort - use a real finger until reaches false acceptance	13-19	0	0	1	0	14-20	Moderate - High

**Table 2.3:** The evaluation factors on attacks with difficulty levels and rating positions  
(source: Henniger, 2010)

Factors	Level	Value
Time taken	$\leq 1$ day	0
	$\leq 1$ week	1
	$\leq 1$ month	4
	$\leq 3$ months	10
	$\leq 6$ months	17
	$> 6$ months	19
	Not practical	$\infty$
Expertise	Layman	0
	Proficient	3
	Expert	6
	Multiple experts	8
Knowledge of target system	Public	0
	Restricted	3
	Sensitive	7
	Critical	11
Window of opportunity	Unnecessary/unlimited	0
	Easy	1
	Moderate	4
	Difficult	10
	None	$\infty$
Tools	Standard	0
	Specialized	4
	Bespoke	7
	Multiple bespoke	9

The investigation shows that each attack contributes different potentialities. For instance, the attack potentiality for constructing fingerprint dummies from fingerprint images is rated as basic. This is because it is not difficult to implement the attack, as it only takes less than a week to construct fingerprint dummies and only rather simple proficient expertise is required for constructing the dummies. Other attacks, such as avoiding liveness detection, is rated high, as it is more challenging to carry out this



attack since knowledge of the target system is required. Such information is very sensitive, and it would probably need to involve help from insiders (persons involved in the development of the fingerprint sensors). It would also require a rather high level of expertise.

In face recognition systems, at position a, a printed face image (captured from social media applications and others) of an authorised person may be placed in front of the scanner (camera) to deceive the system and obtain a successful authorization. The captured face image captured from the scanner (possibly before a watermark is embedded) may also be used in an attack.

b) Attacks at the channel between the scanner and the feature extractor (position b)

An attack at position b may take place after the scanner captures the biometric trait and sends it to the feature extraction module for further processing. At this location, the transmission channel is vulnerable to several threats, such as eavesdropping attacks, replay attacks, man in the middle attacks, and brute force attacks. Countermeasures to these attacks include transmitting data over an encrypted channel, use of symmetric or asymmetric keys, digital signatures and utilization of Timestamp/Time to Live (TTL) tags. However, these countermeasures only protect the transmission channel but not the transmitted biometric data, e.g. an encrypted channel only protects the biometric data while in transmission, but once decrypted, the biometric data is no longer secure. Watermarking is one of the solutions to overcome this problem, as a hidden data may be attached to the biometric data without being destroyed.

c) Attacks on the feature extractor module (position c)

At this location, the resubmission of false data or component replacement may be forced by an attacker to produce pre-selected features for a successful authorization using a Trojan horse injected in the feature extractor module. A Trojan horse is basically a program that hides in a standard program in a system and will infect other files the system. A Trojan horse enables an attacker to control the system remotely and captures private information from the system through an online connection and may send imposter feature values to the matcher module. The counter measures for such attacks include creating strong and tested feature extraction algorithms with signed

components. The matcher module should be able to recognize that the extracted features are from the specific feature extractor module and not from elsewhere.

Position c attacks involve face feature values extracted from the face image. The captured face features from this location and from two other locations (positions d and e) cannot be resubmitted at positions a and b as the original face image, as they are in a non-reversible compression form, meaning that the extracted features cannot be reconstructed back to its original biometric image (James L Wayman et. al. 2005).

d) Attacks at the channel between the feature extractor and matcher (position d)

At position d, the feature values of an authorized user may be replaced by attacker selected values. This type of attack is similar to a position b attack (biometric traits captured for resubmission later on), except that here the attacker captures the feature values of an authorized user on the transmission channel between the feature extractor and matcher.

Adler (2003) reports on a specific user account being attacked using a face image synthesis technique. An initial face image is selected randomly, and then modified using the matching scores coming from the matcher that is generated for each previously successful face image. A weighted sum of Eigen-faces at each step that is generated from public domain face databases is added to the current candidate face image. The modified face image that leads to the highest matching score is given as input as a new candidate image. After a number of iterations for a modified face image, a sufficiently large matching score may be obtained.

In general, features values may be captured at three positions: positions – c, d and e. and resubmitted back at positions c and d. A mechanism is needed to ensure that the features values have not been tampered and at the same time will not disturb the originality of the features values.

e) Attacks on the matcher (position e)

Attacks at position e are similar to the type 3 attacks (position c), except that at this location the Trojan horse program is injected into the matcher module. The Trojan horse program enables the attacker to control the matcher module to produce high matching scores and eventually grants authorization to access the system. In addition, the attacker

may even be able to command the system to produce low matching scores or block authorized users from accessing the system and finally causing denial of service.

f) Attacks at the channel between the system database and matcher (position f)

This type of attack is similar to type 2 attacks (position b) except that the biometric images are intercepted between the system database module and matcher module. The attacker can capture, replace or alter the biometric images and resubmitted later. The resubmission of captured biometric image cannot be done at position g, since there is not much position, as it carries the authenticating data and not the data to be authenticated. However, the biometric image captured from this position may be resubmitted at positions a and position b.

g) Attacks on the system database (position g)

In biometric authentication systems, the authorized user biometric images are stored in the database system module. The main threat at this module is the attacker compromising the database security, such as reading or replacing biometric image(s). This can be due to unintended activity or misuse by authorized users, with design flaws and programming bugs in the database giving rise to various security vulnerabilities. Once the database has been exploited, the attacker can make adjustments to the stored biometric images, such as to add new unauthorized biometric images as genuine users, or to modify or remove existing images from the system.

As mentioned in (Skoric, 2010), unauthorized access to this module is among the most dangerous threats to users' privacy and security, and thus many researchers have focused on protecting the database, in particular with the use of watermarking techniques. In 2001, Hill demonstrated a method where a fingerprint image could be recreated based on the fingerprint template retrieved from database. The method is adapted from Sherlock and Monro (1993), which uses the location of singular points to estimate the orientation field of the fingerprint. Then the ridge patterns that pass through the minutiae points are generated using a line drawing algorithm. However, Ross et al., (2005) pointed out that several vendors of minutiae-based fingerprint systems disagreed that the template information could be regenerated to produce fingerprint images. The authors also showed that the minutiae templates are vulnerable to masquerade attacks and the orientations of fingerprint ridges can be predicted using the minutiae points.

They proposed an approach to exclude certain minutiae from the template that are critical for reconstructing fingerprint images without affecting the recognition performance. Furthermore, according to James L. Wayman et al. (2005), the extracted features are in a form of non-reversible compression, which means that the extracted features cannot be reconstructed back to its original biometric image.

Position g is indeed the core and one of the most vulnerable modules in biometric authentication systems. As with position f, the biometric images captured from this position could be resubmitted at positions a and b. A mechanism such as certificates, signatures and others is needed to ensure that the biometric images belong to this specific biometric system. If an attacker tries to submit his/her own biometric image, the system would then know that the biometric image is not part of the certified biometric images at position g. Furthermore, if the certified biometric images from position g is resubmitted at position a, they will be immediately rejected as the mechanism already exists and can be readily detected.

h) Attacks at the channel between the matcher and the application device (position h)

In position h, the attacker may intercept the results of the matcher at the transmission channel between the matcher and the application device (e.g. a door), either to accept or reject the user from accessing the system. The approval code may also be captured and resubmitted at this position at a later stage. For the moment, this type of attack is very difficult to protect against, but it is also extremely difficult to mount.

## **2.5 DIGITAL IMAGE WATERMARKING**

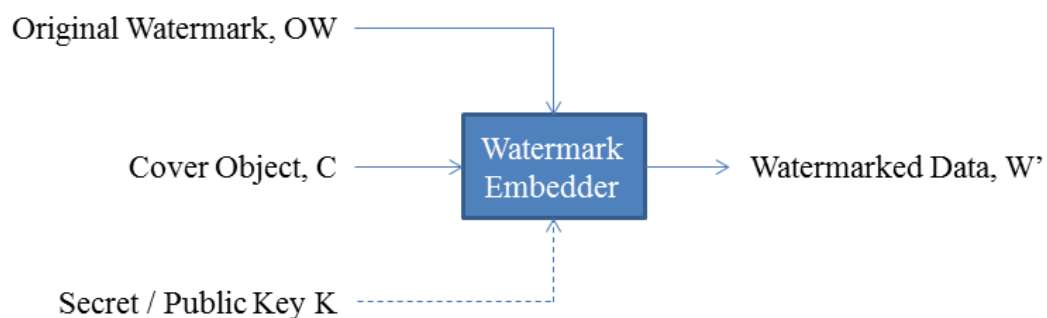
A watermark is defined as the imperceptible information embedded into a medium while integrity of that medium remains intact, while watermarking is the process of achieving this objective (Petitcolas et al., 1999). A typical example is the watermark used in banknotes. The concept of watermarking may also be referred to as a passive way of protecting data because it does not control access to the data – it only marks data by not destroying it.

Watermarking is also considered as data concealment or data hiding, a concept known from steganography, although steganography is mainly concerned with data hiding, whereas watermarking has stringent rules with concerns on securing the

embedded data and protecting it against removal and tampering. It provides a secure way of data transmission.

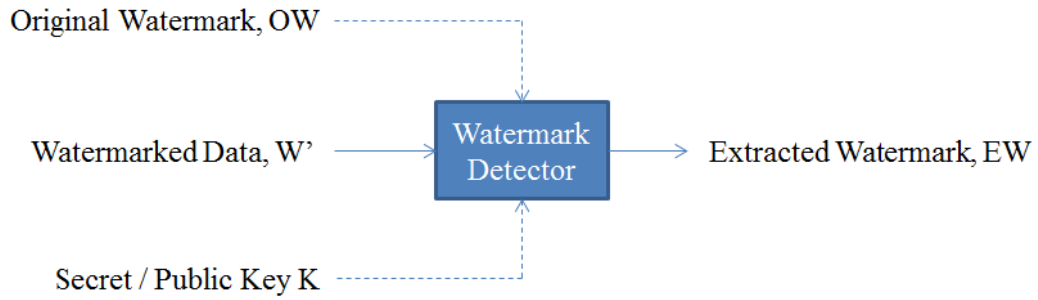
### 2.5.1 Generic watermarking system

In general, a watermarking system consists of an embedder and a detector. As illustrated in Figure 2.6 below, during the embedding process the original cover object  $C$  (e.g. image) and a watermark  $OW$  (e.g. text, logo image, audio) are combined together with an optional secret key  $K$  to generate the watermarked medium  $W'$ . There are several ways the embedding processes can be classified. The image, video, and audio watermarking techniques modify the cover medium in the spatial domain or in the frequency domain, or a combination in both domains. The watermarking techniques are described further on in section 2.5.6. The watermarked medium is then typically transmitted, recorded or shared for further processing.



**Figure 2.6:** Watermark embedding

In the detector process (see Figure 2.7), the watermarked medium is presented as an input to the watermark detector. Most detectors try to identify whether a particular watermark is or is not present in the watermarked medium. If a watermark is detected, a similarity measurement between the original watermark and the extracted watermark is computed to validate the ownership of watermarked medium.



**Figure 2.7:** Watermark detection

The watermark detection/extraction process can be divided into three categories:

- Informed/non-blind: the original medium as well as the watermark are needed for the retrieval process; it is also known as a private watermarking scheme, and it is for general purposes.
- Semi-blind: the original medium is not required for detection, but the detector needs access to some other information; it is also known as a semi-private watermarking scheme, and its purpose is mainly to find whether that the watermark can be detected, such as for copyright protection (ownership), copy control (i.e. as in DVD where copying is not allowed), and fingerprinting where the goal is to identify the original recipient of the pirated copies.
- Blind: does not require any reference to the original medium nor the watermark; it is also known as public watermarking scheme, and is the most challenging type of watermarking system, where it extracts in bits of the watermark data from the watermarked medium; it is mainly used for authentication purposes.

### 2.5.2 Watermarking Properties

There are three main properties of watermarking systems for digital images (Agreste et al., 2006):

#### a) Robustness

This property defines the watermark strength to adversary attacks. A watermark may be *fragile*, *semi-fragile* or *robust* based on the application needs. Fragile watermarks are designed to be distorted or ‘broken’ under the slightest changes to the cover image.

Semi-fragile watermarks are designed to break under all changes that exceed a user-specified threshold (a threshold of zero would form a fragile watermark). Robust watermarks withstand moderate to severe signal processing attacks (compression, rescaling and others).

There are a few methods of developing robust watermarking techniques, such as creating a dual watermarked image. In dual watermarking techniques, the cover image is protected using visible and invisible watermarks. The visible watermark is embedded into the cover image and the invisible watermark is added to it. Even if the visible watermark is removed, the invisible one would act as a backup. The other method is to add watermarks at different positions in the cover image, thus if one or two watermarks data are removed from the image then the other watermark would be there for validation.

A common method to create a robust watermarked image is by strategically determining the location of embedding the watermark. For example, in the DCT domain, the image is divided into three different frequencies – High, Middle and Low. The high frequencies are prone to compression and noise attacks. The low frequencies are more visible to human eyes, but are more robust to image processing attacks. Most researchers select the middle frequencies to balance both of these factors, although other reasons may indicate otherwise.

Another factor that may influence the robustness of a watermarked image is the size of the embedded watermark image. Smaller watermarks are easier to erase, whereas larger watermarks have more data values – if an attacker removes watermark data in one area, the watermark data in others area may still be left undisturbed.

Watermarks in the robust category are resistant to malicious and non-malicious distortions, covering common image processing operations (noise insertion, contrast adjustment, smoothening, cropping), compression (JPEG), and geometrical transform (rotation, scaling, translation).

#### b) Data Payload

Data payload is the number of watermark bits encoded within a unit of time or within a Work. For instance, for image, the data payload would refer to the number of bits

encoded within the image (Ingemar, 2008). This property evaluates how much hidden data can be embedded as a watermark so that it can remain detectable during an extraction process later on. The watermark can fall into two categories: the 1-bit or 'yes/no' watermark, and the multi-bit watermark. In the former, a single sequence is embedded into an image as the watermark and the watermark detector correlates the received image with this known sequence and compares the results against a threshold to decide whether a watermark is present or not. For the multi-bit watermark, the embedded watermark detection can be achieved by comparing the watermark bits to the given pattern. If all watermark bits match, then the watermark is detected.

### c) Imperceptibility

Watermarks may be visible or invisible depending on the desired applications. Visible watermarks are commonly used in ownership identification and for informing the public of the genuine owners of the cover images. However, such watermarks can be quite easily removed by attackers as the location of the watermark is visible, e.g. the BBC's logo is always displayed at the corner of the broadcasted television programs, small prints of copyrighted images are clearly displayed in popular magazines. Invisible watermarks are mainly used for proof of ownership and for fingerprinting applications. Such watermarks are much more difficult to remove as their location in the cover medium is unknown and can only be estimated by an attacker. The watermark can be imperceptibly embedded into the cover medium by slightly modifying the host signal.

An embedded watermark should not affect the quality of the cover image. It is usually preferred to have a watermarked image that is perceptually similar to the cover image. Watermarking should not introduce visible distortions as it degrades the aesthetic value of the watermarked image. Furthermore, the affected area might cause suspicion and a giveaway vulnerability for attackers. Some researchers use the terms fidelity or perceptual transparency for this property. Imperceptibility is the measurement of similarity between un-watermarked and watermarked images. The performance of imperceptibility for watermarking algorithms, in general, is calculated based on measures such as peak signal-to-noise ratio, mean square error, normalized cross correlation, and histogram similarity.



Again as with the more popular selection of the middle frequencies for robustness, for the popularly targeted low level of imperceptibility, other reasons may also indicate otherwise. Sometimes, the quality of the images to the naked eye may not be important if the images are always internal to the system and never presented to users, as long as the principal function of the system is effective. Watermarking in face recognition is a clear example of this, as the quality of the face image is not important as long as a high recognition rate is maintained and the security level is enhanced.

### **2.5.3 Watermarking Applications**

The main applications of digital watermarking include the following.

#### **a) Copyright protection**

Copyright material distributed over the untrusted network may be protected using watermarking. The owner can protect the data audio, image or video from being illegally commercialized. Copyright protection here concerns the identification of the specific content ownership in protecting the rights of the owner. Robust watermark is most suitable in this application, as any attempt to remove the watermark would result in a severe degradation of the image perceptibility. The ownership of the image can also be identified from the embedded watermark. In biometric systems, watermarking may also be used to validate the owner of the biometric data, where a watermark may be attached with the relevant information for identification.

#### **b) Fingerprinting**

Fingerprinting embeds unique information of the legal receiver in the image. Each distributed image is embedded with different watermarks allowing the owner to trace and monitor pirated images that are illegally obtained. Fingerprinting is quite similar to giving a barcode number to each product. Watermarking is an appropriate solution for this application as it can be invisible and is always attached to the image (Kougianos et al., 2009). If any illegal copy of an image is found, the source of the illegal copy can be traced back using the watermark extracted from the image. A robust watermark is required for this application, as the watermark has to survive many malicious and non-malicious distortions.

### c) Image and content authentication

Image authentication is mainly associated with content integrity. The main objective of this application is to detect any modification on the original image. Fragile watermarking is suitable for this application, as any tampering and modification to the original image can be readily detected from the 'broken' watermark. Furthermore, the watermark is designed to be destroyed such that the tampered regions and how much it is altered can be determined (Zeng and Liu, 1999; Tian, 2003).

#### **2.5.4 Attacks on watermarks**

There is a variety of possible intentional and unintentional attacks on watermarking systems. The attacks can be classified into five different categories as listed below (Kundur and Hatzinakos, 2001; Cox et al., 2008):

- a) Signal processing operations – The attackers intentionally subject the watermarked image with various operations such as cropping, scaling, filtering, and compression to destroy the watermark data.
- b) Removal and interference attacks – The attackers attempt to remove or destroy the watermark data with additional noise, given that watermarks usually contain some noise in the host signal. Lossy compression, quantization, collusion, de-noising, re-modulation, averaging, and noise storm are examples of this category of attacks.
- c) Geometric operations – The main intention of these attacks is to manipulate the watermarked image in a certain way such that the detector would not be able to find the watermark data. If the watermarked image survives affine transformations such as rotation, translation, and scaling, the watermarking scheme is resistant to geometric attacks.
- d) Cryptographic attacks - These attacks involve cracking the security installations in the watermarking scheme that are different from removal and geometric attacks. An example is searching for the secret key using brute force and embedding misleading watermarks.
- e) Protocol attacks - The attackers exploit the loopholes in the watermarking technique, such as to remove the watermark from the watermarked image and thereby claiming ownership. One known example of such an attacks is the IBM (Friedman, 1993) attack,

also known as the deadlock attack, inversion attack, or fake-original attack. This attack embeds extra fake watermarks to deceive the detector from being able to certify the original watermark.

### **2.5.5 The embedded watermark media in biometric systems**

In a watermarking environment, the embedded watermark media plays an important role to protect the original image. Various types of watermark media have been considered in biometric systems for different purposes depending on the application – for example, the use of watermarks as secondary authentication, or as a mechanism in protecting the ownership of biometric images. We give below some of the embedded watermark media that have been used in biometric systems. Further details are given in Appendix A.

#### **a) Text**

Text is a common embedded watermark media in a watermarking environment. For example, (Sabu and Ann, 2011; Isa and Aljareh, 2012) have adapted text to be used as an additional authentication step to protect biometric images.

#### **b) Biometric image or feature value**

Many embed a biometric image or a feature value as a watermark especially in multimodal biometric authentication systems (Bedi et al., 2012; Behera and Govindan, 2013; Kekre et al., 2015; Abdullah et al., 2015). The main purpose of such biometric watermarking schemes are to hide the owner's additional biometric data and later to be extracted for verification during the authentication process.

#### **c) Demographic image**

A demographic image is made up of information related to the owner of the biometric image, such as name, id number, phone number, etc., to be used for ownership protection. For example, (Behera and Govindan, 2013) proposed embedding a demographic image together with fingerprint information as watermarks in their work as additional authentication.

As far as we have surveyed, none has so far implemented a timestamp as the embedded watermark media to protect the data transmitted against replay attacks. This will be one of our main contributions in this research.

### **2.5.6 Watermarking techniques**

Watermarking is a process of embedding, into any form of information, digital signal that cannot be easily removed (Syed, 2011). Bamatraf et al., (2011) puts watermarking as a pattern of bits embedded into the digital image, audio and video signals to specify the file's copyright information. Today, with the emergence of the internet and other electronic file transfer systems, user information can be easily altered without the author's consent (Huang et al., 2010). It is thus important to protect the original medium against altering or tempering, whereupon watermarking may be attached to the original work for copyright control and others.

Over the years, a number of watermarking techniques have been developed, and they can be categorized into two main types – Spatial Domain, and Frequency domain.

#### **2.5.6.1 Spatial Domain Techniques**

The watermark embedding process in the spatial domain involves the manipulation of the least significant bits of the multimedia content (Cox et al., 2002). The pseudo-random number traversing method or a spread spectrum method can be used together with a key to disperse its spatial locations. The modified watermark can then be united with the content after applying a weighting factor that ensures robustness of the watermark as well as its imperceptibility.

Although spatial domain watermarking is simpler to implement, and usually involves minimal computational complexity, its lack of robustness against many attacks (such as compression, blurring, cropping, and others) make it unfavourable as a watermarking scheme. Furthermore, spatial domain watermarking does not exploit the properties of the cover image, which can significantly help with the robustness of the watermark.

Arguably the most effective, widely used, and certainly the simplest spatial domain technique is the Least Significant Bit (LSB). In computing terms, LSB is the bit position in a binary integer that is located at the rightmost end, which can determine whether the number is odd or even. In contrast, the Most Significant Bit (MSB) is the bit position

that is located at the leftmost end, which determines whether the number is negative or positive (Support, 2002).

According to Sharma et al., (2012), LSB can survive image cropping, but when it comes to the addition of noise and lossy compression, the watermark may be easily defeated. Nonetheless, the attack is somehow not significant on the perceptibility of the cover image. There is an improvement on basic LSB substitution by using a pseudo-random number generator to determine the pixels that would be useful for embedding, resulting in the watermark being secure from a third party (Sharma et al., 2012). LSB has proven to be a simple and quite powerful tool for steganography but still lacks robustness for watermarking (Shoemaker, 2002).

In a paper by Bamatraf et al., (2011), another method of LSB watermarking is proposed, with an inversion of the watermark text and embedding it in a different order of the LSB. By doing this, no one would expect that the hidden watermark text is in a different order, and the operation comes with its inverses.

#### **2.5.6.2 Frequency domain techniques**

Watermarking in the frequency domain exploits the properties of the cover image, essentially based on the imperceptibility of the watermarked image and the robustness of the embedded watermarks. The human visual system is more sensitive to the degradation in smoother regions of an image and this is a prime target for lossy compression schemes. Therefore it is preferable to embed the watermark in noisy regions and the edges of the images. However, these would degrade the robustness of the watermark scheme. Two common watermarking techniques in the frequency domain are Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT).

##### **2.5.6.2.1 Discrete Cosine Transform (DCT)**

DCT is a conversion technique on a signal into elementary frequency components (Rao et al., 1990). It converts an image to a sum of varying magnitudes and frequencies. Most DCT based watermarking techniques segment an image into non-overlapping blocks and apply DCT to each block. This will result in the converted blocks being grouped into three different frequency sub-bands – low frequency, middle frequency and high frequency, Shoemaker (2002). DCT-based watermarking is based on two facts.

The first is that most of the signal energy lies at the low frequency sub-band, which contains the most important visual parts of the image. The second is that usually signals in the high frequency sub-band can be readily removed through compression and noise attacks. As such, as both these properties affect each other, most watermarking schemes embed the watermark at the middle frequency sub-band, so that the image perceptibility will not be affected and the watermark cannot be easily removed through compression or noise attacks (Deng and Wang, 2003).

Of main interest here is the Two-dimensional discrete cosine transform (2D-DCT) as defined in equation (8) for calculating the forward DCT, and with equation (9) as the means to calculate the reverse DCT coefficients (Gonzalez and Woods, 2002). DCT is closely related to the discrete Fourier transform. It is a separable linear transformation; that is, the two dimensional transform is equivalent to a one-dimensional DCT performed along a single dimension followed by a one-dimensional DCT in the other dimension. Both of these functions are provided in Matlab Image Processing Toolbox. The definition of the two-dimensional DCT for an input image  $A$  and output image  $B$  is

$$B_{pq} = a_p a_q \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} A_{mn} \cos \frac{\pi(2m+1)p}{2M} \cos \frac{\pi(2n+1)q}{2N}, \quad 0 \leq p \leq M-1, \quad 0 \leq q \leq N-1$$

where

$$a_p = \begin{cases} \frac{1}{\sqrt{M}}, & p = 0 \\ \sqrt{\frac{2}{M}}, & 1 \leq p \leq M-1 \end{cases}$$

and

$$a_q = \begin{cases} \frac{1}{\sqrt{N}}, & q = 0 \\ \sqrt{\frac{2}{N}}, & 1 \leq q \leq N-1 \end{cases}$$

(8)

$M$  and  $N$  are the row and column size of  $A$ , respectively. The DCT tends to concentrate information, making it useful for image compression applications. This transform can be inverted using equation (9) below:

$$A_{mn} = \sum_{p=0}^{M-1} \sum_{q=0}^{N-1} a_p a_q B_{pq} \cos \frac{\pi(2m+1)p}{2M} \cos \frac{\pi(2n+1)q}{2N}, \quad 0 \leq m \leq M-1, \quad 0 \leq n \leq N-1$$

where

$$a_p = \begin{cases} \frac{1}{\sqrt{M}}, & p = 0 \\ \sqrt{\frac{2}{M}}, & 1 \leq p \leq M-1 \end{cases}$$

and

$$a_q = \begin{cases} \frac{1}{\sqrt{N}}, & q = 0 \\ \sqrt{\frac{2}{N}}, & 1 \leq q \leq N-1 \end{cases}$$

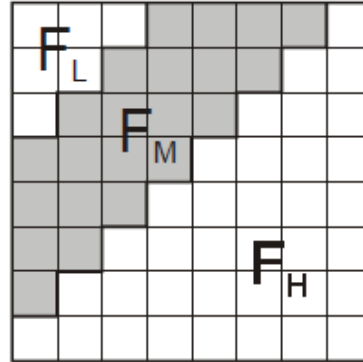
(9)

In DCT, the absolute values of the coefficients corresponding to the low frequencies are higher and appear in the top-left corner of the image, while the high frequency coefficients appear in the bottom-right corner with lower absolute values (Guan-Ming Su, www).

Robustness has become a key issue in watermarking techniques. More robust watermarking schemes are required to survive watermarking attacks. A watermarking scheme is considered robust if the cover image may be exploited but the hidden watermark remains intact and undisturbed. According to Barni et al. (1998), a watermark embedded by the DCT technique is robust to several signal processing techniques such as:

- JPEG compression
- low pass and median filtering
- histogram equalization and stretching
- dithering
- addition of Gaussian noise
- resizing
- multiple watermarking

The above mentioned DCT frequency regions can be represented as in Figure 2.8 below.  $F_M$  represents the middle band frequency, and  $F_L$  and  $F_H$  are respectively the lowest and highest frequency bands.



**Figure 2.8:** DCT frequency regions

One of the methods for watermark detection is by comparing  $F_M$  with the PN sequences (Pseudo-random sequences). A PN sequence is a sequence of binary numbers, e.g.  $\pm 1$ , which appears to be random but is actually in a perfectly deterministic order. If the correlation exceeds some threshold, then the watermark is present. According to Poljicak et al., (2011), the DCT approach is very robust to JPEG compression since JPEG itself makes use of DCT, but the DCT method lacks resistance to strong geometric distortions.

#### 2.5.6.2.2 Discrete Wavelet Transform (DWT)

Another very well-known watermarking technique is DWT in the wavelet domain. According to Singh et al., (2010), DWT is the multiresolution description of an image. The decoding can be processed sequentially from low resolution to high resolution. In the low frequency, the signals are located in the frequency domain, while in the high frequency, the signals are located in the pixel domain. Wavelets have their energy concentrated in time and are well suited for the analysis of the transient, time varying signals.

The 2D wavelet transform decomposes an image into the lower resolution approximate image (LL), horizontal (HL), vertical (LH), and diagonal (HH) detailed components. The perceptible watermark is embedded in the low frequency region, while the imperceptible watermark is embedded in the high frequency region. Figure 2.9 below presents the transformation of the 2D wavelet transform.



LL <sub>2</sub>	HL <sub>2</sub>	HL <sub>1</sub>
LH <sub>2</sub>	HH <sub>2</sub>	
LH <sub>1</sub>		HH <sub>1</sub>

**Figure 2.9:** 2 scale 2D Discrete Wavelet Transform

The main advantage of the wavelet transform is that it is believed to have the most accurate model features of the Human Visual System (HVS) as compared to the FFT or DCT. The higher energy regions are the most appropriate for watermark embedding. The HVS is less sensitive to high-resolution details bands, namely LH, HL and HH. Furthermore, embedding watermarks in these regions help to increase the robustness of the watermark and has minimal impact on image quality (Katzenbeisser and Petitcolas, 1999). However, the DWT technique lacks resistance to geometric transformations (Poljicak et al., 2011).

### 2.5.7 Encryption – Arnold Transformation

Within digital image watermarking, we have looked at:

- Generic watermarking systems (2.5.1),
- Watermarking properties (2.5.2),
- Watermarking applications (2.5.3),
- Attacks on watermarks (2.5.4),
- The embedded watermark media in biometric systems (2.5.5), and most significantly,
- Watermarking techniques (2.5.6).

There is perhaps only one component left within this topic. For further security, sometimes it can be very useful to encrypt the watermark before embedding it in the cover image. Should an attacker steal the watermark, they would not be able to see the original watermark image, but only an encrypted version of it.

A common encryption technique used together with watermarking is the Arnold transformation (AT). AT is a simple and periodic algorithm, and the watermark is easily recoverable (unscrambled) from the encrypted version detected from the corresponding watermarked image [using the Arnold Transformation Algorithm (Wu et. al., (2009))]. The original image matrix is randomized into a new matrix for protection. Equation (10) is used to compute and map changes from an original point  $(x,y)$  to another point  $(x_{n-1}, y_{n-1})$  for a digital square image  $(N \times N)$  array and the coordinate of the pixel is  $F = \{(x,y) | x, y = 0, 1, 2, \dots, N - 1\}$ .

$$\begin{bmatrix} x_n \\ y_n \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & ab + 1 \end{bmatrix} \begin{bmatrix} x_{n-1} \\ y_{n-1} \end{bmatrix} \text{mod} N \quad (10)$$

where  $N$  represents the height or width of the square image processed;  
 $x_n$  and  $y_n$  are the location coordinates of scrambled image's pixels;  
 $x_{n-1}$  and  $y_{n-1}$  are the location coordinate of the original image pixels after  $n$  iterations, respectively,  $a$  and  $b$  are positive integers.

In general, AT changes the position of pixels based on the number of iterations. The number of iterations taken is known as the Arnold period. The period depends on the image size (pixel values), and so for different image sizes, the Arnold period will be different (Peterson, 1997). After several iterations on the image, a disordered image is generated. As extra protection, the Arnold transformation can be adapted as a pre-treatment method to encrypt the watermark data against copying and tempering (Ding and Jing, 2010).

## 2.6 PREVIOUS STUDIES ON BIOMETRIC WATERMARKING TECHNIQUES

This section looks at previous work on watermarking techniques within biometric systems, in particular within face recognition, in an effort to increase the level of security of the systems against attacks on the biometric as well as the watermarking systems. We begin by looking at work on watermarking techniques in general, before zooming in on their applications within face recognition systems.

A summarized list of watermarking techniques on biometrics and their application domains is given in Appendix A.

### **2.6.1 Work on Biometric Watermarking Techniques**

Over the years, it is clear that a lot of work has been carried out on watermarking techniques, as improvements to existing techniques or as experiments on hybrid techniques. To help appreciate the development of the domain, the following is given in chronological order. These have also been chosen as they are the most relevant in the development of the work for this thesis, providing the groundwork for the contributions to be proposed.

One of the earliest watermarked fingerprint recognition schemes was proposed by Pankanti and Yeung in 1999. They proposed an invisible fragile watermarking technique for image verification, especially for fingerprint recognition. They adapted the chaotic mixing digital watermarking technique, whereby mixing the watermark to a random-textured pattern would make the fingerprint images (captured in monochrome gray scales) more resilient against attacks.

Ratha et al., (2000) proposed a robust data hiding algorithm based on the wavelet-compressed domain for fingerprint images. The fingerprint image is converted to wavelet transform and then goes through a quantization process before being encoded using the Huffman algorithm, and completed with data compression. The proposed algorithm is simple and can be easily implemented on other types of images, such as medical and satellite images. However, the robustness and the fingerprint recognition rate of the proposed scheme was not investigated.

Another well-known fingerprint watermarked scheme is from the work of Jain et al., (2002), which used a fingerprint image as the cover image and a face image as the hidden image. The authors used the Eigen-face coefficients of a user's face and embedded them into selected minutiae of the fingerprint template. The verification rate for the scheme is shown to be identical to those for the original fingerprint image. In addition, the proposed scheme is robust against certain types of attacks, especially image cropping and JPEG compression.

In Ahmed and Moskowitz, (2005), a robust watermarking technique for fingerprint images authentication is proposed, extending on their previous work, Phasemark, from image authentication to biometrics for forensic analysis. The authors used a Fourier frequency domain algorithm to generate a signature as the watermark data.

Moon et al., (2005) presented a biometric watermarking technique for user verification in remote multimodal biometric systems, concentrating on fingerprint and face information. The authors investigated the verification of a watermarked image under two scenarios. In the first, the fingerprint image is used as a cover image while the facial features are adopted as watermark data. In the second, the situation is reversed, with the face image as the cover image and the fingerprint features as hidden data. The experiments indicated that the second scenario performed better in terms of the watermarked image verification accuracy. However, there was no mention of which watermarking embedding technique was used. Moreover, the robustness of the proposed scheme was not investigated. The authors discussed the serious distortion of the face image as the value of watermark strength increases. Apparently, the imperceptibility of the face image is not important for replay attack prevention as long as the feature extraction module is able to extract the face features. This is a major point to be retained in various works later on.

Chung et al., (2005) gave a similar concept paper, except this time the robustness of the proposed scheme was investigated. They also explored the dual watermarking technique, with experimental results showing that embedding a dual watermark would provide superior performance on the watermark detection accuracy. However, there is room for improvement on the robustness of the proposed scheme, such as against JPEG compression attacks.

In the work of Vatsa et al., (2006), the authors combined the DWT (Discrete Wavelet Transform) domain with the LSB (Least Significance Bits) watermarking techniques to protect biometric data. The authors used the fingerprint image as a cover image and face template as the hidden message. The face template is converted to a 2D Gabor before embedding into the cover image. They tested the verification rate of the fingerprint based on minutiae matching, while the extracted face templates are matched using the texture based technique. They claimed that the proposed scheme (DWT + LSB) is robust to geometric and frequency attacks based on the verification rate. However, the watermark performance assessment was not done during this research. The robustness of the watermark (watermark modifications or removal) and the perceptual invisibility (how well the watermark conceals) should also be considered. The aim of the biometric watermarked image scheme is not only to maintain the verification rate, but must be

able to sustain the security and integrity of the watermark to ensure that the biometric data does belong to the genuine owner.

Noore et al., (2007) proposed a fingerprint image watermarking algorithm using DCT. The proposed scheme is made up of multiple watermarks, face image and demographic text data, intended for protecting the fingerprint image from tempering. The quality of the extracted watermarks was investigated, giving very good results and can thus provide extra information for identification purposes.

Zebbiche et al., (2008) proposed an efficient robust watermarking technique by embedding watermarks into the ridges area of fingerprint images, mainly because attackers are mostly interested in that area. The watermark was embedded using DCT and DWT watermarking techniques. The experiments conducted showed that the technique outperforms conventional techniques in terms of both embedding and robustness against known attacks such as filtering, noise and compression.

In the research by Islam et al., (2008), a fingerprint image is also used as the cover image, but a palm print template is selected as the hidden message, and a DWT watermarking technique is used for the biometric data protection. The palm prints classification is carried out using the Wu et al. (2004) classification algorithm, which has the ability to classify palm prints into six categories according to the number of principal lines and the number of intersections. The hidden password derived from the palm prints classification is used in the embedding process to encrypt the watermarked template. Vulnerability attacks against the proposed fingerprint watermarked scheme were discussed, but the experiments were not performed by the authors.

Hui et al., (2009) did a study on fingerprint watermarking for copyright protection. The fingerprint characteristics are embedded as multi-bit watermarks into the cover image using the spatial domain as well as the DCT watermarking technique. Experimental results showed that the proposed technique is feasible and effective.

Yadav et al., (2011) proposed to secure biometric templates by using the Spatial Domain Techniques for Watermarking, adopting the Steganography Method known as the Parity Checked Method. For additional security the watermark is embedded four times, so that if an attacker forges one watermark, the other watermarks would remain intact. If the attackers were to modify or replace the secure biometric template, the

system will cue the database manager should the watermark be absent or present but at incorrect pixel positions. In the experiments conducted, the matching score between the secret and the enrolled templates is higher than the threshold value, which gives successful results for authentication even after the embedded of the watermark. One advantage of the proposed method is that precise control over the maximum difference between the original and watermarked content is possible, which allows the design of near-lossless watermarking systems.

Geetha et al., (2011) presented a novel statistical attack invariant watermarking scheme for ownership protection by embedding an offline handwritten signature invisibly in the original image. The scheme employs a combination of DCT and SVD with LSB encoding for the watermarking embedding process. In the proposed DCT-SVD watermarking scheme, the features of watermark signature is embedded in the first two bits of the LSBs in the Discrete Cosine Transform of the host image. The two dimensional DCT (2D-DCT) is applied to the original image and SVD is used to find the higher coefficients. This technique is highly robust against geometric attacks and other image processing operations.

Reversible watermarking is another way in which both the original image and the hidden message or image can be perfectly recovered. Thampi and Jacob (2011) proposed using a rotational replacement of LSB reversible watermarking techniques as compared with Tian (2003) Different Expansion (DE) reversible watermarking techniques. In the rotational replacement of LSB, the original image as well as the watermark is first built into matrices and the original image matrix is divided into blocks. Each byte of watermark data can be embedded into one block. The replacement of the last row with the second last row data of the original image will be rotationally constructed until the first row is empty and one byte of watermark data can be placed in this row. The extraction process of the watermark is similar to alternately reconstructing the watermark by removing the first row of the LSB. The remaining rows are replaced in the reverse order of embedding until the watermark is entirely constructed. By measuring the quality using SSIM Index, the experimental results show that the rotational replacement of LSB is a better reverse watermarking scheme than DE.

Bansal et al., (2012) proposed a novel hybrid technique to secure and authenticate a gray scale fingerprint image by watermarking with the corresponding grey scale facial

image using NN-PSO (Neural Network-Particle Swarm Optimization). The embedding process begins by dividing the original image into blocks. The feed forward NN (Neural Network) is used to define the number of secret bits based on the block features for each block. In the second part, a PSO (Particle Swarm Optimization) module is implemented to find the best DCT coefficient locations in that block where the secret data can be embedded. The hidden data can be extracted from the watermarked fingerprint image by reversing the process. The results showed that the proposed scheme is robust against a numbers of frequency and geometric attacks as well as maintained high perceptibility vis-à-vis the original image.

From the literature review above, the first thing to note is that most researchers tend to hide biometric templates as a watermark to validate the ownership of the host image (Jain et al., 2002; Chen and Chang, 2005; Vatsa et al., 2006; Islam et al., 2008; Yan et al., 2010; Yadav et al., 2011; Thampi et al., 2011; Geetha et al., 2011; Bansal et al., 2012;). This concept is called **biometric watermarking**, where a biometric template is employed as a watermark whereas the host can be any copyright document. On the other hand, where the host image is biometric data, and the watermark can be biometric or any other trademark (logo, name, id, and others), the approach is called **watermarked biometrics**. In recent years, several studies have focused on multimodal biometric watermarking techniques, i.e. using biometrics as both host and watermark. However, such techniques can be very costly and time consuming, as they need two or more devices for authentication. In addition, the vulnerabilities could be twice as much if the biometric images get captured, as the attacker would have access to multiple number of valid biometric information.

More importantly, the literature review also reveals at least two issues that are still to be resolved, at least for watermarking in face recognition, as some of the investigations have yet to be thoroughly done:

- One main concern is that researchers so far tend to concentrate on investigating only one area, leaving the other quite untouched, whereas both properties are important:
  - high biometric recognition level, or
  - high watermark detection watermark rate.

- Another point is that, given that most proposed solutions have been for fingerprint images, the main research objective has been for a secure scheme that does not degrade the quality of the cover image, which would reduce recognition accuracy. The minutiae features (ridge ending, bifurcation, short ridge) are important for fingerprint recognition to maintain the perceptibility of the image. However, for face recognition, the quality of the face image is not necessarily important as long as the feature extraction module is able to extract the necessary face features from the face image.

### **2.6.2 Work on the implementation of Watermarking in Face Recognition Systems**

Unlike for work on watermarking in general, it has been found that only a few watermarked biometrics schemes have been proposed specifically for protecting face images (Tzouveli et al., 2002; Vatsa et al., 2004; Chen and Chang, 2005; Park et al., 2007; Vatsa et al., 2007; Hoang et al., 2008; Salahi et al., 2008; Li et al., 2010; Ma et al., 2010; Yan and Liu, 2010; Zhang, 2011; Bedi et al., 2012; Isa and Aljareh, 2012; Behera and Govindan, 2013; Kekre et al., 2015; Isa et al., 2016).

Tzouveli et al., (2002) proposed a robust watermarking scheme with a face detection method on real life images. The scheme detects the face region using a two dimensional Gaussian model of skin color distribution, and then the QSWT (Qualified Significant Wavelet Trees) as well as the DWT watermarking technique to embed the watermark in the selected area. The experimental results showed that the efficiency of the proposed face detection algorithm and the robustness of the watermarking scheme against various signal distortions were good. Unfortunately, the proposed scheme was not designed for biometric authentication systems, but rather for protecting the face area of real life images for copyright protection. The proposed scheme could possibly be enhanced so that it would be compatible with biometric authentication systems.

A robust biometric watermarking scheme was proposed in Vatsa et al., (2005). It was to improve recognition accuracy and for protecting face and fingerprint images from tampering. The Multi-resolution Discrete Wavelet Transform (DWT) watermarking technique for embedding a face image into a fingerprint image was used. The quality of the extracted face image is enhanced using a Support Vector Machine (SVM) algorithm by selecting the best quality pixels from two extracted face images. Experimental results



showed that the fingerprint verification accuracy is maintained at a high level even under attacks. As for the extracted face images, the SVM improved by at least 10% for verification accuracy.

Chen and Chang (2005) proposed a watermarking system for personal image copyright protection by embedding the owner's eigenvalue information as a bar code image into different positions based on a SHA-1 sequence. Experiments showed that the imperceptibility value and the watermark detection rate are over the acceptable benchmark. Even though the proposed scheme indeed protects the cover image, again the scheme was not designed for nor experimented on biometric image authentication.

Another interesting approach is found in Salahi et al., (2008), where a CT (Contourlet Transform) watermarking technique is used for securing face recognition systems. First, the face image is transformed in the CT domain at three levels, and then the smallest variance is selected for watermark embedding. A logo which is generated using a Walsh code is used as the hidden message. Experiments were conducted to calculate the performance of the face recognition system with and without watermarking under several attacks. The results show that the proposed scheme is robust against various attacks with the performance of the face recognition being hardly affected due to the watermark embedding. However, other face recognition algorithms were not tried with the CT domain watermarking technique to investigate their performance. This is a robust watermarking technique to cater for ownership authentication, but the embedding does not cover the entire face image, nor is there a check for the most appropriate places for embedding. Furthermore, it is also possible that the recognition rate is not affected because the watermark is embedded in a place from where the face features are not extracted for authentication. The image processing attacks used to investigate the robustness of the proposed scheme were also apparently not very strong, as the attacks did not deeply ruin the face image.

Most image watermarking is performed using DWT. However, one of the major drawbacks of DWT is that the transformation does not provide for shift invariance because of the down-sampling of its bands. To address the problems of DWT based watermarking, Yan and Liu (2010) presented a 3-level RDWT (Redundant Discrete Wavelet Transform) biometric watermarking scheme. The proposed scheme first computes the embedding capacity of a face image by using an edge and corner phase

congruency method. RDWT decomposes a face image into four sub-bands such that the size of each sub-band is equal to the original image. The redundant space in RDWT provides for additional locations for embedding, and the watermarking scheme can be designed as such that the exact location for watermark embedding can be determined. Since the size of each RDWT sub-band is equal to the size of the input image, the three levels of the RDWT decomposition provide adequate capacity to embed the watermark data without affecting the edge and corner locations. Only the second and third levels of the RDWT are used for embedding because these two levels provide more resilience to geometric and frequency attacks. Extraction is simply the reverse of the embedding process. Experimental results show that the scheme is resilient to many different signal processing attacks.

A fragile watermarking scheme was proposed in Zhang, (2011) that focuses on the facial image database in a face recognition system. The main objective is to protect the face images against tampering attacks by detecting the locations of any modifications. Experiments were conducted on the impact on recognition accuracy, detection rate, as well as the speed of face recognition with and without the watermark. The results from the experiments indicated that the scheme has a high recognition rate, sustains a good imperceptibility level of face images, as well as a high sensitivity level against tampering the watermarked facial images.

Li et al., (2012) proposed a novel salient region based authentication watermarking scheme to protect biometric templates by embedding the watermark in the region of background (ROB) and the region of salient (ROI) to investigate the face recognition rate. Experimental results showed that the proposed scheme is able to detect any interfered area, and recover the original biometric features while maintaining the recognition rate. They also proposed a semi fragile biometric watermarking to protect a face image from tampering. It was shown that the recognition rate is very minimally affected due to the watermark embedding.

Inamdar and Rege (2014) proposed a dual watermarking scheme for biometric data as copyright protection, where multiple biometric watermarks (speech and face biometric traits) of the owner are embedded as well as an offline signature is delicately overlaid on the cover image. Before embedding, speech is compressed using Linear Predictive Coding (LPC) and Gabor face is created from a face biometric trait. All three

watermarks Gabor face, LPC coefficients, and offline signature are the biometric characteristics of the owner and hence are highly related to the copyright holder. The proposed scheme is robust because as multiple watermarks are embedded in different areas of an image, at least one watermark should survive under watermarking attacks.

In 2012, Isa and Aljareh proposed a watermarked face recognition scheme based on a DCT watermarking technique using the COX algorithm. According to Isa and Aljareh (2012), the embedded watermark did not degrade the face recognition rate of the PCA algorithm. The proposed scheme is applied to face images where the password of a given person is hidden in the corresponding image to authenticate him. In their latest work (Isa et al., 2016) proposed a blind robust watermarked face recognition scheme based on the combination of PCA as face recognition algorithm with the DCT watermarking technique to enhance the security of the face recognition system without degrading the recognition rate. The authors analyzed, in particular, the 8 vulnerable positions where data could be intercepted and/or resubmitted (Ratha, 2001), and proposed a mechanism for enhancing the level of security of the PCA face recognition system.

From a rather thorough literature survey, it is found that previous research tends to protect the face image against certain threats on biometric authentication systems only in general, rather than trying to recognize and reject attempts to attack at specific points in the system. There is indeed a need for a watermarking technique that would be able to cover the 8 positions described earlier against intentional attack, as given by Ratha et al., (2001).

In summary (of the above and of the details in Appendix A), one sees that most researchers tend to focus on protecting the biometric image using additional biometric data for multimodal authentication. However, this would essentially provide protection only at certain positions (a and g in Figure 1,1), but not during the data transmission between modules. There is also a need to protect the face image against replay attacks at all possible vulnerable points while still maintaining the effectiveness of the face recognition system.

Furthermore, most of the proposed biometric watermarking techniques tend to consider high imperceptibility of the biometric image as one of the major factors to be

accomplished. However, in biometric systems, the imperceptibility of the biometric image may not be that important as long as the feature extraction module can extract the biometric features from the image for authentication. With imperceptibility not being a major factor, then robustness of the watermark may be increased, as the two are usually inversely proportional. Other researchers have tried to balance these two factors to achieve a high recognition rate, but in our case we only need to focus on the robustness of the watermark as long as it does not impact the recognition rate.

## **2.7 Conclusion**

This chapter began with an analysis of biometric authentication systems, with an emphasis on face recognition. Attention is also given to the approaches employed, and in particular, the viability of PCA as an appropriate technique. Threats to biometric authentication systems were investigated, with specific reference to the 8 threats highlighted by Ratha et al., (2001). As a means to enhance the level of security of biometric systems, watermarking is studied, covering the generic system, properties, possible attacks, applications, and most significantly the techniques. The literature reviewed not only encompass watermarking, but include the use of watermarking in relation to face recognition techniques.

The study leads to a clear idea towards proposing a suitable combination of a face recognition algorithm and a watermarking technique, and contributes to the design of the proposed scheme. The proposed scheme aims at enhancing the security of face recognition authentication systems in terms of the authenticity of the data being transmitted. The scheme is explained and analyzed, tested and evaluated in the following two chapters.

## **CHAPTER THREE**

### **PROPOSED WATERMARKED FACE RECOGNITION SCHEME**

#### **3.1 Introduction**

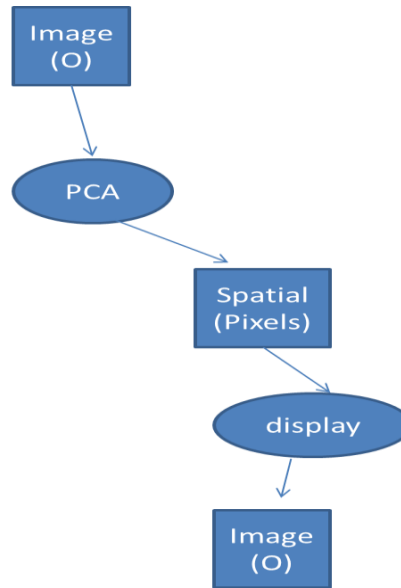
This thesis proposes a watermarked face recognition scheme to enhance the level of security in a face recognition system. This will be the core of this chapter and that of the thesis. The first main objective, which is to propose a suitable combination of a face recognition algorithm and a watermarking technique, and to show that the combination does not degrade the performance of the individual systems, will also be discussed here, together with the third main objective, being the robustness of the proposed watermarked face recognition scheme. All three proposals will be validated via five experiments to be presented in Chapter Four, with their set up being explained at the end of this chapter.

#### **3.2 Analysis**

##### **3.2.1 Face Recognition and Watermarking**

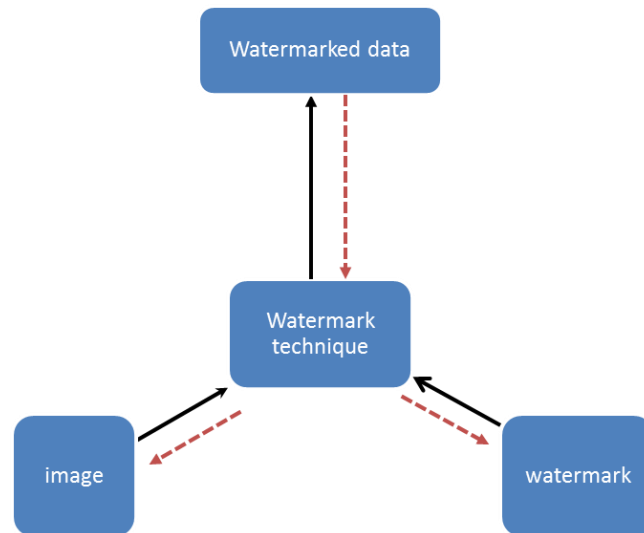
A typical face recognition process is as shown in Figure 2.2 from Chapter Two. In the first stage of any face recognition system, faces are detected and extracted from raw images. The face image can be treated with a series of pre-processing techniques to minimize the face variants that could influence the recognition rate. Feature extraction is applied to extract facial features that can then be used for recognition and identification purposes. The most commonly used features in face recognition are eigenfaces (extracted from Principal Component Analysis, PCA) and the standard recognition algorithm is the Euclidean distance to match features.

Face recognition systems are based on image processing, where a typical image processing process is as given in Figure 3.1. An original image is processed via some feature extraction process (as in Figure 2.2) to be stored as a spatial file (mainly pixels). The original image may be reproduced via some display function.



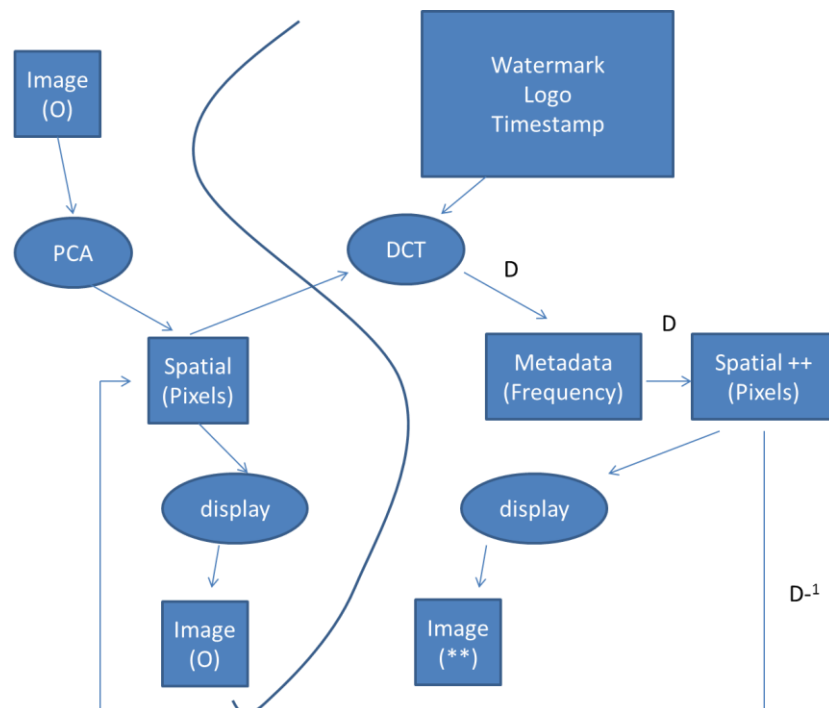
**Figure 3.1:** Image processing

Digital watermarking is a process of information hiding by embedding additional information in the cover image that can later be extracted or detected for various purposes (e.g. for authentication, owner identification, protection and security of content and others). Since the aim of this research is to provide security of the face image content and to protect the face data from illegal users, we will use watermarking approaches in face recognition. The generic watermarking process is as illustrated in Figure 3.2 that includes both the encoding and decoding processes. There are two types of watermarking techniques – spatial and transform domains. The most commonly used digital watermarking technique is the spatial domain that works directly on pixels, such as Least Significant Bit (LSB). The transform domain technique is known to be more effective than the spatial domain, a well-known example being Discrete Cosine Transform (DCT) that modifies the transform domain coefficients.



**Figure 3.2:** Watermark embedding and decoding processes

Figure 3.3 shows the stages of the proposed watermarked face recognition scheme that is robust to protect face images against replay attacks. For this illustration, we use PCA for face recognition and DCT for watermarking, with a logo and a timestamp as watermarks.



**Figure 3.3:** Watermarking and Image Processing

Firstly, PCA is applied on the image as part of the normal face recognition process, resulting in a spatial file as indicated earlier in Figure 3.1. Then DCT (a function, say  $D$ ) takes the spatial file together with the watermarks (logo and timestamp) as input to produce a non-spatial file (in frequencies), upon which some transformation of coefficients are carried out to embed the watermarks. The resulting file (watermarked data, as indicated in Figure 3.2) is reconverted into a spatial file to continue with the face recognition process.

It is to be noted that the application of the display function on this output spatial file will of course produce an image different from the original image. Nonetheless, watermarking algorithms are always designed to be invertible, and so (if needed) the inverse function ( $D^{-1}$ ) would be able to reproduce the original input spatial file, and subsequently the original image via the same display function.  $D^{-1}$  can be seen as the arrow from the watermarked Spatial++ (pixels) file on the right hand side of Figure 3.3 to the Spatial (pixels) file on the left hand side – it would be as if DCT had never taken place. This is simply an illustration to show that one can get the original image if ever needed.

The underlying idea of using watermarks is that the face recognition algorithm will now be working on watermarked images rather than the original images, whereupon there will be additional modules to always verify the watermarks at any instance within the face recognition process. The key is then to determine how exactly the chosen watermarks will be able to enhance the security of the face recognition process.

### **3.2.2 DCT algorithm does not degrade the accuracy of PCA algorithm**

Principal Component Analysis (PCA) is one of the most successful algorithms in image recognition and compression. The main purpose of PCA is to reduce the data space utilized to a significantly smaller dimension. In a face recognition environment, PCA is adopted to help in the face image feature space reduction and in the classification process.

Face recognition algorithm are divided into two main categories: feature-based and holistic approaches. In feature-based approaches, the geometric measurements among facial points (eyes, mouth, nose and others) are computed and converted into a vector of geometric features, which are then used for recognition. PCA falls within the holistic



approach category, where a face is recognized using global information on face images rather than local features. As holistic approaches use global face image information for recognition, the quality of the face image is not very critical as long as the feature extractor module is able to extract the features from the biometric traits and if the recognition rate is reasonably high.

Watermarking techniques are also divided into two main categories: spatial domain and frequency domain. Spatial domain techniques operate directly on the pixels of an image, thus embedding the watermark in the pixel file. On the other hand, frequency domain techniques convert pixels into frequencies, and watermarks are embedded within the frequencies. DCT falls within the frequency domain approach, where it converts image processing data from the spatial domain to the frequency domain into a summation of a series of cosine waves oscillating at different frequencies.

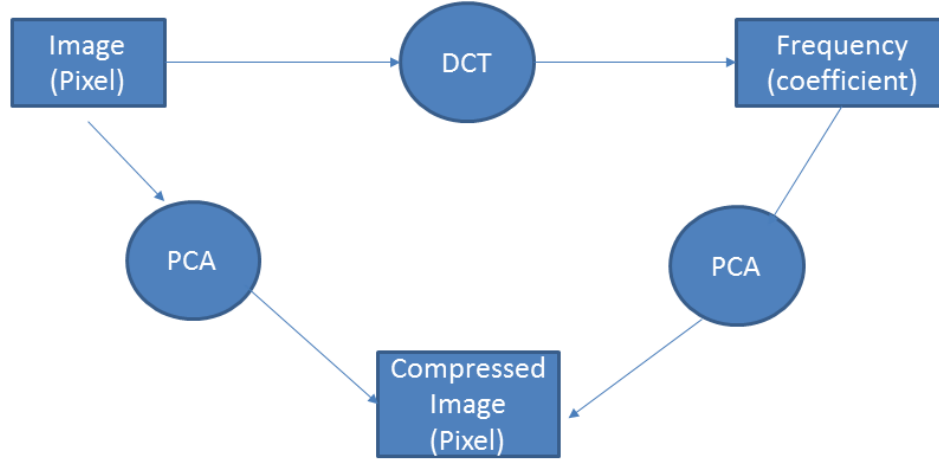
In general, the high frequencies are prone to compression and noise attacks, whereas the low frequencies are more visible to human eyes but are more robust to image processing attacks. Since the imperceptibility of the face image is not critical as long as the feature extraction module is able to recognize the face, the low frequency band is arguably a more appropriate choice for watermark embedding.

When watermarking is used to enhance security in a biometric system, in this case in a face recognition system, it is important to show that the combination does not degrade each other's performance, in particular in terms of accuracy. In our case, we need to ensure that DCT does not degrade the performance of PCA, and vice versa.

On this point, analytical results validated by experiments as presented by Weilong, Meng and Shiqian (2005) have shown that when DCT is first applied on a pixel file to obtain a frequency domain file (with changes in coefficients), and then followed by the application of PCA for compression as well as reconverting to an image (compressed file), the result is the same as that of a direct application of PCA on the original pixel file. This is as illustrated in Figure 3.4.

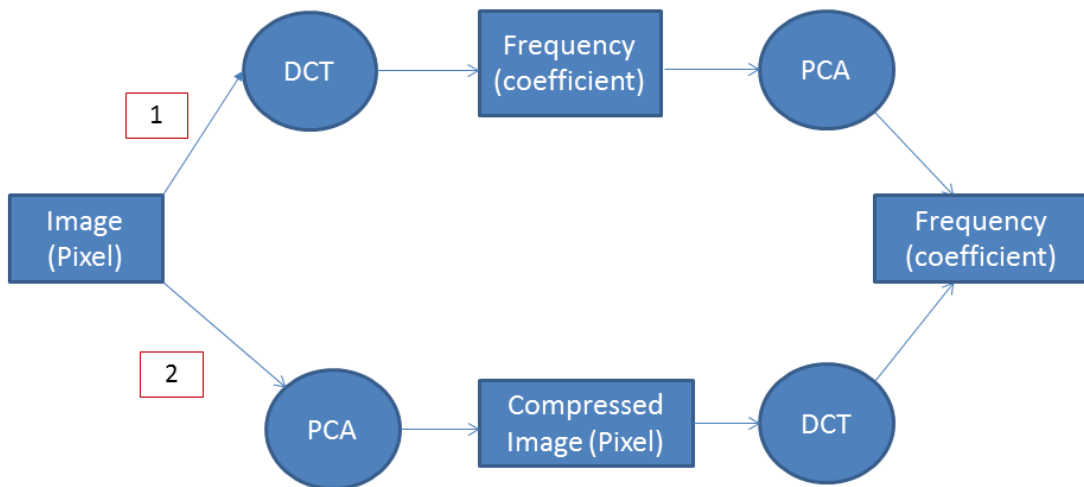
This result would mean that it safe to say that DCT does not degrade the performance of PCA, at least in terms of the accuracy of face recognition, should there be a need to introduce watermarking at certain points of the face recognition system. This claim is

towards the first main objective of the thesis, and will be validated by an experiment in Chapter Four.



**Figure 3.4:** DCT does not disturb the accuracy of PCA

The top and right hand part of Figure 3.4 is path 1 in Figure 3.5. Ideally, we would want to have the same analytical results both ways, namely also for the application of DCT following an application of PCA – path 2 in Figure 3.5 – which would then show that PCA also does not degrade the accuracy of DCT. Proving this result, i.e. path 2, is beyond the scope of this thesis, and so we will conduct experiments to show some form of validation of this result.

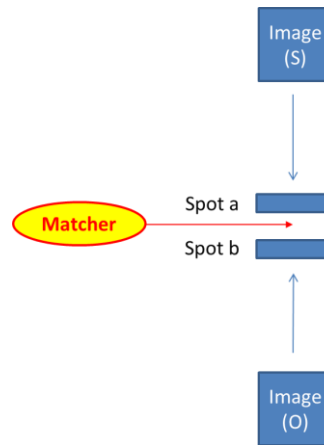


**Figure 3.5:** DCT and PCA do not degrade the accuracy of each other

### 3.3 Design

#### 3.3.1 Proposed secure watermarked face recognition scheme

We now move on to the second and most important main objective of this thesis, which is to propose a watermarked face recognition scheme to enhance the level of security in a face recognition system. First, we relook at the standard face recognition algorithm process, as illustrated in Figure 3.6, which is an extension of Figure 2.2 in view of how a face recognition algorithm would work on watermarked images.

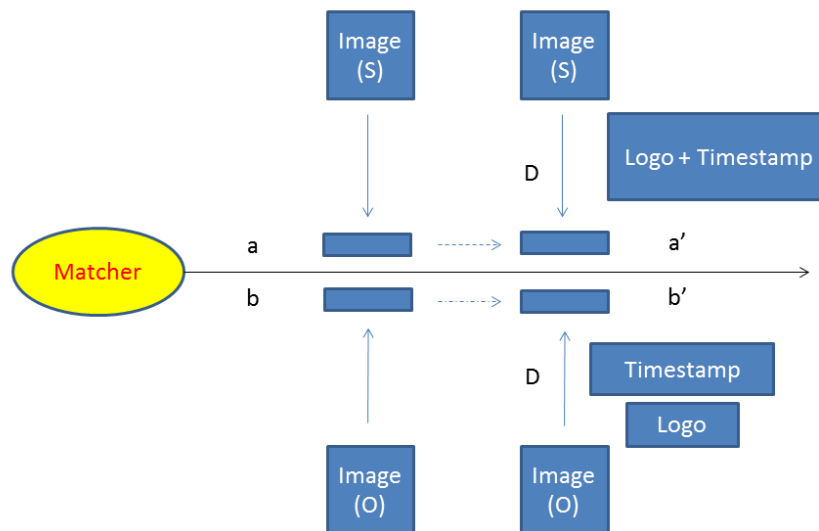


**Figure 3.6:** Face recognition process

Face recognition systems essentially match a captured image of a subject (S) to an image of an approved/certified person, referred to as the object (O), the latter being stored in some facial database. To do this, there is a feature extraction module that works on the image of the subject, and the same is done for the targeted object (the target object is determined by some means, perhaps by tagging a smart card carrying the identity of the subject). A matching algorithm (Matcher) is then used to match the extracted features (face features/ spot ‘a’ and face features/ spot ‘b’), resulting with an approval if there is a match, and a rejection otherwise.

Figure 3.7 gives an overall picture of the use of watermarking in a face recognition system. Watermarks are embedded into the image of the subject (with the method shown in Figure 3.3) as soon as it is captured, and the same is done for the object image once retrieved from the database. In some cases, part of the watermark may have already been embedded earlier for various reasons (in this illustration, the logo would have already been embedded in all object images upon storage). This is then followed

by the feature extraction process on both sides, resulting in their respective spatial files, upon which the matching algorithm will work (position a' and position b'). In essence, the matching is exactly like the matching on the features of the original images (position a and position b), except these features have been in a sense transformed to include the watermarks (position a' and position b') – albeit not done directly.



**Figure 3.7:** Watermarking in face recognition systems

The main thing to note here is that the matching should give exactly the same results (approval or rejection) as with the original face recognition process because exactly the same face recognition algorithm is used, and also due to the following:

- ☐ Exactly the same watermarks are embedded into both the subject and object images
- ☐ The same original face recognition feature extraction algorithm is used on both ends
- ☐ The same original face recognition matching algorithm is used.

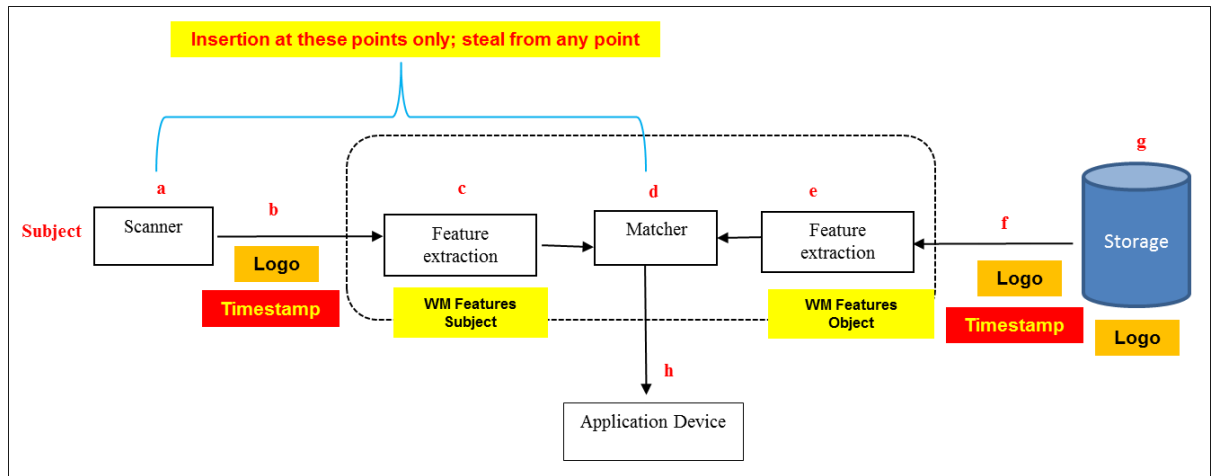
Now, it remains to see how the watermarking technique will enhance security. The proposed watermarked face recognition scheme makes use of two different watermarks:

- ☐ Logo
- ☐ Timestamp

The logo serves as in any other watermarking technique that embeds particular images within object images. The main purpose is usually to identify genuine images within the database of objects. However, in this proposed work, it will be seen further on that it is also used to identify captured images.

The timestamp is the main security enhancer, as it will be used as a form of session ID. Any image captured from within the process and resubmitted later will be immediately recognized as coming from a different session and will be rejected. In addition, like the logo, it can also be used to identify captured images by its mere existence within the image.

In order to check on the coverage of the proposed watermarked face recognition scheme, Figure 3.8 depicts the proposed scheme indicating the places where the watermarks are present within the system, and most importantly the positions where attackers can capture biometric data from within the system and then resubmit it at the same or at other positions.



**Figure 3.8:** The proposed watermarked face recognition scheme

The diagram indicates that data may be captured from any of the 8 positions a, b, c, d, e, f, g, h, and then resubmitted at the same place or at any other position, which gives rise to  $8 \times 8 = 64$  situations. We will look at all these situations within a single table below (Table 3.1). First, scope-wise, two key points about the proposed scheme are to be noted:

- ❖ It covers only situations where data has been captured (i.e. stolen) from and reintroduced into the system, and NOT when fresh data is introduced from outside the system.
- ❖ It also covers only situations where the watermark has been introduced, which means only the points that are expecting watermarks are covered.

The above means that the following situations are excluded, and may be left for future work.

➤ Presenting a printed image to the scanner:

- A fresh image is shown to the scanner (camera), possibly a picture of an authorised person. In this situation, the scanner has to recognise that it is a printed image, and not that of a physical person. There is a need for a good method for this, but in the meantime, CCTVs may be deployed to monitor such a situation.
- Images are captured from the scanner (position a) before the watermark is embedded. The images are printed, and then placed in front of the scanner. This can happen if the scanner has a memory, which can and perhaps should be removed. In any case, this situation is similar to the above (fresh image).

- The approval code is captured at position h and resubmitted later on at the same position. This requires different forms of protection, certainly not by watermarking. As such, position h will not be considered in this proposal, leaving a total of 7 positions.

From these, and also in general, a few additional positions can be noted:

- ❖ In as much as data may be captured from any of the 7 remaining positions, there is nothing to gain by resubmitting the captured data at positions e, f and g, as these positions transmit or store authenticating data and not the one to be authenticated – which then reduces the total number of situations to be checked down to  $7 \times 4 = 28$ .

❖ In verifying the security in these 28 situations, it is important to note the types of data that are present at the 7 remaining positions:

- Image only (of subject)
- Image with watermarks logo and timestamp (of subject)
- Features including those of the watermarks logo and timestamp (of subject)
- Features including those of the watermarks logo and timestamp (of subject and object)
- Features including those of the watermarks logo and timestamp (of object)
- Image with watermarks logo and timestamp (of object)
- Image with watermark logo only (of object)

The above lead to two fundamental points that underlie the proposed watermarked face recognition scheme:

- ❖ Any image captured from anywhere other than from position a will already have a watermark embedded (at least a logo), and its presence can be readily detected. As such, the image can be immediately rejected if it is resubmitted at position a.
- ❖ Data captured from one position may have to be processed externally before resubmitting at another position. For example, for an image captured from position a, to be resubmitted at positions c or d will have to have its features extracted before being resubmitted. However, apart from positions a and g, all data would have the timestamp watermark, and so a later resubmission (as a subject) will not tally with the timestamp of the object watermark.

With all the above points well-noted, we can now proceed to present how the 28 situations are secured, as given in Table 3.1 below.

This would cover the second main objective of this thesis, and as with the first main objective presented in 3.2, the claim will also be validated via an experiment in Chapter Four.

**Table 3.1:** The 28 situations which need to be secured and protected

Situation	Data captured from position	Data resubmitted at position	Type of data captured	Type of data resubmitted	Security mechanism	Status
1	a	A	face image (no watermark)	face image (no watermark)	reject if there is an existing watermark	Resolved
2	a	B	face image (no watermark)	face image (no watermark)	reject if there is an existing watermark	Resolved
3	a	C	face image (no watermark)	extract face features from face image (no watermark)	will not match with the object as there are no features of the watermark	Resolved
4	a	D	face image (no watermark)	extract face features from face image (no watermark)	will not match with the object as there are no features of the watermark	Resolved
	a	E	Resubmission only up to position d			
	a	F				
	a	G				
5	b	A	face image (with watermark)	face image (with watermark)	reject if there is an existing watermark	Resolved
6	b	B	face image (with watermark)	face image (with watermark)	reject if timestamp does not tally	Resolved
7	b	C	face image (with watermark)	extract face features from face image (with watermark)	reject if timestamp does not tally	Resolved
8	b	D	face image (with watermark)	extract face features from face image (with watermark)	reject if timestamp does not tally	Resolved
	b	E				



	b	F	Resubmission only up to position d			
	b	G				
9	c	A	features (inc. of watermark)	features extraction is a form of non-reversible compression	Not relevant	
10	c	B	features (inc. of watermark)	features extraction is a form of non-reversible compression	Not relevant	
11	c	C	features (inc. of watermark)	features (inc. of watermark)	reject if timestamp does not tally	Resolved
12	c	D	features (inc. of watermark)	features (inc. of watermark)	reject if timestamp does not tally	Resolved
	c	E	Resubmission only up to position d			
	c	F				
	c	G				
13	d	A	features (inc. of watermark)	features extraction is a form of non-reversible compression	Not relevant	
14	d	B	features (inc. of watermark)	features extraction is a form of non-reversible compression	Not relevant	
15	d	C	features (inc. of watermark)	features (inc. of watermark)	reject if timestamp does not tally	Resolved
16	d	D	features (inc. of watermark)	features (inc. of watermark)	reject if timestamp does not tally	Resolved
	d	E	Resubmission only up to position d			
	d	F				
	d	G				

17	e	A	features (inc. of watermark)	features extraction is a form of non-reversible compression	Not relevant	
18	e	B	features (inc. of watermark)	features extraction is a form of non-reversible compression	Not relevant	
19	e	C	features (inc. of watermark)	features (inc. of watermark)	reject if timestamp does not tally	Resolved
20	e	D	features (inc. of watermark)	features (inc. of watermark)	reject if timestamp does not tally	Resolved
	e	E	Resubmission only up to position d			
	e	F				
	e	G				
21	f	A	face image (with watermark)	face image (with watermark)	reject if there is an existing watermark	Resolved
22	f	B	face image (with watermark)	face image (with watermark)	reject if timestamp does not tally	Resolved
23	f	C	face image (with watermark)	extract face features from face image (with watermark)	reject if timestamp does not tally	Resolved
24	f	D	face image (with watermark)	extract face features from face image (with watermark)	reject if timestamp does not tally	Resolved
	f	E	Resubmission only up to position d			
	f	F				
	f	G				
25	g	A	face image	face image	reject if there is an existing watermark	Resolved

			(with logo)	(with logo)	(logo)	
26	g	B	face image (with logo)	face image (with logo)	will not match with the object as there are no features of the timestamp	Resolved
27	g	C	face image (with logo)	extract face features from face image (with logo)	will not match with the object as there are no features of the watermark	Resolved
28	g	D	face image (with logo)	extract face features from face image (with logo)	will not match with the object as there are no features of the watermark	Resolved
	g	E	Resubmission only up to position d			
	g	F				
	g	G				

### **3.4 Conclusion**

This chapter discussed the three main objectives of the thesis. The first is the PCA-DCT combination as a more secure face recognition system, and in particular the relationship between image processing and watermarking to justify that the DCT watermarking technique will not degrade the performance of the PCA recognition rate. The second, being the core of this chapter and the thesis, is the proposed watermarked face recognition scheme to enhance the level of security in a face recognition system. Thirdly is the robustness of the proposed watermarking scheme. The experiment set up and the actual experiments for five experiments to validate these three proposals, their results, analysis and discussion, will be presented in Chapter Four.

# CHAPTER FOUR

## IMPLEMENTATION, TEST AND EVALUATION

### 4.1 Introduction

As mentioned in CHAPTER THREE, the claims towards the first and second main objectives of the thesis will be validated via experiments to be presented in this chapter. The third main objective of the thesis, being the robustness of the proposed watermarking scheme will also be carried out via an experiment, with the addition of two other experiments that are needed to support these three main experiments.

This chapter then presents the five evaluation experiments for the proposed scheme:

- 1) Determining the frequency band for watermarking
- 2) Non degradation of PCA and DCT due to the combination
- 3) Replay attack prevention – system rejection of captured data
  - Illegitimate presence of watermarks (logo)
  - Timestamp does not tally
  - Value of features do not match (based on the face recognition system)
  - Additional: Logo does not exist (for fresh data)
- 4) Robustness of the watermark scheme
- 5) Comparative study of watermarking techniques

Experiment 3 is for the second main objective of this thesis, and it is the core of this thesis. Experiment 2 is towards the first main objective of the thesis, supported by Experiment 5, as the said objective also includes a proposal for a secure face recognition and watermarking combination. Experiment 1 is a pre-requisite for all the other experiments, while Experiment 4 is towards the third main objective of the thesis.

All the experiments are conducted using the Database of Faces (ORL, 2002) at AT&T Laboratories, Cambridge University. The database contains a set of face images of forty

persons with ten different images for each person. The images were taken at different times, with various lighting conditions, different facial expressions (open /closed eyes, open/closed mouth, smiling/unsmiling and others) and dissimilar facial details (glasses/ no glasses). All the images were taken against a dark homogeneous background with the subjects in an upright and frontal position. The size of each image is 92x112 pixels with 256 grey levels per pixel in PGM format.

## 4.2 Experiment Set Up

As the basis for setting up the experiments, recall that the proposed watermarked face recognition scheme is aimed at enhancing security in a face recognition system, in particular against **data captured from within the system**. We refer to the earlier Figure 3.8, where the critical positions of the system are shown, and where the watermarks (logo and timestamp) are present. In general, data may be captured from any of the positions a, b, c, d, e, f, g, h. Recall also that resubmission (after possible additional external processing/tampering) would only happen at positions a, b, c, d, as resubmissions at positions e, f, g would be of no interest since these positions transmit the images of verifying data and not data to be verified.

Recall also that fresh data introduced from outside is out of the scope of this thesis, but this would only be reasonably introduced at points a, g and h, as all the other points would be secured by the presence of watermarks. At point a, the system would have to be able to detect that the image introduced is not captured from a human, but rather via a printed image in front of the camera, or as a digital image before the watermarks are introduced. [The case for point a after the watermark has been embedded, and the case for point g, are covered later on as an additional check.] In addition, an approval code stolen at point h and later reintroduced also at point h is also out of the scope of this thesis, as it does not involve any watermarking (unless, of course, if the same watermarking and verification technique is also used on approval codes, and not just on images and their corresponding features).

The set up for the five experiments will now be presented in turn.

#### 4.2.1 Experiment 1 - Determining the frequency band for watermarking

This experiment is to determine the best frequency band to place the watermarks in an image. Watermarking techniques are commonly distinguished based on two watermarking domains: Spatial Domain and Transform (frequency) Domain (Gaurav et al., 2012).

The underlying concept of the spatial domain (Cheung, 2000) is to embed a watermark into an image by modifying the grey value of certain pixels in the image (Ramkumar, 2000; Navas, Sasikumar and Sreevidya, 2007). The classical methods are to modify the last significant bits (LSB) of specific pixels of the host image based on the watermark bits (Wang, Pan and Jain, 2009). For the transform domain, the underlying concept is to embed a watermark via the frequency coefficients of the transformed image using discrete cosine transform (DCT), discrete wavelet transform (DWT) (Vetterli, 1995), or some other kind of transform techniques (Shih, 2008; Wang, Pan and Jain, 2009). The frequency coefficients are very slightly adjusted, which makes it more robust against attacks, and that the changes are quite unnoticeable. However, they are more difficult to implement and the computer resources required tend to be more expensive.

DCT is a conversion technique of a signal into elementary frequency components (Rao et al., 1990). It converts an image to a sum of varying magnitudes and frequencies. The output array of DCT coefficients contains integers, which can range from -1024 to 1023. Most DCT-based watermarking techniques segment an image into non-overlapping blocks and applies DCT to each block. This would split the converted block into three different frequency sub-bands: low frequency, middle frequency and high frequency, Shoemaker (2002), as illustrated in Figure 2.8 earlier in Chapter Two.

DCT-based watermarking is based on two well-known facts. The first is that the high frequencies are more prone to compression and noise attacks, while the second is that the low frequencies are more visible to human eyes but are more robust to image processing attacks. To balance these two advantages/disadvantages, most watermarking schemes tend to embed the watermark at the middle frequency sub-band so that the image perceptibility will not be very much affected while at the same time the watermark cannot be readily removed through compression or noise attacks (Deng and Wang, 2003). However, for

biometric systems, since the imperceptibility of the face image is not critical as long as the feature extraction module is able to recognize the face, the low frequency band would arguably be more appropriate for watermark embedding.

This experiment is to show that the embedding of watermarks does not degrade the accuracy of the face recognition system (accuracy of recognition). Equally fundamental, the watermark detection rate must also be investigated to ensure that the face image had been watermarked correctly, and in particular the timestamps can be retrieved accurately (watermark detection/ recognition).

Before these, in order to determine which frequency bands give the best results for attaining a high face recognition accuracy rate as well as a high watermark detection rate, a watermark logo and a timestamp are embedded into each frequency band. Both these properties are then measured by increasing the strength value of the watermarking scheme, based on the fact that the quality of the face images would be increasingly disturbed as the strength value increases. At a particular strength value, the watermark detection rate and face recognition rate would decrease, and this would be recognised as the threshold.

Given the above, measures for accuracy of recognition and watermark detection/recognition are required, whereby the following are used.

a) Accuracy of face recognition

The performance of face recognition can be measured based on the similarity between each of the training watermarked face images in the database against the test images. The Euclidean distance  $\|y_1 - y_2\|$  is chosen to measure the similarity between both images. The highest similarity score indicates a face matched in the training set. The similarity score is based on the inverse Euclidean distance, which is defined as follows:

$$FR(y_1, y_2) = \frac{1}{1 + \|y_1 - y_2\|} \in [0,1] \quad (11)$$



where  $y_1$  is the weight of test image and  $y_2$  is the distance of training image.

b) Watermark detection/recognition

Normalized Correlation (NC) is selected to compare the original embedded watermark with the extracted watermark of watermarked image. NC is measured between 0 and 1. The nearer the NC value to 1, the better is the watermark detection rate. The calculation for NC is as follows:

$$NC = \frac{\sum_i \sum_j W(i, j) \tilde{W}(i, j)}{\sum_i \sum_j [W(i, j)]^2} \quad (12)$$

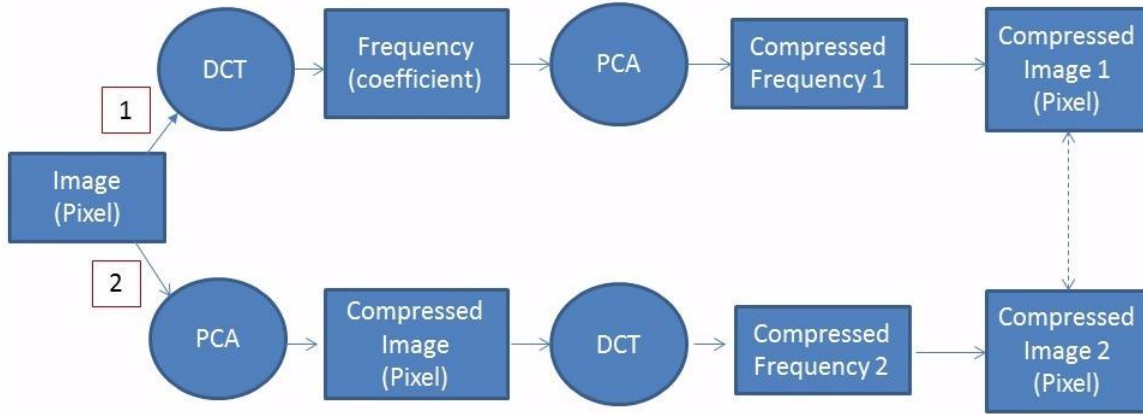
where  $W(i, j)$  is the original embedded watermark and  $\tilde{W}(i, j)$  is the extracted watermark from watermarked image.

#### 4.2.2 Experiment 2 - Non degradation

This experiment is to validate the claim that the use of DCT will not degrade PCA-based face recognition, and vice versa.

Repeating the earlier explanation and also Figure 3.5 within Figure 4.1 below, the analytical result validated by experiments as presented by Weilong, Meng and Shiqian (2005) is shown as path 1 in the Figure 3.5. This experiment will be repeated in Chapter Four. An experiment will also be conducted for the application of DCT following an application of PCA, i.e. path 2, which would then show that PCA also does not degrade the accuracy of DCT (albeit only by experimentation).

The difference between the earlier Figure 3.5 and Figure 4.1 is the right end, which will be explained shortly.



**Figure 4.1:** Experiment 2- DCT and PCA do not degrade each other

The experiment will carry out both paths with the same input images, and to show that the results are identical. Since PCA has been shown not to degrade DCT (Path 1), identical results (from Path 2) would indicate that DCT also does not degrade PCA.

Referring to Figure 4.1 above, first note that both paths result in essentially compressed coefficient files. For Path 1, the DCT produces frequencies, which are then compressed by the PCA (Compressed Frequency 1). For Path 2, the PCA compresses the image file, and the DCT produces the frequencies of the compressed file (Compressed Frequency 2). These two files are technically quite different, but equality may be shown by reconverting the files resulting from both paths into pixel files and then compare them to the respective original input images (hence the right end of the above figure). For this comparison, the structural similarity (SSIM) index is used.

The SSIM index is based on the concept of full reference image quality assessment (Wang et al., 2004). The SSIM index is calculated for various types of images, such as to check on the preservation of the quality of digital television and cinematic pictures, as well as for digital images and videos in general. The SSIM index is calculated on the various windows of an image. The measure is between two windows of common size  $N \times N$  from two given images  $x$  and  $y$  where the SSIM index compares local patterns of pixel intensities that have been normalized for luminance, contrast and structure, and it is defined as follows:

$$SSIM(x, y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)} \quad (13)$$

where  $\mu_x$  and  $\mu_y$  are respectively the means of the signals for  $x$  and  $y$ ,  $\sigma_x$  and  $\sigma_y$  are the standard deviations of the signals for  $x$  and  $y$ , while  $C_1$  and  $C_2$  are constants with values much smaller than 1.  $\sigma_{xy}$  is the estimated correlation coefficient of the signals for  $x$  and  $y$ . A  $SSIM(x, y)$  value of 1 would mean the images  $x$  and  $y$  are completely identical, but for this experiment, a threshold value of 0.85 would already suffice.

#### 4.2.3 Experiment 3 - System Rejection

First and foremost, it is to be noted that data captured from the following positions will have the given contents (data captured from positions a and h are out of the scope of this thesis):

**Table 4.1:** The contents of captured data from position b to position g

b	c	d	e	f	g
Subject	Subject	Subject & Object	Object	Object	Object
Image	Features	Features	Features	Image	Image
Logo	Logo	Logo	Logo	Logo	Logo
Timestamp	Timestamp	Timestamp	Timestamp	Timestamp	

The above means that only the following combinations of captured → resubmissions are possible:

Captured at	Resubmission at	
b, f, g	a	<i>Requires image</i>
b, f, g	b	<i>Requires image</i>
c, d, e	c	<i>Requires features</i>
c, d, e	d	<i>Requires features</i>

In general, as given by an earlier table 3.1, the system will reject captured data at the resubmission positions, namely a, b, c, d, and based on the following:

**Table 4.2:** The main basis in experiment 4.2.3 - system rejection

Rejection by	Captured at	Resubmission at	Rejection at
Illegitimate presence of logo	b, f, g	a	a
Timestamp does not tally	b, f, g	b	b
Value of features do not match (based on the face recognition system)	c, d, e	c, d	d

The table 4.2 above will be the main basis for the experiments:

- Illegitimate presence of watermarks (logo)
- Timestamp does not tally
- Value of features do not match (based on the face recognition system)

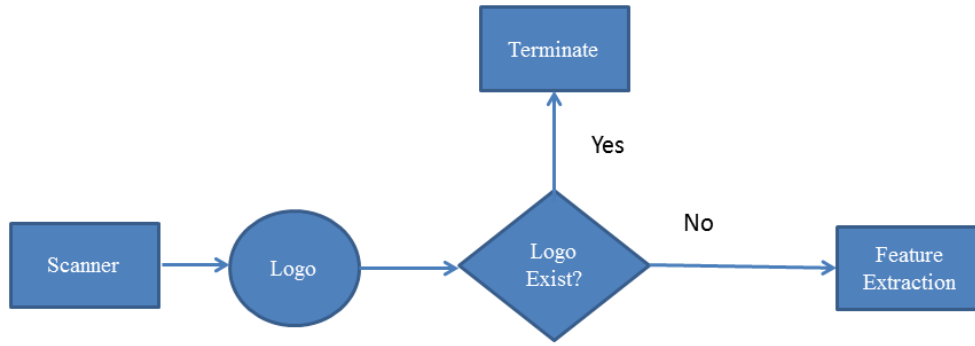
There is also an additional check for fresh data submitted at a and g:

- Additional: Logo does not exist.

The following provide more details.

a) Rejection 1 - Illegitimate presence of logo (at position a)

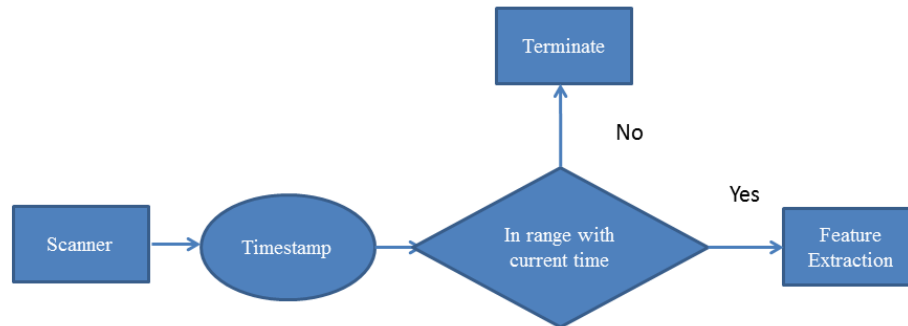
Any captured data (apart from those captured at position a) will already have the watermarks. Any image submitted at position a that already has a watermark will be immediately rejected.



**Figure 4.2:** Illegitimate presence of logo

b) Rejection 2 - Timestamp does not tally (at position b)

The timestamp is one of the most crucial mechanisms adopted for the proposed watermarked face recognition scheme. The function of the timestamp is similar to a session id where the current time, as well as the unique module id, is captured and embedded as watermarks at position a before the face data is submitted through the transmission channel. The purpose of the timestamp watermark is to validate that the current face data is fresh and it is not one captured from an earlier session and then resubmitted back into the system.

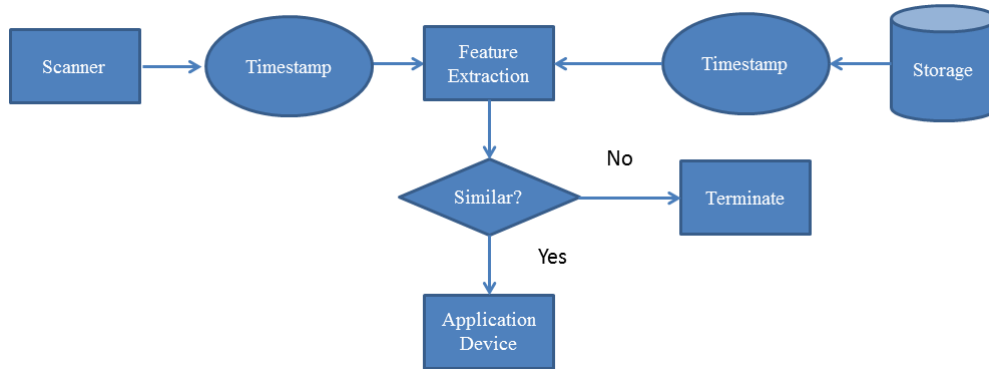


**Figure 4.3:** Timestamp is no tally

c) Rejection 3 - Feature values do not match (at position d)

The timestamp watermark is also key for resubmissions of captured data at positions c and d. Should they carry a different timestamp than the current time, the

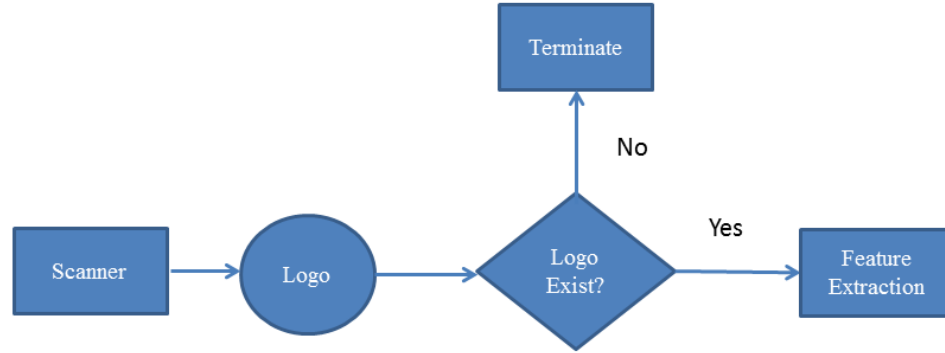
features of that timestamp would certainly not match the features of the current timestamp carried by the verifying image coming from the database. This matching is simply done by the face recognition system.



**Figure 4.4:** Features value does not matched

d) Additional - Logo does not exist (at positions a, g)

The proposed watermarked face recognition scheme embeds a logo watermark at two positions: in position a once the face image is captured at the sensor, and during the enrolment process after a certified face image gets stored in the database at position g. The existence of the logo watermark is checked at positions a and g as validation towards two scenarios. First, if an attacker tries to submit his own face image at position a (after the system is supposed to have embedded the watermark), the system will check for the existence of the logo, and if it does not exist, the system will reject the face data transmission. At position g is when an attacker wants to submit a face image into the face database. Again, the system will reject the update of the face database if there is no embedded logo.



**Figure 4.5:** Additional rejection - logo does not exist

#### 4.2.4 Experiment 4 - Robustness

The needs for more robust watermarking schemes are required to survive watermarking attacks. Robustness has become a key issue in watermarking techniques. Hidden watermark images should remain intact even if the cover image may be disturbed due to attacks. According to Barni et al. (1998), the watermark embedded using the DCT technique is robust to several signal processing techniques, such as:

- i. JPEG compression
- ii. low pass and median filtering
- iii. addition of Gaussian noise

In this research, the robustness of the watermark scheme also needs to be investigated to ensure that the watermark cannot be easily removed by an attacker.

The highest recognition rates for accuracy of face recognition and watermark detection will determine which frequency band to choose for embedding the watermark. Similar to the detection experiment in (b), NC is also selected to measure the robustness of a watermarked image. The watermarked image is exposed to various attacks for evaluation, and the closer the NC value is to 1, the more robust the watermarked image is, and the extracted watermark will then be considered well preserved.

#### 4.2.5 Experiment 5 - Comparative study of watermarking techniques

The watermarking technique used in this research is DCT. This experiment is carried out to validate this choice. Three of the most used watermarking techniques are compared:

- Spatial: LSB
- Transform (or frequency)
  - DCT
  - DWT

In the comparison, the same three accuracy rates of recognition, detection and robustness are tested using the same measures FR and NC as described above.

### **4.3 Validation – Experiments**

We are now in a position to conduct the five experiments. However, first recall that one of the main purposes of our proposed scheme is for countering replay attacks with a robust blind watermarking technique to protect the biometric traits from being re-used (replayed) by attackers. The face image can be protected against such an attack by placing the watermark in the area where the face feature extraction happens. As such, the proposed scheme should meet the following goals:

- Reject face images that have been captured and resubmitted later at any position in the biometric authentication system.
- Retain the recognition rate for watermarked face images to maintain the effectiveness of the biometric authentication system.

In the proposed watermarked face recognition scheme, the Viola and Jones algorithm (Viola and Jones, 2004) is adopted for the face detection algorithm, and the PCA for the feature extraction technique. The Viola and Jones algorithm is very effective for the localization of the spatial extent of the face and to determine its boundaries. The algorithm



was observed to perform reasonably well on the face images used in this work. PCA has been chosen as the feature extraction algorithm because PCA has proven to be very effective for information compression, and several researchers have also shown that PCA performs better in face recognition when the training data set is small, which is our case.

In the biometric authentication system, the sensor, which in our case is a camera, captures the face image and embeds a watermark before transmitting it to the feature extraction module. At the feature extraction module, the watermark is extracted and validated. If the watermark can be extracted properly and matches correctly, only then the feature extraction module can begin its task. The feature extraction module then passes its results to the Matcher, which matches the results with a targeted set of features obtained from the database of certified images.

The aim of watermarking is to ensure ownership protection of the face image. This approach prevents an attacker from trying to inject a sniffed face image (and possibly subsequently modified) into the communication channel between the sensor and the feature extraction module, or between the feature extraction module and the matcher – namely at the positions a, b, c and d in the diagram given earlier in Figure 3.8.

As the embedded watermark is robust, slight changes to modify the face image would also disturb the watermark as well as the face recognition rate. A similar approach is applied in the face database environment. In the scenario where an attacker tries to use a sniffed face image to fool the sensor (i.e. print the sniffed face image and show it to the camera), the face detection module will not be able to detect the face area, mainly because the embedded watermark would have disturbed the perceptibility of the sniffed face image.

#### **4.3.1 General Modules**

The five experiments will be presented in turn further below, but first we present the two most critical modules utilized in the system – the watermark embedding module and the watermark extraction module.

### a) Watermark embedding module

The overall watermark embedding process is illustrated in Figure 4.6, and the details of the steps are as follows.

#### Step 1.

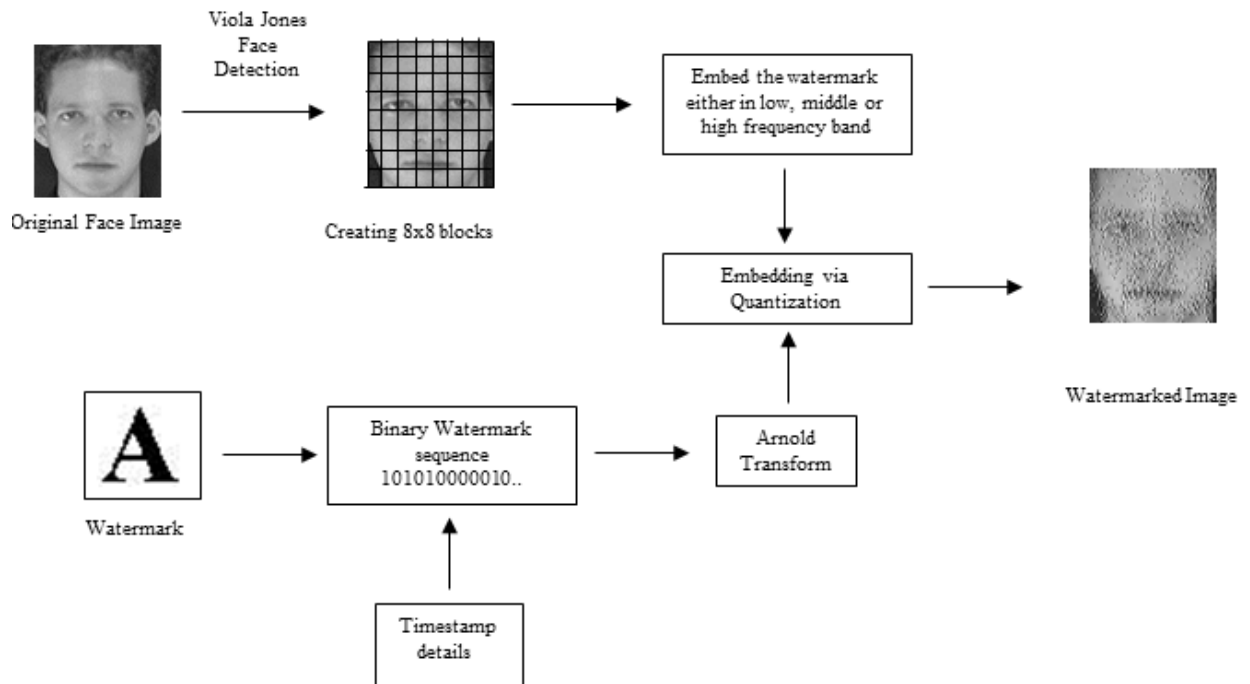
Read the face image and the watermark image.

#### Step 2.

Transform the watermark image into binary and convert the binary watermark sequence into an Arnold Transform (AT). The AT is used in order to protect the watermark against intentional reconstruction by intruders.

#### Step 3.

Detect the face area using the Viola Jones technique.



**Figure 4.6:** Watermark embedding process

Step 4.

Divide the face area image into 8x8 blocks, and convert each block into a DCT transform.

Step 5.

Protect against compression. In order to protect the watermark against JPEG compression, each DCT coefficient from every block is quantized using the quantization table of the JPEG compression standards. (See Figure 4.7)

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

**Figure 4.7:** Quantization table recommended in the JPEG specification

Step 6.

Choose the frequency band for watermark embedding to be done in Step 7. [This frequency band is decided based on Experiment 1 – see below.]

Step 7.

Choose the robustness level for watermark embedding [This watermark strength value is decided based on Experiment 4.] Then execute watermark embedding. For this, let  $C(k,l)$  be the DCT coefficients in the chosen frequency range,  $R$  the modulus,  $P$  the mathematical remainder of  $|C(k,l)|$  with  $P \in \{0,1,2, \dots, R-1\}$ , and the other variables be declared via the formulae as given below. The value of  $R$  is a predefined constant and is used as a reference threshold. The higher the value of  $R$ , the higher the level of robustness of the method, but the quality of the watermarked image decreases. The value of  $R$  is chosen in such a way so as to obtain a balance between robustness and the face

recognition rate, which apparently also depends on image quality.

$$P = |C(k, l)| \bmod R;$$

if watermark bit = 0:

if watermark bit = 1:

$$\text{if } P \geq 3 \times \frac{R}{4}$$

$$\text{if } P \ll \frac{R}{4}$$

$$C(k, l)^* = C(k, l) - P + 5 * \frac{R}{4}$$

$$C(k, l)^* = C(k, l) - P - \frac{R}{4}$$

$$\text{else if } P < 3 * \frac{R}{4} \&\& P \geq 2 * \frac{P}{4}$$

$$\text{else if } P > \frac{R}{4} \&\& P \ll 2 * \frac{R}{4}$$

$$C(k, l)^* = C(k, l) - P + \frac{R}{4}$$

$$C(k, l)^* = C(k, l) - P + 3 * \frac{R}{4}$$

else

else

$$C(k, l)^* = C(k, l)$$

$$C(k, l)^* = C(k, l)$$

(11)

Step 8.

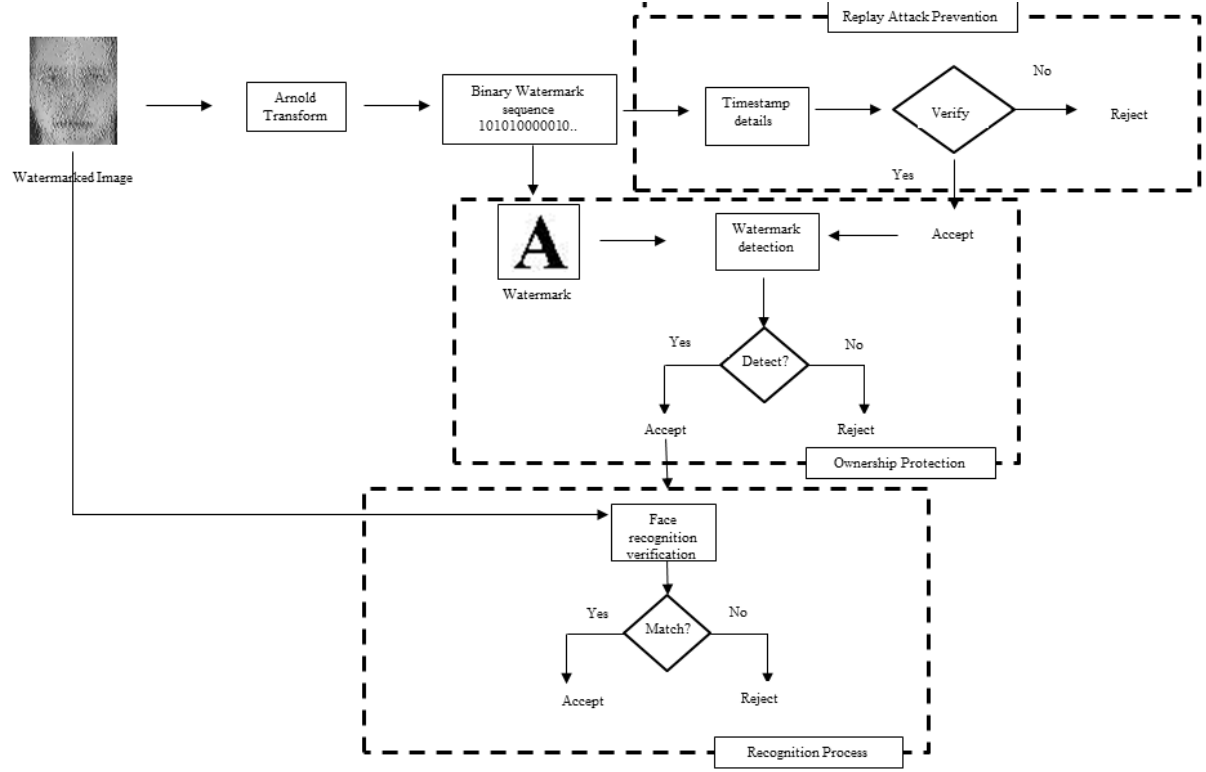
Repeat steps 6 and 7 until the entire watermark is successfully embedded into the remaining blocks. Apply inverse DCT to each block to construct the watermarked face image.

#### *b) Watermark extraction module*

The overall watermark extraction process is illustrated in Figure 4.8, and the details of the steps are given after that.

The watermark extraction steps are very closely related to the watermark embedding steps. In essence, the watermark can be extracted by reversing the embedding steps provided the location of the embedded watermark is known. As the scheme is based on blind watermarking concepts, the original image is not needed as a reference. There are two

variables needed for extraction: the locations of the watermark bits and the value of the modulus R. The extracted bits are assembled to obtain the watermark pattern and then the inverse Arnold transformation is applied.



**Figure 4.8:** Watermark extraction process

Step 1.

Detect the face area of the watermarked face image.

Step 2.

Divide the watermarked image into 8x8 blocks and convert each block into the DCT frequency domain.

Step 3.

Extract the watermark bits using the equation below and the embedded watermark location. Let  $C(k,l)^*$  be the DCT chosen frequency coefficients of the embedded watermark,  $eb$  the extracted watermark bit, and  $R$  the modulus.

$$eb = \begin{cases} 0, & \text{if } (C(k, l) \bmod R) < \frac{R}{2} \\ 1, & \text{if } (C(k, l) \bmod R) \geq \frac{R}{2} \end{cases} \quad (12)$$

Step 4.

Repeat steps 2 and 3 on each block until all watermark bits have been extracted and concatenated into a watermark pattern.

Step 5.

Inverse the watermark pattern with the Arnold transformation.

Step 6.

Reconstruct the watermark pattern to obtain the extracted watermark.

The watermark embedding and extraction processes are used at runtime as well as in all the five experiments, which we are now in a position to present.

#### **4.3.2 Experiment 1 - Determining the frequency band for watermarking**

This experiment is to determine the best frequency band to place the watermarks in an image, with the highest level of accuracy for face recognition, as well as the highest level of accuracy for watermark detection and recognition.

##### **4.3.2.1 Implementation**

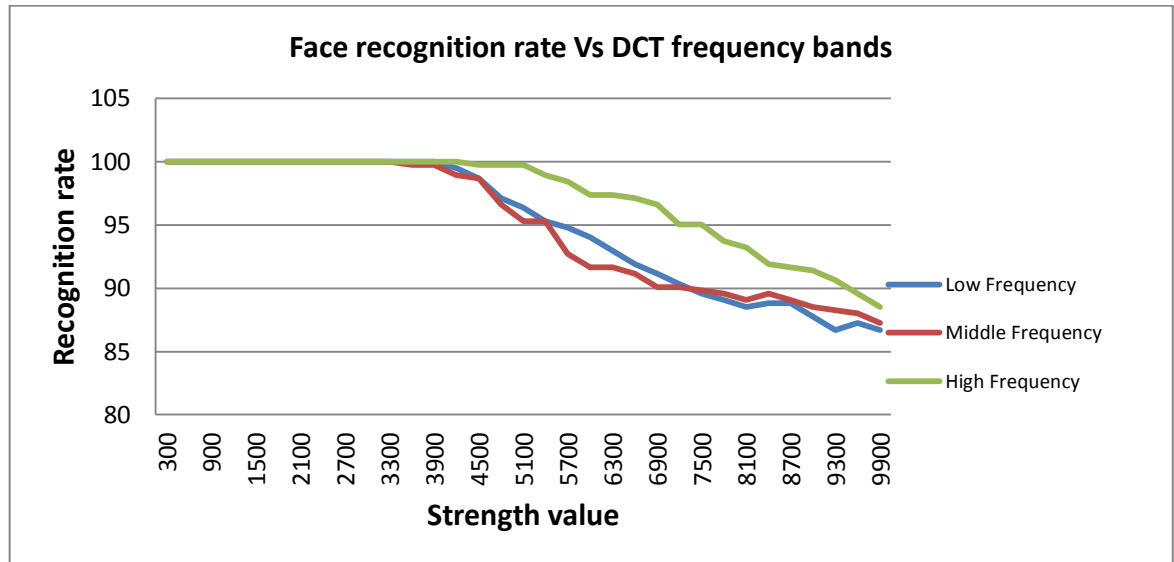
The experiment is conducted with a set of face images of forty persons, with ten different facial expressions for each person. As such, four hundred face images are used in this experiment for each frequency band. In this experiment, the Matlab tool is selected to carry out the watermarking process (embedding and detecting the watermark) as well as for the face recognition process where PCA is used as the face recognition algorithm to measure the accuracy rate. The detailed steps are as follows:

- i. Every face image is embedded with the watermark in the low frequency band area.
- ii. The watermarked face images are tested in the system to measure the face recognition accuracy rate as well as the watermark detection rate.
- iii. The strength value of the watermark is increased slowly to find out at which level the accuracy and detection rate begins to deteriorate.
- iv. Repeat step i with the middle and high frequency band areas.

#### 4.3.2.2 Results

##### a) Accuracy - Maintaining the accuracy of face recognition with high watermark strengths

It is essential to investigate which frequency band has the least effect on the face recognition rate due to the embedded watermark. The results show that, as the strength value of the watermark increases, the face recognition rate for the middle frequency bands starts to decrease first, followed by the low bands and finally the high bands.



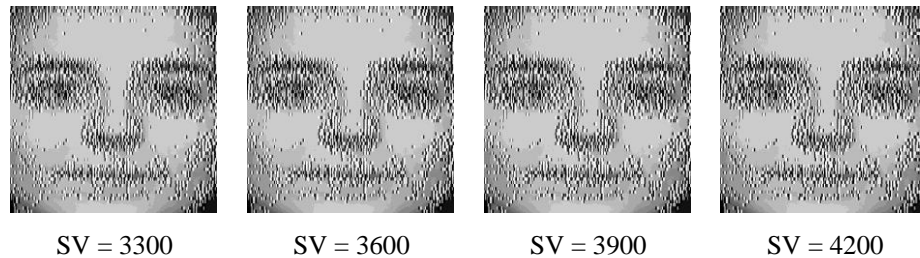
Strength Value (Modulus)	300	900	1500	2100	2700	3000	3300	3600	3900	4200	4500
Low Frequency	100	100	100	100	100	100	100	100	100	99.48	98.70

Middle Frequency	100	100	100	100	100	100	100	<b>99.74</b>	99.74	98.96	98.70
High Frequency	100	100	100	100	100	100	100	100	100	100	<b>99.74</b>

**Figure 4.9:** Face recognition accuracy rate comparison with each DCT frequency band under different strength value

Figure 4.9 above shows the performance for the face recognition rate for each DCT frequency band. The underlying idea is to select the maximum strength value for the watermark where the face recognition still has 100% accuracy for feature extraction. Referring to Figure 4.9, the recognition rate begins to decrease around the strength value of 4200. Therefore, it can be summarized that the high frequency band is the best location to maximise the watermark strength while maintaining the face recognition rate.

Figure 4.10 shows the quality of the face image after embedding the watermark with different watermark strengths. It can be seen that at a very high watermark strength of 4200, where the recognition rate is still maintained at 100%, perceptibility is still quite high even with the naked eye.



**Figure 4.10:** The quality of the face image for different watermark strength values

#### b) Detection - existence of watermark for acceptance or rejection

At the same time, it is also crucial to look at the watermark detection rate on each frequency band to balance with the face recognition rate. The proposed scheme not only needs to have a high face recognition rate but also a high watermark detection rate, with or without intruder attacks. The detection rate is measured using the Normalized Correlation (NC) score.

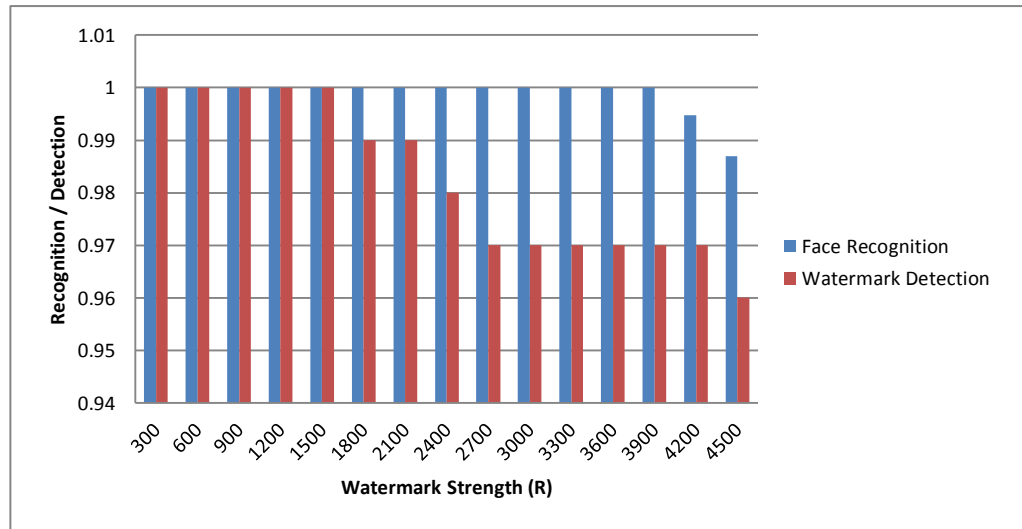


The previous experiment (a) showed that a 100% face recognition rate can still be maintained up to a certain watermark strength value for each frequency band. This experiment looks at the watermark detection rates up to those specific values. From the results (see Table 4.3), it can be concluded that the watermark detection rate can be maintained at a high level on the low frequency band as the watermark strength value increases. In general, it is universally recognized that a watermark detection rate of over the threshold value of 0.75 is considered acceptable, as at such rates the watermark can still be fully recovered (Al-Haj, 2007).

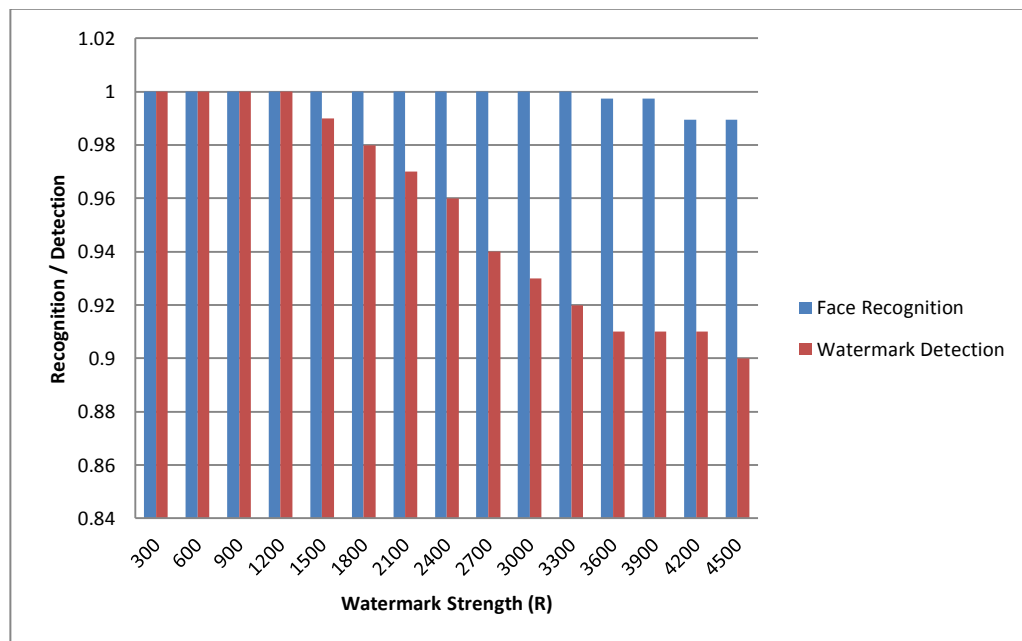
**Table 4.3:** Detection rate for different frequency band

Watermark Strength (R)	Detection rate (NC)		
	Low Freq.	Middle Freq.	High Freq.
300	1	1	1
600	1	1	1
900	1	1	1
1200	1	1	0.99
1500	1	0.99	0.98
1800	0.99	0.98	0.97
2100	0.99	0.97	0.96
2400	0.98	0.96	0.95
2700	0.97	0.94	0.94
3000	0.97	0.93	0.94
3300	0.97	0.92	0.94
3600	0.97	0.91	0.94
3900	0.97	0.91	0.94

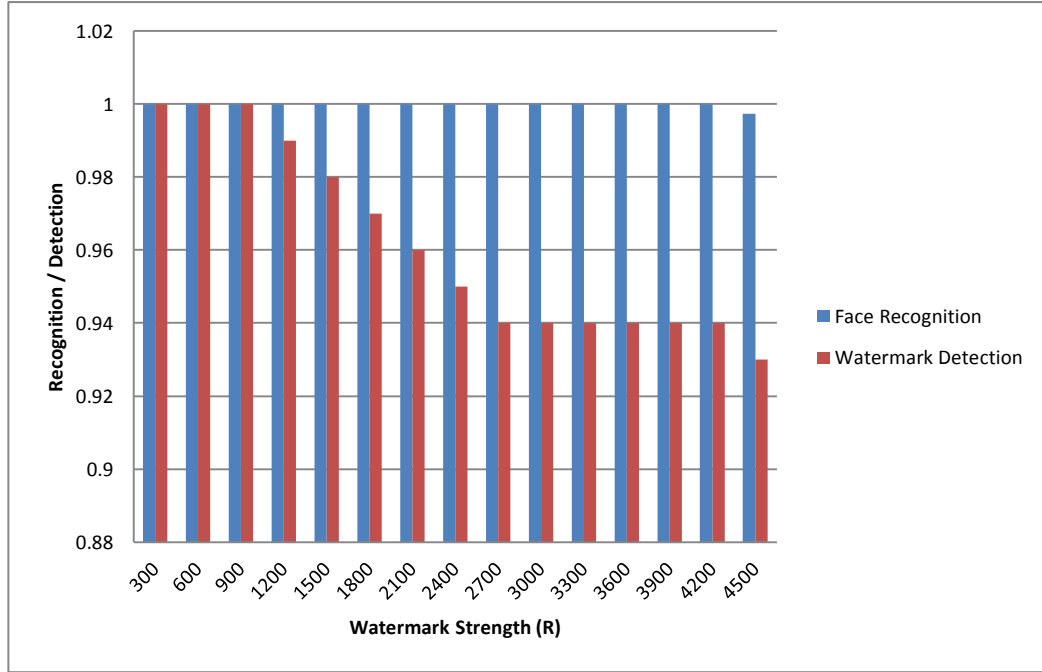
The comparisons for face recognition and watermark detection rates for each frequency band are then compiled in Figures 4.11 to 4.13 in order to help determine which frequency band should be finally selected for watermark embedding.



**Figure 4.11:** Comparison of face recognition and watermark detection rates for watermarks embedded in the low frequency bands



**Figure 4.12:** Comparison of face recognition and watermark detection rates for watermarks embedded in the middle frequency bands



**Figure 4.13:** Comparison of face recognition and watermark detection rates for watermarks embedded in the high frequency bands

#### 4.3.2.3 Discussion

From the first experiment (a), it is found that the face recognition rate performs better in the high frequency band, whereas the second experiment shows that the low frequency band outperform the higher band on the watermark detection rate.

From the Figures 4.11 to 4.13, it can be seen that all watermark detection rates are above the threshold value of 0.75 in all frequency bands. However, both face recognition and watermark detection rates are mostly maintained at high levels in the low frequency bands. This then leads to the conclusion that the low frequency bands are the most suitable for watermark embedding.

The watermark strength value for the last point of the highest recognition rate (100%) in the low frequency bands is then selected for the evaluation of the robustness value of the proposed scheme – which turns out to be 3900.

### **4.3.3 Experiment 2 – Non degradation of PCA and DCT due to the combination**

This experiment is to validate the claim that the use of DCT will not degrade PCA-based face recognition, and vice versa.

Recall the explanation given earlier in 4.2.2 and Figure 4.1 with path 1 and path 2. The analytical result validated by experiment as presented by Weilong Chen, Meng Joo Er, and Shiqian Wu (2005) as shown by path 1 will have the experiment repeated here. The other part of the experiment is the application of DCT following an application of PCA, i.e. path 2, in an effort to show that PCA also does not degrade the accuracy of DCT.

The experiment is carried out for both paths with the same input images, with a hope to show that the results are identical with the input images. Should this be the case, given that PCA has been shown not to degrade DCT (Path 1), identical results from Path 2 would indicate that DCT also does not degrade PCA.

Recall that both paths result in essentially compressed coefficient files. For Path 1, the DCT produces frequencies, which are then compressed by the DCT (Compressed Frequency 1). For Path 2, the PCA compresses the image file, and the DCT produces the frequencies of the compressed file (Compressed Frequency 2). These two files at face value are quite different, but equality may be shown by reconvertng the files resulting from both paths into pixel files and then both are compared to the respective original input images. For the comparison, the structural similarity (SSIM) index is used, and recall that the closer the value is to 1, the closer are the compared images.

#### **4.3.3.1 Implementation**

The experiment is conducted with a set of face images of forty different persons. The experiment first validates path 1, by showing that the output pixel files are identical to the input images, i.e. with an SSIM index of 1. This is then followed by comparing the results of path 2 with the input images, with the hope of similar results.

For PCA in the experiment, 20 principal components are used. In path 1, the face image is first converted into the frequency domain using DCT, after which the DCT coefficients

are compressed using PCA. The compressed DCT coefficients are then reconstructed back into a pixel file using the Inverse DCT (IDCT) technique (Gonzalez and Woods, 2002). As for path 2, the face image is first compressed using PCA, after which the compressed face image is then converted into the DCT frequency domain and then reconstructed back into a pixel file using IDCT.

#### 4.3.3.2 Results

The SSIM index measurements for the similarity values between the original face images and the output pixel files for path 1 and path 2 are as given in the table 4.4 below.

**Table 4.4:** The SSIM index measurements for Path 1 and Path 2

Face images	SSIM	
	Path 1	Path 2
Person 1	1	0.9216
Person 2	1	0.8692
Person 3	1	0.9543
Person 4	1	0.8950
Person 5	1	0.9387
Person 6	1	0.8938
Person 7	1	0.8936
Person 8	1	0.9518
Person 9	1	0.9290
Person 10	1	0.9216
Person 11	1	0.8798
Person 12	1	0.9402
Person 13	1	0.9089
Person 14	1	0.8717
Person 15	1	0.8670
Person 16	1	0.8730
Person 17	1	0.9053
Person 18	1	0.9111
Person 19	1	0.9320

Person 20	1	0.9006
Person 21	1	0.9287
Person 22	1	0.8929
Person 23	1	0.9383
Person 24	1	0.9016
Person 25	1	0.9295
Person 26	1	0.9311
Person 27	1	0.8818
Person 28	1	0.9044
Person 29	1	0.9307
Person 30	1	0.9221
Person 31	1	0.9113
Person 32	1	0.8732
Person 33	1	0.9223
Person 34	1	0.8687
Person 35	1	0.9397
Person 36	1	0.8658
Person 37	1	0.8655
Person 38	1	0.9131
Person 39	1	0.9420
Person 40	1	0.9107

#### 4.3.3.3 Discussion

The results above show that for path 1 the compressed face images are exactly the same (identical) to the respective original face images, as stipulated by Weilong, Meng and Shiqian (2005).

As for path 2, the compressed face images have different SSIM values, but are all very close to 1. This shows that there is some disturbance in the quality compared with the original face images. As mentioned in 4.2.2, the SSIM threshold value of 0.85 is considered acceptable, which is the case here. *[Note: Admittedly, this threshold value of 0.85 is essentially a conjecture. Further experiments will have to be conducted to ascertain the*

*correct threshold value (comparable to the universally accepted watermark detection rate of 0.75 – see Experiment 1 above). This will be left for future work.]*

#### **4.3.4 Experiment 3 - Replay attack prevention – system rejection of captured data**

This experiment is to validate the three types of rejection of resubmitted sniffed images (with possible modifications), captured at the positions and resubmitted at the positions as given in Table 4.2 earlier, with the vulnerable positions a, b, c, d, e, f, g being as given in Figure 3.8 earlier.

##### **4.3.4.1 Implementation**

The experiment results will also include: Additional - Logo does not exist (at positions a, g). Each experiment is conducted with forty face images from ten different persons. The persons are randomly picked from the database mentioned earlier. Essentially, the face images are only selected from the set with true positive acceptance.

We refer to Table 4.1 earlier, which provides the foundation for the validation criteria at each position in the system. There are three positions at which the system embeds the watermark – at position b (logo and timestamp), at position f (additional timestamp) and at position g (logo only). Recall that the purpose of embedding the watermark at these positions are to protect the ownership of face image (logo) as well as ensure the data transmitted is fresh and it is not one captured from an earlier session and then resubmitted back into the system (timestamp).

The watermarked face image may be captured at positions b, f and g only, and then resubmitted back at positions a and b only (there is nothing to be gained from resubmitting at f or g).

- At position a, a mechanism in the sensor module can detect the presence of the logo watermark in the face image. If the mechanism is able to extract the logo from the face image, the current transaction is immediately rejected as it shows that the face image belongs to this system and has been processed earlier.

- As for resubmission at position b, the watermark timestamp (the time the face image leaves from position a) is used to check against the current time the image arrives at position c. If the embedded timestamp has lapsed the current time considerably, the current transaction is rejected, as it shows that the face image must have been a resubmission back into the system from an earlier session.

The other positions where biometric data may be captured from are at positions c, d and e. However, the data there are feature values and thus can only be resubmitted back at positions c and d (again there is nothing to be gained from resubmitting at e). In this scenario, the timestamp originally embedded at position a would now be part of the feature values of the subject data and can be compared at position d (matching module) with the timestamp features coming from the object database, based on the face recognition system itself. A subject data containing the timestamp from an earlier session would not match with the object data containing the timestamp from the current session. The current transaction will then be rejected. Notice here that watermark extraction is not necessary at both positions c and d, as the validation is done by the matcher module of the face recognition system.

#### 4.3.4.2 Results

From the experiment, the results are as follows.

a) Rejection 1 - Illegitimate presence of logo (at point a)

Rejection at point a is based on the presence of a logo within the submitted image.

**Table 4.5:** Rejected status on Illegitimate presence of logo (at point a)

Watermarked face images	Stolen at	Reinsertion at	Rejection at	Rejected
Person 1	b	a	a	Yes
Person 2	b	a	a	Yes
Person 3	b	a	a	Yes
Person 4	b	a	a	Yes
Person 5	b	a	a	Yes



Person 6	b	a	a	Yes
Person 7	b	a	a	Yes
Person 8	b	a	a	Yes
Person 9	b	a	a	Yes
Person 10	b	a	a	Yes
Person 1	f	a	a	Yes
Person 2	f	a	a	Yes
Person 3	f	a	a	Yes
Person 4	f	a	a	Yes
Person 5	f	a	a	Yes
Person 6	f	a	a	Yes
Person 7	f	a	a	Yes
Person 8	f	a	a	Yes
Person 9	f	a	a	Yes
Person 10	f	a	a	Yes
Person 1	g	a	a	Yes
Person 2	g	a	a	Yes
Person 3	g	a	a	Yes
Person 4	g	a	a	Yes
Person 5	g	a	a	Yes
Person 6	g	a	a	Yes
Person 7	g	a	a	Yes
Person 8	g	a	a	Yes
Person 9	g	a	a	Yes
Person 10	g	a	a	Yes

b) Rejection 2 - Timestamp does not tally (at point b)

Rejection at point b is based on the value of the timestamp not within the acceptable range of the current time.

**Table 4.6:** Rejected status on Timestamp does not tally (at point b)

Watermarked face images	Stolen at	Reinsertion at	Rejection at	Rejected
Person 1	b	b	b	Yes
Person 2	b	b	b	Yes

Person 3	b	b	b	Yes
Person 4	b	b	b	Yes
Person 5	b	b	b	Yes
Person 6	b	b	b	Yes
Person 7	b	b	b	Yes
Person 8	b	b	b	Yes
Person 9	b	b	b	Yes
Person 10	b	b	b	Yes
Person 1	f	b	b	Yes
Person 2	f	b	b	Yes
Person 3	f	b	b	Yes
Person 4	f	b	b	Yes
Person 5	f	b	b	Yes
Person 6	f	b	b	Yes
Person 7	f	b	b	Yes
Person 8	f	b	b	Yes
Person 9	f	b	b	Yes
Person 10	f	b	b	Yes
Person 1	g	b	b	Yes
Person 2	g	b	b	Yes
Person 3	g	b	b	Yes
Person 4	g	b	b	Yes
Person 5	g	b	b	Yes
Person 6	g	b	b	Yes
Person 7	g	b	b	Yes
Person 8	g	b	b	Yes
Person 9	g	b	b	Yes
Person 10	g	b	b	Yes

c) Rejection 3 - Feature values do not match (at point d)

Rejection at point d is done by the face recognition Matcher, also based on the features converted from the timestamp in the submitted image which do not match with the features converted from the timestamp converted from the image coming from the object database.

**Table 4.7:** Rejected status on Feature values do not match (at point d)

Watermarked face images	Stolen at	Reinsertion at	Rejection at	Rejected
Person 1	c	c	d	Yes
Person 2	c	c	d	Yes
Person 3	c	c	d	Yes
Person 4	c	c	d	Yes
Person 5	c	c	d	Yes
Person 6	c	c	d	Yes
Person 7	c	c	d	Yes
Person 8	c	c	d	Yes
Person 9	c	c	d	Yes
Person 10	c	c	d	Yes
Person 1	c	d	d	Yes
Person 2	c	d	d	Yes
Person 3	c	d	d	Yes
Person 4	c	d	d	Yes
Person 5	c	d	d	Yes
Person 6	c	d	d	Yes
Person 7	c	d	d	Yes
Person 8	c	d	d	Yes
Person 9	c	d	d	Yes
Person 10	c	d	d	Yes
Person 1	d	c	d	Yes
Person 2	d	c	d	Yes
Person 3	d	c	d	Yes
Person 4	d	c	d	Yes
Person 5	d	c	d	Yes
Person 6	d	c	d	Yes
Person 7	d	c	d	Yes
Person 8	d	c	d	Yes
Person 9	d	c	d	Yes
Person 10	d	c	d	Yes
Person 1	d	d	d	Yes
Person 2	d	d	d	Yes
Person 3	d	d	d	Yes

Person 4	d	d	d	Yes
Person 5	d	d	d	Yes
Person 6	d	d	d	Yes
Person 7	d	d	d	Yes
Person 8	d	d	d	Yes
Person 9	d	d	d	Yes
Person 10	d	d	d	Yes
Person 1	e	c	d	Yes
Person 2	e	c	d	Yes
Person 3	e	c	d	Yes
Person 4	e	c	d	Yes
Person 5	e	c	d	Yes
Person 6	e	c	d	Yes
Person 7	e	c	d	Yes
Person 8	e	c	d	Yes
Person 9	e	c	d	Yes
Person 10	e	c	d	Yes
Person 1	e	d	d	Yes
Person 2	e	d	d	Yes
Person 3	e	d	d	Yes
Person 4	e	d	d	Yes
Person 5	e	d	d	Yes
Person 6	e	d	d	Yes
Person 7	e	d	d	Yes
Person 8	e	d	d	Yes
Person 9	e	d	d	Yes
Person 10	e	d	d	Yes

d) Additional - Logo does not exist (at points a, g)

Rejection at point a is based on the existence of a logo, while rejection at point g is when the logo does not exist.

**Table 4.8:** Rejected status on Logo does not exist (at points a, g)

Attackers face images	Reinsertion at	Rejection at	Rejected
Person 1	a	a	Yes
Person 2	a	a	Yes
Person 3	a	a	Yes
Person 4	a	a	Yes
Person 5	a	a	Yes
Person 6	a	a	Yes
Person 7	a	a	Yes
Person 8	a	a	Yes
Person 9	a	a	Yes
Person 10	a	a	Yes
Person 1	g	g	Yes
Person 2	g	g	Yes
Person 3	g	g	Yes
Person 4	g	g	Yes
Person 5	g	g	Yes
Person 6	g	g	Yes
Person 7	g	g	Yes
Person 8	g	g	Yes
Person 9	g	g	Yes
Person 10	g	g	Yes

#### 4.3.4.3 Discussion

The results clearly fully validate the claims made.

#### 4.3.5 Experiment 4 - Robustness of the watermark scheme

This experiment is to determine the level of robustness of the watermark scheme. The robustness of the watermark scheme needs to be investigated to ensure that the watermark cannot be easily removed by an attacker.

##### 4.3.5.1 Implementation

From the results of Experiment 1, the lower frequency bands are chosen for watermark embedding, and the selected strength value for the watermark is 3900. For these chosen frequency bands and the watermark strength, this experiment is conducted with the same four hundred watermarked face images used for Experiment 1. Each watermarked face image is disturbed with various signal processing attacks (median filter, Gaussian noise, salt and pepper, JPEG compression) using the Matlab tool, after which the watermark is extracted to evaluate the quality preservation performance. The extracted watermark is compared with the original watermark, also using the Normalized Correlation (NC) score.

#### 4.3.5.2 Results

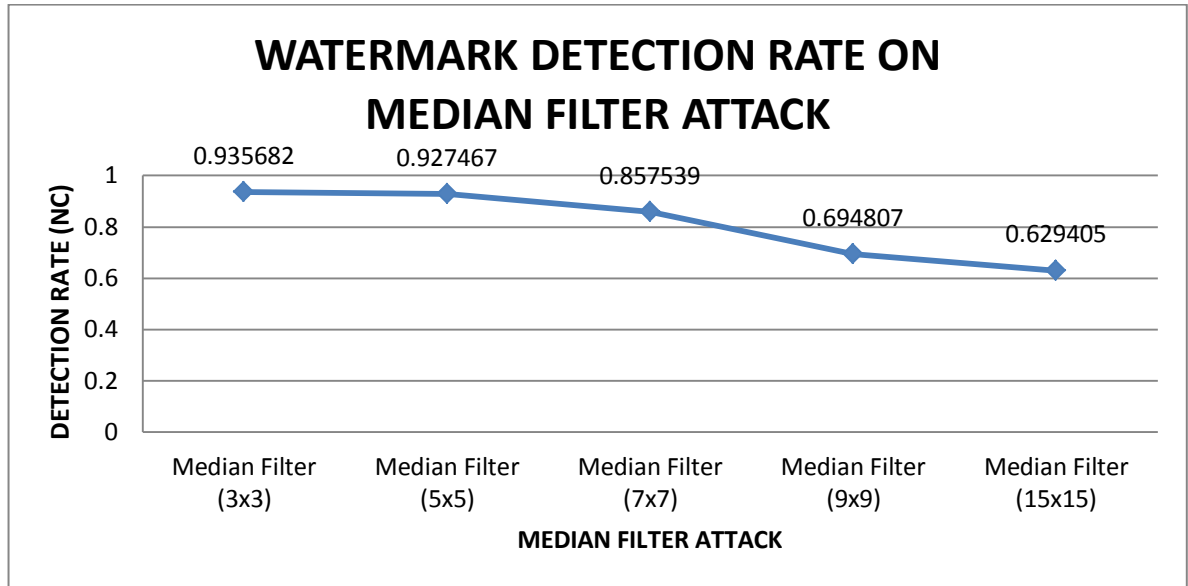
Table 4.9 gives the experiment results for robustness, followed by some details.

**Table 4.9:** Detection Rate after Attacks

Attack Type	Detection Rate (NC)
Median Filter (3x3)	0.935682
Median Filter (5x5)	0.927467
Median Filter (7x7)	0.857539
Median Filter (9x9)	0.694807
Median Filter (15x15)	0.629405
Gaussian Noise (0,0.01)	0.907509
Gaussian Noise (0,0.05)	0.891861
Gaussian Noise (0,0.1)	0.886505
Gaussian Noise (0.01,0)	0.967328
Gaussian Noise (0.02,0)	0.968085
Gaussian Noise (0.1,0)	0.973004
Gaussian Noise (0.05,0)	0.970751
Salt&Pepper (0.001)	0.963221
Salt&Pepper (0.002)	0.960227
Salt&Pepper (0.01)	0.940843
Salt&Pepper (0.05)	0.904951
Salt&Pepper (0.1)	0.893861
JPEG compression (10%)	0.807241
JPEG compression (30%)	0.883940

JPEG compression (50%)	0.914256
JPEG compression (70%)	0.938168
JPEG compression (90%)	0.959181

a) Median Filter attack



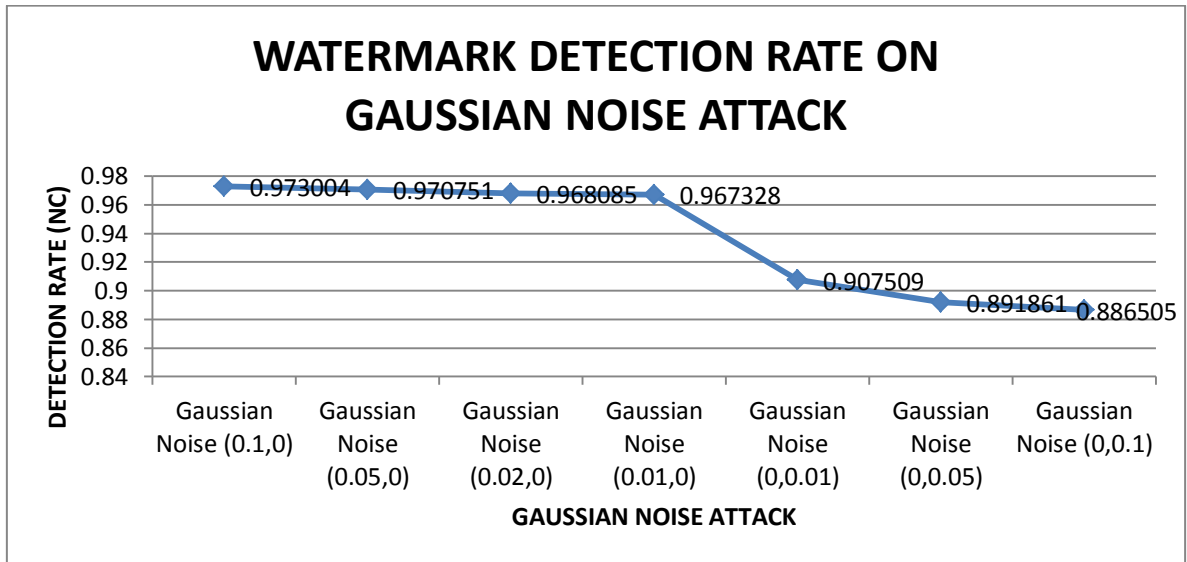
**Figure 4.14:** Detection rate after Median Filter attacks



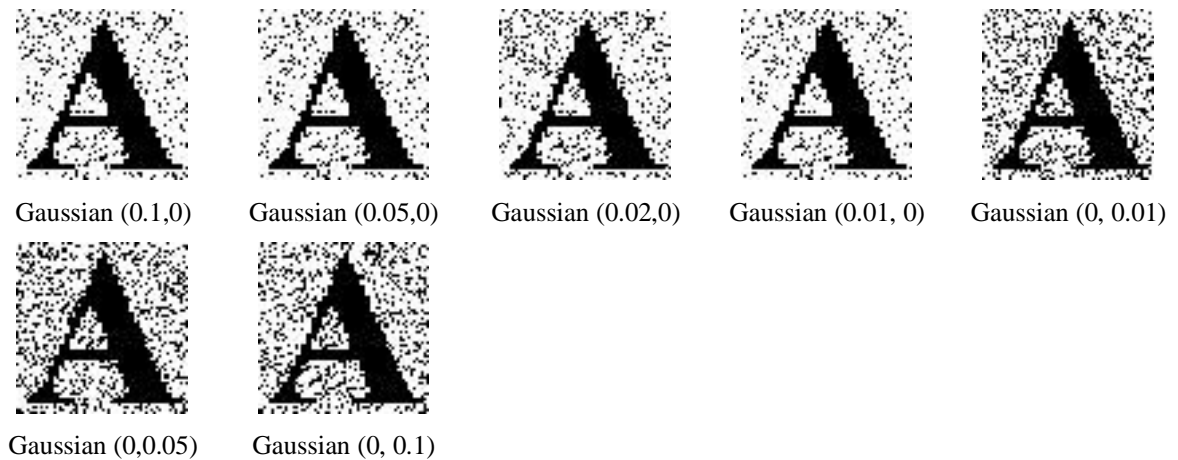
**Figure 4.15:** Quality of watermark image after Median Filter attacks

As investigated, the median filter has given some trouble to the watermark detection rate of the proposed watermarked face recognition scheme. Figure 4.14 shows that as the number of median filter value increases, the watermark detection rate decreases. It can be clearly seen that the embedded watermark can barely survive a median filter attack value of (9x9). Therefore it can be concluded that the DCT watermarking technique is only fairly resilient against median filter attacks.

b) Gaussian Noise attack



**Figure 4.16:** Detection rate after Gaussian Noise attacks



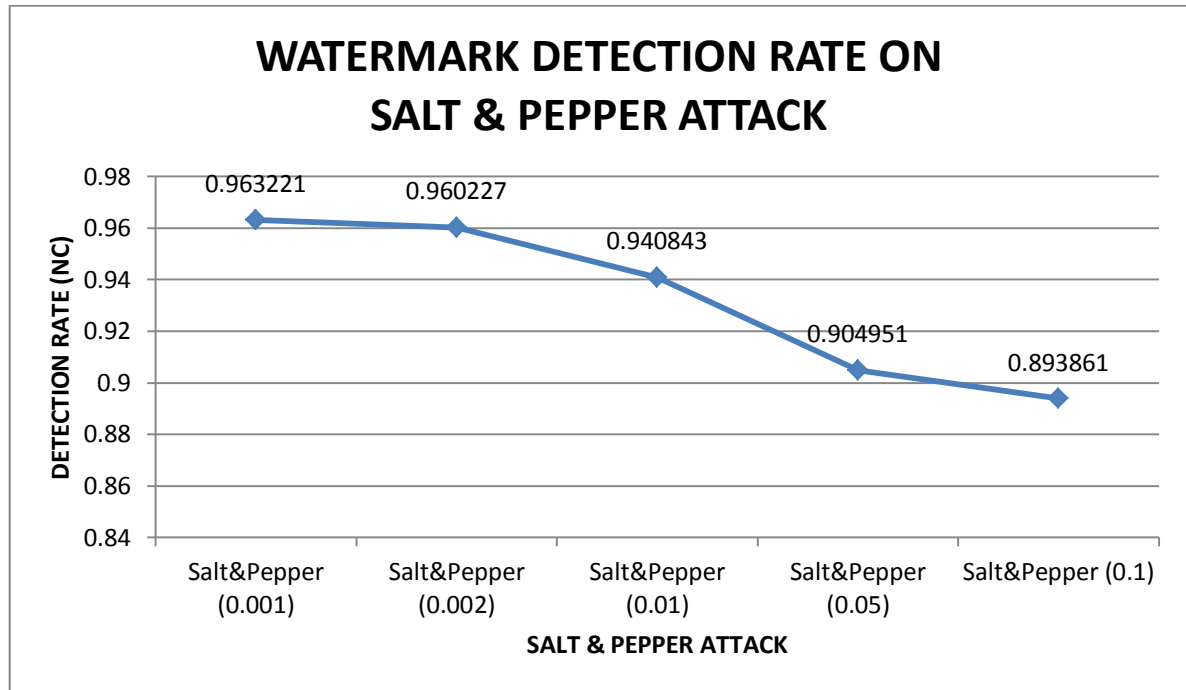
**Figure 4.17:** Quality of watermark image after Gaussian Noise attacks

Figure 4.16 above shows that the watermark detection rate decreases gently as we increase the value of the Gaussian Noise attack. The quality of the embedded watermark also can be seen to be barely disturbed as we can see that the watermark is almost fully

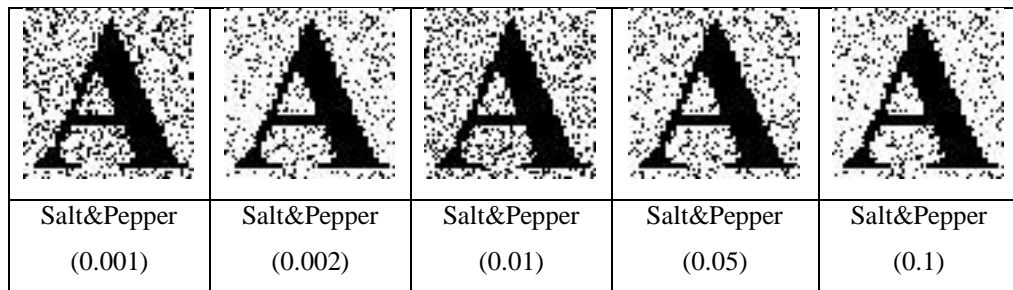


preserved. Therefore, it can be concluded that the proposed watermarked face recognition scheme is resilient against a Gaussian Noise attack.

c) Salt and Pepper attack



**Figure 4.18:** Detection rate after Salt and Pepper attacks

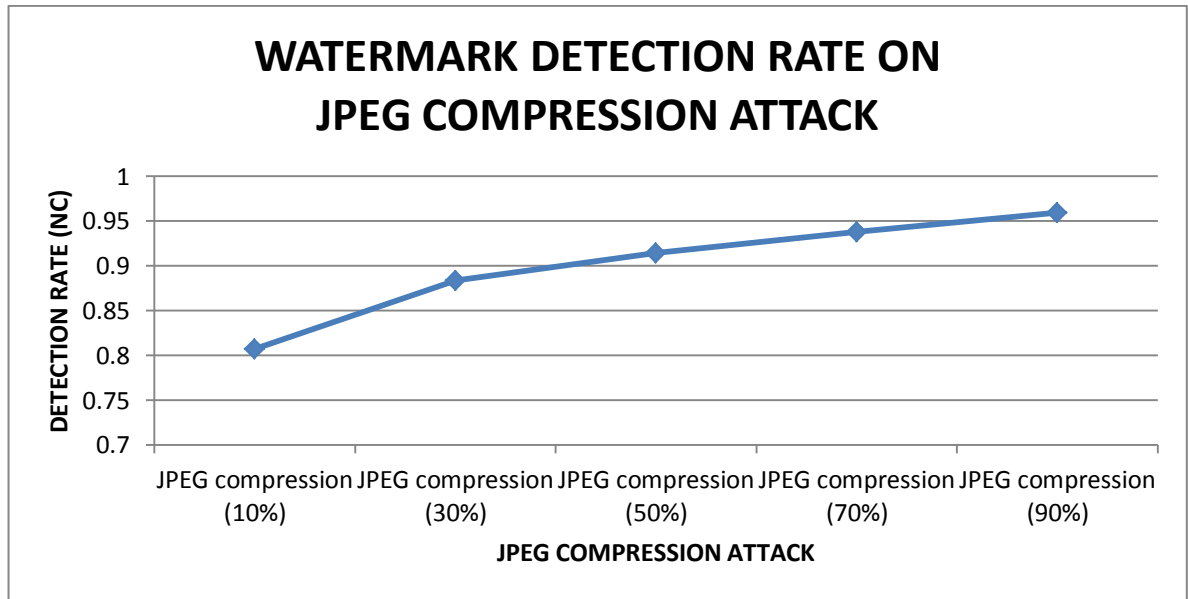


**Figure 4.19:** Quality of watermark image after Salt and Pepper attacks

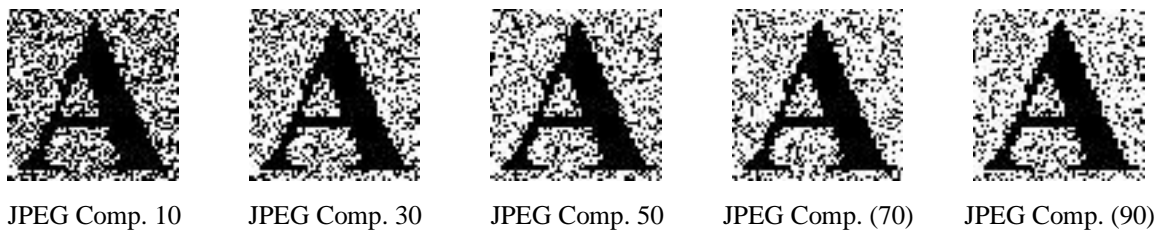
As can be seen clearly from Figure 4.18, the watermark detection rate slowly decreases as the salt and pepper attack increases. This is supported by Figure 4.19, where it can be noted that the attacks did not really affect the watermark detection. Therefore, it can be

concluded that the proposed watermarked face recognition scheme is also very robust against salt and pepper attacks.

d) JPEG Compression attack



**Figure 4.20:** Detection rate after JPEG compression attacks



**Figure 4.21:** Quality of watermark image after JPEG compression attacks

Figure 4.20 shows the detection rate on the embedded watermark after undergoing a JPEG compression attack. From the graph we can clearly see that the watermark detection rate increases as we raise the JPEG compression value on the watermarked image. It had been mentioned earlier in Chapter Two that according to Poljicak et al., (2011), the DCT approach is very robust to JPEG compression since JPEG itself makes use of DCT. This result shows that the proposed watermarked face recognition scheme is not only resilient to

a JPEG compression attack, but the JPEG compression may even increase the robustness of the proposed scheme. This is nothing new as Poljicak et al., (2012) had discovered that certain signal processing techniques could influence the watermark detection rate.

#### **4.3.5.3 Discussion**

From the results, it can be seen that the proposed scheme is resilient especially against JPEG compression, Gaussian noise, as well as salt and pepper attacks, where the embedded watermark is hardly disturbed from such attacks. As for the median filter attack, the proposed scheme is able to survive up to 7x7 filters, which indicates that it is fairly robust.

### **4.3.6 Experiment 5 - Comparative study of watermarking techniques**

This experiment is to validate the choice of DCT as the watermarking technique to be coupled with DCT, by comparing it with two other most used watermarking techniques – namely LSB (spatial) and DWT (transform/frequency).

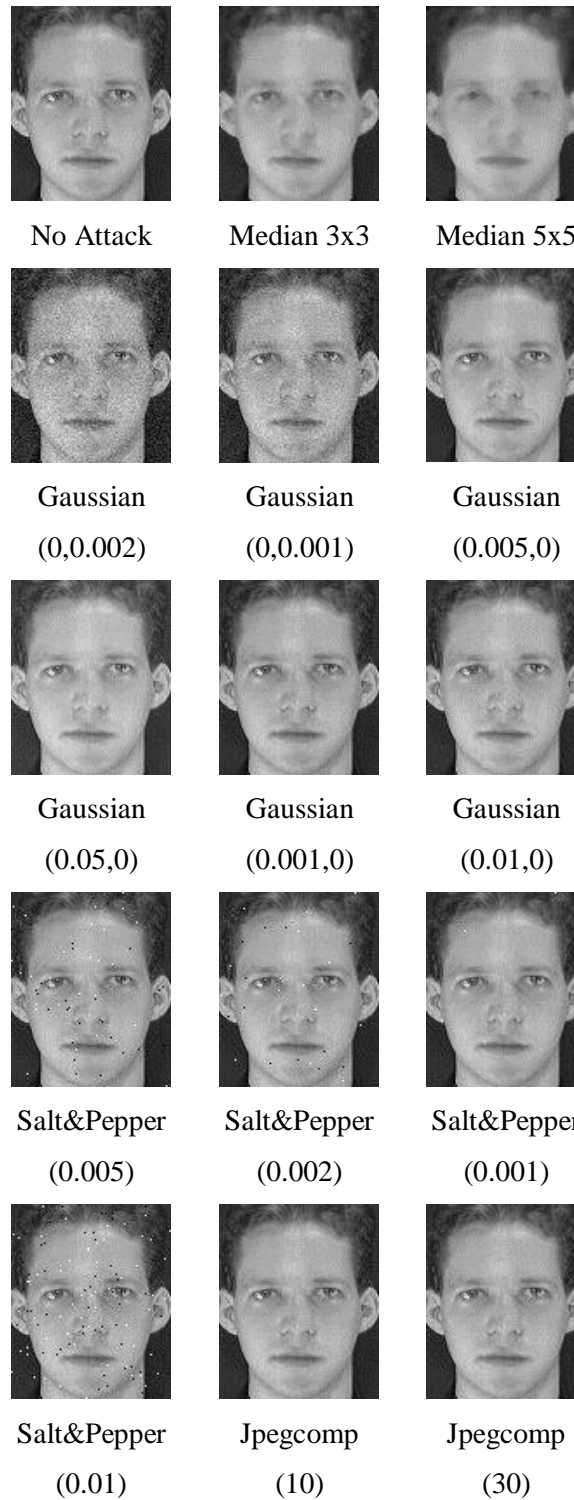
As with most of the earlier experiments, this experiment is also conducted with face images of forty persons, each with ten different facial expressions, giving a total of four hundred different images. The images are embedded using the three said watermark techniques. The same earlier accuracy measurements for face recognition, watermark detection, and watermark robustness are used for this experiment. The measures are to see how much degradation would the watermark technique affect the PCA recognition rate in the three mod combinations/models:

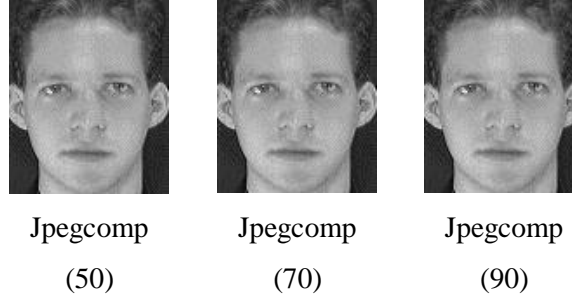
- Model 1: PCA-LSB
- Model 2: PCA-DCT (our choice)
- Model 1: PCA-DWT

#### **4.3.6.1 Implementation**

In the initial part of the experiment, the three models are evaluated based on face recognition accuracy as well as watermark robustness against signal processing attacks,

essentially by adding noises, some effects of which are illustrated in Figure 4.22. This experiment is very similar to the previous experiment where the Matlab tool is chosen to run all the signal processing attacks.





**Figure 4.22:** Samples of various attacked images

The face recognition rate is measured using the PCA algorithm to investigate the effect of the watermarking. The correlation factor, as given by the following equation (Sangeeta and Anjali, 2010), is computed to measure the similarity between the embedded watermark denoted as  $w$  and  $\hat{w}$  as the extracted watermark for watermark detection.

$$\rho(w, \hat{w}) = \frac{\sum_{i=1}^N w_i \hat{w}_i}{\left( \sqrt{\sum_{i=1}^N w_i^2} \sqrt{\sum_{i=1}^N \hat{w}_i^2} \right)} \quad (16)$$

#### 4.3.6.2 Results

##### *Experiment A – Face recognition rate*

The experiment results are given in Table 4.10, which shows the face recognition verification accuracy rate of the three models when exposed to the various noise attacks. The results show that all the models produce high recognition rates with little difference amongst them under normal circumstances when no attacks are taking place. Nonetheless, Model 2 (PCA-DCT) still has the best recognition rate at 98.91 %.

When under attack, the results show that the recognition rate slightly decreases for all the models except for under the Gaussian Noise (0.01.0) attack, where all the recognition rates drop tremendously. This is obviously because the face image cannot be recognized anymore as the attack is simply too heavy and has destroyed the image. In the rest of the

table, it can be seen that, overall, Model 2 has better results when compared with the two models.

**Table 4.10:** Face recognition rate comparison for Model 1, Model 2 and Model 3 under various attacks

<b>Attack</b>	<b>Model 1 (PCA + LSB)</b>	<b>Model 2 (PCA + DCT)</b>	<b>Model 3 (PCA + DWT)</b>
No attack	98.74	<b>98.91</b>	98.79
Median Filter (3x3)	95.96	<b>96.24</b>	95.94
Median Filter (5x5)	84.87	<b>85.27</b>	84.75
Gaussian Noise (0,0.001)	98.32	98.48	<b>98.66</b>
Gaussian Noise (0,0.002)	97.95	<b>98.62</b>	98.47
Gaussian Noise (0.001,0)	98.74	<b>98.91</b>	98.79
Gaussian Noise (0.005,0)	88.41	<b>90.76</b>	88.72
Gaussian Noise (0.01,0)	19.84	<b>26.49</b>	20.68
Salt&Pepper (0.001)	98.58	<b>98.78</b>	98.68
Salt&Pepper (0.002)	98.37	<b>98.62</b>	98.45
Salt&Pepper (0.005)	97.72	98.03	<b>98.08</b>
Salt&Pepper (0.01)	96.16	<b>96.57</b>	95.78
JPEG compression (10%)	98.74	<b>98.91</b>	98.79
JPEG compression (30%)	98.74	<b>98.91</b>	98.79
JPEG compression (50%)	98.74	<b>98.91</b>	98.79
JPEG compression (70%)	98.74	<b>98.91</b>	98.79
JPEG compression (90%)	98.74	<b>98.91</b>	98.79

#### *Experiment B - Watermark detection (Robustness)*

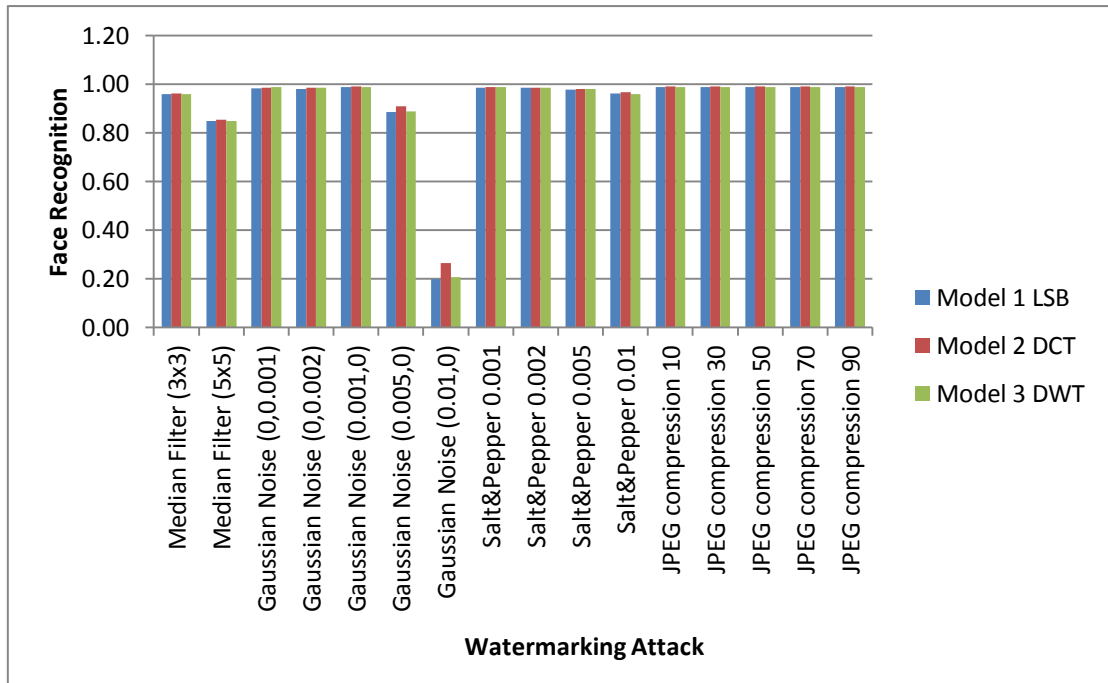
In this part of the experiment, the robustness of the three models is measured to find out the immunity of the watermark against attempts to remove or degrade unintentionally, with the same types of digital processing attacks. Table 4.11 gives the results, showing clearly that Model 2 outperforms the other models. *[Note also here that the detection rate of 0.75*

and above is considered acceptable, as the watermark can still be fully recovered (Al-Haj, 2007).]

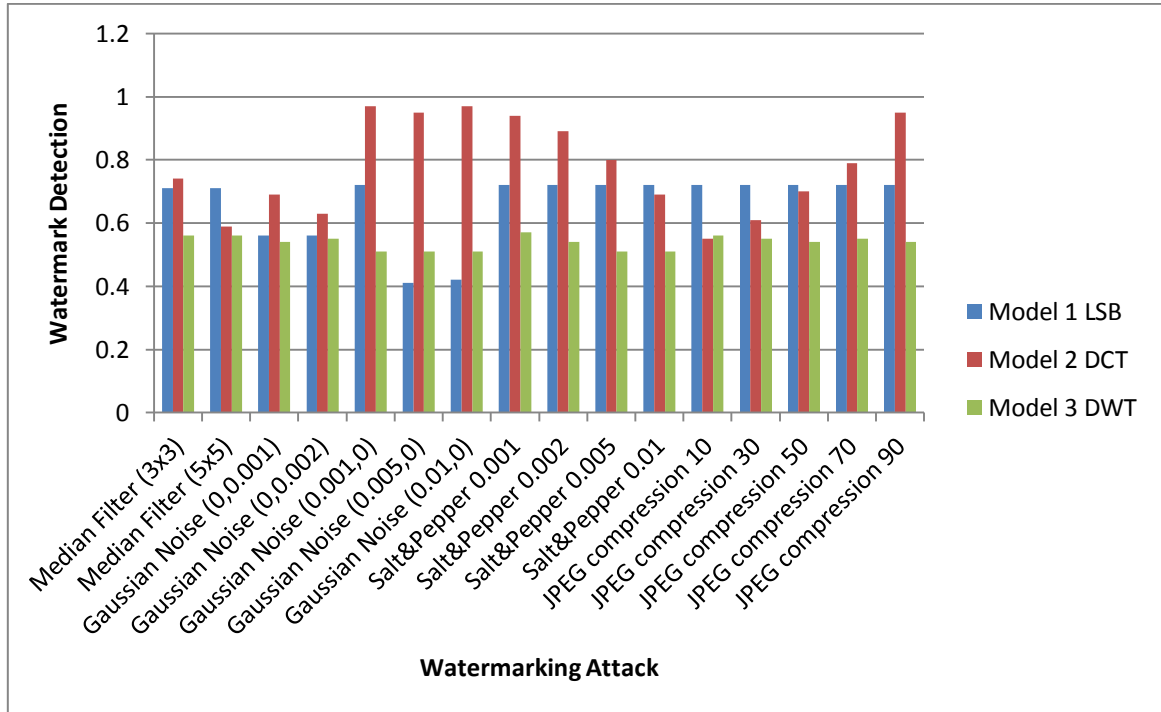
**Table 4.11:** Watermark detection rate comparison for Model 1, Model 2 and Model 3 under various attacks

<b>Attack</b>	<b>Model 1 (PCA + LSB)</b>	<b>Model 2 (PCA + DCT)</b>	<b>Model 3 (PCA + DWT)</b>
No attack	0.72	<b>0.97</b>	0.64
Median Filter (3x3)	0.71	<b>0.74</b>	0.56
Median Filter (5x5)	<b>0.71</b>	0.59	0.56
Gaussian Noise (0,0.001)	0.56	<b>0.69</b>	0.54
Gaussian Noise (0,0.002)	0.56	<b>0.63</b>	0.55
Gaussian Noise (0.001,0)	0.72	<b>0.97</b>	0.51
Gaussian Noise (0.005,0)	0.41	<b>0.95</b>	0.51
Gaussian Noise (0.01,0)	0.42	<b>0.97</b>	0.51
Salt&Pepper (0.001)	0.72	<b>0.94</b>	0.57
Salt&Pepper (0.002)	0.72	<b>0.89</b>	0.54
Salt&Pepper (0.005)	0.72	<b>0.80</b>	0.51
Salt&Pepper (0.01)	<b>0.72</b>	0.69	0.51
JPEG compression (10%)	<b>0.72</b>	0.55	0.56
JPEG compression (30%)	<b>0.72</b>	0.61	0.55
JPEG compression (50%)	<b>0.72</b>	0.70	0.54
JPEG compression (70%)	0.72	<b>0.79</b>	0.55
JPEG compression (90%)	0.72	<b>0.95</b>	0.54

The results from Tables 4.10 and 4.11 can be re-represented as in the following Figures 4.23 and 4.24 for a better presentation to compare the performance of the three models.



**Figure 4.23:** Face recognition rate comparison with methods of Model 1, Model 2 and Model 3 under various attacks



**Figure 4.24:** Watermark detection rate comparison with methods of Model 1, Model 2 and Model 3 under various attacks



#### **4.3.6.3 Discussion**

It can be clearly noted from the results above that the PCA-DCT combination (Model 2) outperforms the other two combinations, especially in terms of resilience against watermarking attacks. Analysing further, we would see that DCT performs better than DWT under frequency transform attacks. This shows that even though DWT is believed to have more accurate model features of HVS than DCT, it is found to be not robust against attacks (especially under JPEG compression attacks), and thus the adoption of DWT as a watermarking technique to protect the security of biometric systems is not recommended.

In conclusion, the results from the above show that the PCA-DCT combination (Model 2) is the best combination amongst the three for the watermarked face recognition scheme, showing both high recognition and watermark detection rates as well as robustness against various attacks.

#### **4.4 Conclusion**

This chapter presented the five experiments in an effort to validate the claims made there, namely (1) Determining the frequency band for watermarking, (2) Non degradation of PCA and DCT due to the combination, (3) Replay attack prevention – system rejection of captured data. (4) Robustness of the watermark scheme, and (5) Comparative study of watermarking techniques.

The results for experiment in (1) indicated that the best frequency for watermark embedding is in the low frequency band at 3,900, which maintains the recognition rate at 100% with the highest robustness value for the watermark, with the robustness being confirmed by (4). The results for (2) confirmed the full non-degradation for PCA after DCT, and with acceptable minor degradation for DCT after PCA, while (3) confirmed full protection against captured biometric data at the 28 situations under investigation. The experiment in (5) then confirms the best choice of PCA-DCT when compared with PCA-LSB and PCA-DWT.

Further research to improve the scheme by targeting other security issues is outlined in the next chapter.

# CHAPTER FIVE

## CONCLUSIONS AND FUTURE WORK

### 5.1 Summary

The research began with an analysis of biometric systems, with an emphasis on face recognition systems, and in particular with reference to the 8 positions of threats that have been listed out by Ratha et al., (2001), followed by a study of biometric watermarking algorithms proposed by previous researchers within the face recognition environment and these are classified according to their proposed solutions to the said threats.

The above had given a good idea towards proposing a watermarked face recognition scheme to enhance the security of face recognition systems, especially in terms of the authenticity of the data being transmitted. This watermarked face recognition scheme is the main objective.

For an implementation to validate the proposed scheme, the Principal Component Analysis (PCA) algorithm, the most popular holistic approach for face recognition, is singled out with the reasons backing the choice. For the watermarking techniques, the Least Significant Bits (LSB), Discrete Cosine Transform (DCT), and Discrete Wavelet Transform (DWT) techniques, being representative of their respective approaches, are looked at to complement the PCA to enhance its level of security. An analysis shows that the DCT would probably perform the best, and a further analysis is carried out to ensure that the PCA—DCT combination will not degrade the performance of the individual systems.

The proposed watermarked face recognition scheme is then worked into the PCA—DCT combination, followed by a check on the 8 vulnerable positions (refer to Figure 1.1) where data may be intercepted and/or resubmitted to ensure the authenticity of the data being transmitted. Within the 64 (8x8) vulnerable positions, some are found to be not relevant, some are shown to be resolved (fully-protected), while the (few) remaining ones are left for future work.

Five experiments are conducted to validate the claims made in this research, which all proved successful:

- 1) Determining the frequency band for watermarking
- 2) Non-degradation of PCA and DCT due to the combination
- 3) Replay attack prevention – system rejection of captured data
  - a) Illegitimate presence of watermarks (logo)
  - b) Timestamp does not tally
  - c) Value of features do not match (based on the face recognition system)
- 4) Robustness of the watermarking scheme
- 5) Comparative study of watermarking techniques

Experiment 1 is a pre-requisite for all the other experiments; experiment 2 is towards non-degradation, supported by experiment 5, as the claim also includes a proposal for a secure face recognition algorithm and watermarking technique combination. Experiment 3 is for the main objective, while experiment 4 is for computing robustness of the proposed watermarked face recognition scheme.

## **5.2 Contributions**

While biometric techniques often offer reliable identification mechanisms, the problem of authenticity and integrity of the biometric data poses new issues. One fundamental advantage in biometric techniques is that biometric traits are irreplaceable as compared to passwords, locks or cards. A copy of biometric data will look identical to the original one. However, biometrics-based verification systems can only be trusted if the verifier system can guarantee that the biometric data came from the same legitimate person as the one at the time of enrolment. Watermarking on biometric data can fill this gap by ensuring the ownership of the said data. There is not much research done in combining the two technologies and there is indeed a need for more research to explore this idea further more

as the impact of this research will not only contribute to the security problem in biometric techniques but also to digital image processing in general.

This research contributes to a study on the combination of face recognition algorithm and watermarking techniques to enhance the security of face recognition systems. The main contributions are the following:

- 1) The proposed watermarked face recognition scheme of a suitable combination of a face recognition algorithm and a watermarking technique, namely the PCA-DCT combination, where the combination is shown not to degrade the performance of the individual systems.
- 2) The proposed watermarked face recognition scheme that will ensure the authenticity of the transmitted data in the face recognition system, in particular at the 8 vulnerable positions where data may be intercepted and/or resubmitted, and in doing so will enhance the level of security of the face recognition system (refer to Figure 3.8),
- 3) The proposed watermarked face recognition scheme, as required by any watermarking technique, is shown to be robust against signal processing attacks and in particular that the watermark cannot be easily removed by an attacker.

Within the proposed watermarked face recognition scheme, a logo and a timestamp are embedded as watermarks. The logo serves as identification if the face image is captured. The timestamp is the main security enhancer, which works essentially as a session ID, where a face image or feature set captured from within the process and then resubmitted back to the system will be immediately recognised as coming from a different session and will be rejected.

With positions a and h being not within the scope of this research, and that positions e, f, g, h being not relevant for resubmissions, the remaining  $7 \times 4 = 28$  situations have been found to be fully secured. This means that within the  $8 \times 8 = 64$  total vulnerable situations:

- $7 \times 4 = 28$  are fully covered with this proposal
- $7 \times 4 = 28$  are irrelevant

—  $1 \times 8 = 8$  are left for future work (position h)

### **5.3 Future work**

We conclude this thesis by elaborating on possible research directions that can be used to expand the research presented here. In general, the suggested future work would pertain to one of the three following areas:

- Components of the current work that can be complemented
- Extensions of the current work
- Applications of the results in the current work in other areas.

#### **5.3.1 Complementing current work**

##### **1) Presenting a printed image to the scanner (Position a)**

A fresh image is shown to the scanner (camera), possibly a picture of an authorised person. In this situation, the scanner has to recognise that it is a printed image, and not that of a physical person. There is a need for a good method for this, but in the meantime, CCTVs may be deployed to monitor such a situation. Further enhancement to the face recognition system such as a deployment of a face liveness detection mechanism in order to guard against such spoofing could be considered.

##### **2) Captured image captured at the scanner**

Images can be captured from the scanner (position a) before the watermark is embedded. The images are then printed, and placed in front of the scanner. This can happen if the scanner is stored with a temporary memory, which can and perhaps should be removed. In any case, this situation is similar to the above (fresh image).

##### **3) Non-degradation of face recognition performance**

Analytical results validated by experiments as presented by Weilong, Meng and Shiqian (2005) have shown that DCT does not degrade the performance of PCA, at least in terms of the accuracy of face recognition when DCT is first applied on a pixel file to obtain a

frequency domain file (with changes in coefficients), and then followed by the application of PCA for compression as well as reconvert to an image (compressed file). The result is the same as that of a direct application of PCA on the original pixel file.

Ideally, we would want to have the same analytical results both ways, namely also for the application of DCT following an application of PCA which would then show that PCA also does not degrade the accuracy of DCT. This analytical result is definitely an area for future work.

However, as mentioned, proving this result is beyond the scope of this thesis, therefore experiments were conducted to show some form of validation of this result. Even in the experiments, which used the SSIM index to measure the similarity values (where the value 1 would indicate identical), the threshold value of 0.85 was considered reasonable. Further experiments will have to be conducted to ascertain the correct threshold value (comparable to the universally accepted watermark detection rate of 0.75).

### **5.3.2 Future further improvements**

1) Further research may explore others combination of face recognition algorithms within the holistic approaches, such as LDA (Linear Discriminant Analysis) or ICA (Independent Component Analysis), with watermarking techniques. PCA deals with the data as a whole as it tries to characterize variability in the data set without taking into account class membership of the data. LDA on the hand tries to take into account as much as possible the class discriminatory information (Putte et al., 2000). A new technique of ICA has been reported to improve and in many cases exceed the performance of PCA or LDA recognition based systems. Future work should therefore focus on the investigation of achieving the best face recognition accuracy rate from other holistic based algorithms.

2) The need of more robust watermarking schemes is required to survive watermarking attacks. Robustness has become one of the key properties in watermarking techniques. As a further extension to this research, in order to develop a much more robust watermarking scheme, other signal processing attacks such as histogram equalization and stretching,

dithering and resizing, should be considered in testing the robustness of the proposed schemes.

### **5.3.3 Applications in other domains**

1) Further investigation and experimentation into combination of other biometric techniques (e.g. fingerprint, iris) using holistic approaches as the recognition algorithms and combined with watermarking techniques is strongly recommended. A number of possible future studies using the same experimental set up are possible. It would be interesting to assess the effects of biometric recognition accuracy due to the embedding watermark technique as well as the robustness of the watermarked biometric recognition scheme.

2) The use of 3D based face recognition techniques as well as the use of other sensors instead of video cameras may also be considered.

### **5.4 Concluding remarks**

The contributions from this research constitute a solution step to the security problems associated with biometric authentication systems and to the area of digital image processing. In addition, it is hoped that the outcome of this research will stimulate further research by opening up more research gaps in the area of combining biometric and watermarking techniques.

## REFERENCES

- Abdullah, M. A., Dlay, S. S., & Woo, W. L. (2015). Securing Iris Images with a Robust Watermarking Algorithm based on Discrete Cosine Transform.
- Adler A. (2003). Sample images can be independently restored from face recognition templates. <http://www.site.uottawa.ca/~adler/publications/2003/adler-2003-fr-templates.pdf>. [accessed 12.05.15]
- Agreste, S., Andaloro, G., Prestipino, D., Puccio, L. (2006). An Image Adaptive Wavelet Based Watermarking of Digital Images. *Science Direct Journal of Computational and Applied Mathematics*, pp. 1-9.
- Ahmed, F., Moskowitz, I.S. (2005). Composite signature based watermarking for fingerprint authentication. *In: Proceedings of the ACM Workshop on Multimedia and Security (MMSEC 2005)*, pp. 799–802.
- Ahonen T., Hadid A., & Pietikainen M., (2006, Dec). Face Description with Local Binary Patterns: Application to Face Recognition. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 28(12), 2037-2041.
- Al-Haj, A. (2007). Combined DWT-DCT digital image watermarking. *Journal of Computer Science* 3(9), pp. 740-746.
- Asad J., Muhammad F., Muhammad A.M., hnran U., Shafique M.F., Bashir T., & Ashraf M.K., (2013). A new additive watermarking technique for multimodal biometric identification. *Journal of basic and applied science research*, 3(7), 935-942, 2013.
- Australian Biometrics Institute. Biometric vulnerability: A principled assessment methodology. White paper; 2008.
- Australian Defence Signals Directorate. EAL2 certification report for Iridian Technologies KnoWho authentication server and private ID. Certification Report 2003/31; 2003.
- Bamatraf, A., Ibrahim, R., Salleh, M.N. (2011). A new digital watermarking using combination of least significant bit (LSB) and inverse bit. *Journal of computing* 3(4), pp. 177-184.



- Bansal, R., Sehga, P., Bedi, P. (2012). Securing fingerprint images using a hybrid technique. *Proceedings of the International Conference on Advances in Computing, Communications and Informatics*, pp. 557-565.
- Barni, M., Bartolini, F., Cappellini, V., Piva, A. (1998). A DCT-domain system for robust image watermarking. *Elsevier Signal Processing*, pp. 357-372.
- Bedi, P., Bansal, R., Sehgal, P. (2012). Multimodal biometric authentication using PSO based watermarking. *Procedia Technol* 4, pp. 612–618.
- Behera, B. and Govindan, V. (2013). Improved Multimodal Biometric Watermarking in Authentication Systems Based on DCT and Phase Congruency Model. *International Journal of Computer Science and Network*, vol. 2, issue 3, pp. 123-129, June 2013.
- Bolle, R.M., Connell, J.H., Ratha, N.K. (2002). Biometric perils and patches. *Pattern Recognition* 35(12), pp. 2727–2738.
- Brunelli, R., Poggio, T. (1993). Face recognition: features versus templates. *IEEE Transactions on Pattern Analysis and Machine Intelligence* 15, pp. 1042-1052.
- Canadian Communications Security Establishment. EAL2 certification report for Bioscrypt™ Enterprise for NT logon version 2.1.3. Certification Report 383-4-8; 2001.
- Chen, C.H., Chang, L.W. (2005). A digital watermarking scheme for personal image authentication using eigenface. *Lecture Notes in Computer Science* 3333, pp. 410–417.
- Cheung, W.N. (2000). Digital image watermarking in spatial and transform domains. In: *Proceedings of TENCON 2000*.
- Chung, Y., Moon, D., Moon, K., Pan, S. (2005). Hiding biometric data for secure transmission. In: *Khosla, R., Howlett, R.J., Jain, L.C. (eds.) KES 2005. LNCS (LNAI)2005 3683*, pp. 1049–1057.
- Common Criteria Biometric Evaluation Methodology Working Group Biometric evaluation methodology. 2002; Version 1.0.
- Cox, I.J., Leighton, F.T., Shamoon, T. (1997). Secure spread spectrum watermarking for multimedia. *IEEE Transactions on Image Processing* 6(12), pp. 1673-1687.
- Cox, I.J., Miller, M., Bloom, J. (2002). Digital Watermarking. *Morgan Kaufmann Publishers*.

- Cox, I.J., Miller, M., Bloom, J., Fridrich, J., Kalker, Ton. (2008). Digital Watermarking and Steganography. *Morgan Kaufmann Publishers*.
- Deng, F. and Wang, B. (2003). A novel technique for robust image watermarking in the DCT domain. in *Proc. of the IEEE Int. Conf. on Neural Networks and Signal Processing 2*, pp. 1525-1528.
- Ding, M., Jing, M. (2010). Digital image encryption algorithm based on improved Arnold transform. *International forum on Information Technology and Applications*, pp. 174-176.
- Fernandes, S., & Bala, J., (2013). Performance Analysis of PCA-based and LDA-based Algorithms for Face Recognition. *International Journal of Signal Processing Systems*, 1(1), 1-6.
- Friedman, G.L. (1993). The Trustworthy Digital Camera: Restoring Credibility to the Photographic Image. *IEEE Transaction on Consumer Electronics* 39(4), pp. 905-910.
- Gaurav, N.M., Yash, K., Amish, T. (2012). Digital image watermarking: a review. *International Journal of Scientific Engineering and Technology* 1(2), pp. 169-174.
- Geetha, S., Sindhu, S.S., Priya, S.B., Mubakiya, S., Kamaraj, N. (2011). Geometric attack invariant watermarking with biometric bata - applied on offline handwritten signature. *Third National Conference on Computer Vision, Pattern Recognition, Image Processing and Graphics (NCVPRIPG)*, pp. 106-109.
- German Federal Office for Information Security . Fingerprint spoof detection protection profile (FSDPP). Common Criteria Protection Profile BSI-CC-PP-0063; 2010.
- German Federal Office for Information Security. Biometric verification mechanisms protection profile (BVMPP). Common Criteria Protection Profile BSI-CC-PP-0043; 2008.
- German Federal Office for Information Security. EAL2 certification report for VoiceIdent Unit 2.0 from Deutsche Telekom. Certification Report BSI-DSZ-CC-0469; 2008.
- German Federal Office for Information Security. EAL2 certification report for PalmSecure SDK Version 24 Premium from Fujitsu Ltd. Certification Report BSI-DSZ-CC-0511; 2008.

- German Federal Office for Information Security. Fingerprint spoof detection protection profile based on organizational security policies (FSDPP\_OSP). Common Criteria Protection Profile BSI-CC-PP-0062; 2010.
- Gonzalez, R. C., Woods, R. E. (2002). *Digital image processing*. Upper Saddle River, N.J: Prentice Hall.
- Gottumukkal, R., & Asari, V. K. (2004). An improved face recognition technique based on modular PCA approach. *Pattern Recognition Letters*, 25(4), 429-436.
- Grudin, M.A. (2000). On internal representations in face recognition systems. *Pattern Recognition* 33, pp. 1161-1177.
- Guan-Ming Su. An overview of transparent and robust digital image watermarking. <http://digital.cs.usu.edu/~xqi/Teaching/REU05/Labs/RobustWM.pdf>. [accessed 12.03.12].
- Gunsel, B., Uludag, U., Tekalp, A.M. (2002). Robust watermarking of fingerprint images. *Pattern Recognition* 35(12), pp. 2739-2747.
- Halko, N., Martinsson, P.G., Shkolnisky, Y., Tygert, M. (2010). An algorithm for the principal component analysis of large data sets. *SIAM Journal on Scientific Computing* 33(5), pp. 2580-2594.
- Hatem, H., Beiji, Z., & Majeed, R. (2015). A Survey of Feature Base Methods for Human Face Detection. *International Journal of Control and Automation*, 8(5), 61-78.
- Heisele, B., Ho, P., Wu, J., Poggio, T. (2003). Face recognition: component-based versus global approaches. *Computer Vision and Image Understanding* 91, pp.6-21.
- Henniger, O., Scheuermann, D., Kniess, T. (2010). On security evaluation of fingerprint recognition systems. *International Biometric Performance Testing Conference (IBPC)*.
- Hill, C. (2001). Risk of masquerade arising from the storage of biometrics. *Master's thesis*, Australian National University.
- Hoang, T., Tran, D., Sharma, D. (2008). Remote multimodal biometric authentication using bit priority-based fragile watermarking. *19th International Conference on Pattern Recognition*.

- Hsieh, M.S., Tseng, D.C., Huang, Y.H. (2001). Hiding Digital Watermarks Using Multi resolution Wavelet Transform. *IEEE Transactions on Industrial Electronics* 48(5), pp. 875-882.
- Huang, W.T., Tan, S.Y., Chang, Y.J., Chen, C.H. (2010). A Discrete Wavelet Transform Based Robust Watermarking for Copyright Protection. *Recent Advances in Networking, VLSI, and signal processing*, pp. 39-43.
- Hui, K., Jing, L., Xiao-dong, Z., Xiao-xu, Z. (2008). Study on Implementation of a Fingerprint Watermark. in *Proc. International Conference on Computer Science and Software Engineering 2008* 3, pp. 725-728.
- Inamdar V. & Rege P., (2014). Dual watermarking technique with multiple biometric watermarks. *Sadhana*,39(I), 3-26.
- Ingemar J. Cox: *Digital watermarking and steganography*. Morgan Kaufmann, Burlington, MA, USA, 2008.
- International Standard ISO/IEC 18045. Information technology – Security techniques – Methodology for IT security evaluation.
- International Standard ISO/IEC 19792. Information technology – Security techniques – Security evaluation of biometrics.
- Isa, M.R.M., Aljareh, S. (2012). Biometric Image Protection Based on Discrete Cosine Transform Watermarking Technique. *IEEE Proc. of International Conference on Engineering and Technology (ICET)*, pp.1-5.
- Isa, M.R.M., Aljareh, S., Yusoff, Z., Minoi, J.L. (2016). A Watermarking Technique to Improve the Security Level in Face Recognition Systems: An Experiment with Principal Component Analysis (PCA) for Face Recognition and Discrete Cosine Transform (DCT) for Watermarking. *IEEE International Conference on Information and Communication Technology – 2016 (ICICTM'16)*.
- Islam, M.R., Sayeed, M.S., Samraj, A. (2008). A secured fingerprint authentication system. *Journal of Applied Sciences - Asian Network for Scientific Information (ANSINET)* 8(17), pp. 2939-2948.
- Jafri, R. and Arabnia, H.R. (2009). A survey of face recognition techniques. *Journal of Information Processing Systems* 5(2), pp. 41-68.

- Jain, A.K., Uludag, U. (2003). Hiding biometric data. *IEEE Transactions on Pattern Analysis and Machine Intelligence* 25(11), pp. 1494-1498.
- Jain, A.K., Uludag, U., Hsu, R.L. (2002). Hiding a face in a fingerprint image. *ICPR III*, pp. 756-759.
- Jangid, B. L., Biswas, K. K., Hanmandlu, M., & Chetty, G. (2015, November). Illumination Invariant Efficient Face Recognition Using a Single Training Image. In *Digital Image Computing: Techniques and Applications (DICTA), 2015 International Conference on* (pp. 1-7). IEEE.
- Jian Y., David Z., Alejandro, F. F., & Jing-yu Y., (2004, January). Two-Dimensional PCA: A New Approach to Appearance-Based Face Representation and Recognition. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 26(1), 131-137.
- Jolliffe, I.T. (2002). Principal Component Analysis. NJ, USA: Springer.
- Jones, M., & Viola P., (2003). Face Recognition Using Boosted Local Features. *IEEE International Conference on Computer Vision*.
- Kanade, T. (1973). Picture Processing System by Computer Complex and Recognition of Human Faces. Kyoto University, Japan, PhD. Thesis.
- Katzenbeisser, S., Petitcolas, FAP. (1999). Information Hiding Techniques for Steganography and Digital Watermarking. *Artech House*.
- Kaur, M., Jindal, S., Behal, S. (2012). A study of digital image watermarking. *International Journal of Research in Engineering & Applied Sciences* 2(2).
- Kekre, H. B., Sarode, T., & Natu S. (2015). Biometric watermarking using partial DCT-Walsh wavelet and SVD. *2015 Third International Conference on Image Information Processing (ICIIP)*. IEEE.
- Kim, D. J., Lee, S. H., & Sohn, M. K. (2013). Face recognition via local directional pattern. *International Journal of Security and Its Applications*, 7(2), 191-200.
- Kougianos, E., Mohanty, S.P., Mahapatra, R.N. (2009). Hardware assisted watermarking for multimedia. *Computers and Electrical Engineering* 35, pp. 339- 358.
- Kumar, K. S., Semwal, V. B., & Tripathi, R. C., (2011). Real time face recognition using adaboost improved fast PCA algorithm. *arXiv preprint arXiv:1108.1353*.

- Kundur, D., Hatzinakos, D. (2001). Diversity and attack characterization for improved robust watermarking. *IEEE Transactions on Signal Processing* 49(10), pp. 2383-2396.
- Kyunghnam, K. (1996). Face recognition using principle component analysis. *International Conference on Computer Vision and Pattern Recognition*.
- Lades, M., Vorbrüggen, J.C., Buhmann, J., Lange, J., Malsburg, C.V.D., Würtz, R.P., Konen, W. (1993). Distortion invariant object recognition in the dynamic link architecture. *IEEE Trans. Computers* 42, pp. 300-311.
- Lam, K., Beth, T. (1992). Timely authentication in distributed systems. *Proceedings of European Symposium on Research in Computer Security* 648, pp. 293–303.
- Lam, K., Gollmann, D. (1992). Freshness assurance of authentication protocols. *Proceedings of European Symposium on Research in Computer Security*, pp. 261–272.
- Lee, S.J., Jung, S.H. (2001). A Survey of watermarking techniques applied to multimedia. *IEEE Transactions on Industrial Electronics* 2001(1), pp. 272-277.
- Li, C., Ma, B., Wang, Y., Zhang, Z. (2010). Protecting biometric templates using authentication watermarking. In: Qiu, G., Lam, K.M., Kiya, H., Xue, X.-Y., Kuo, C.-C.J., Lew, M.S. (eds.) *PCM 2010. LNCS*, vol. 6297, pp. 709–718.
- Li, C., Wang, Y., Ma, B., Zhang, Z. (2012). Tamper detection and self-recovery of biometric images using salient region-based authentication watermarking scheme. *Computer Standards & Interfaces* 34(4), pp. 367-379.
- Liao S., Fan W., Albert C. S. C. & Yeung D.Y., (2006). Facial Expression Recognition Using Advanced Local Binary Patterns, Tsallis Entropies And Global Appearance Features. *IEEE International Conference on Image Processing*. 665-668.
- Lim, J.Y., Paik, J.P., (2009, Dec). Comparative Analysis of Wavelet- Based Scale-Invariant Feature Extraction Using Different Wavelet Bases. *International Journal of Signal Processing, Image Processing and Pattern Recognition*, 2(4).
- Lin, C. (2000). Watermarking and digital signature techniques for multimedia authentication and copyright protection. *PhD Thesis*. Columbia University.
- Lu, J., Plataniotis, K.N., Venetsanopoulos, A.N. (2003). Face Recognition Using Kernel Direct Discriminant. *IEEE Transactions on Neural Networks* 14(1), pp. 117-126.

- Ma, B., Li, C., Wang, Y., Zhang, Z., Wang, Y. (2010). Block Pyramid Based Adaptive Quantization Watermarking for Multimodal Biometric Authentication. *20th International Conference on Pattern Recognition*, pp. 1277-4.
- Manoharan, J., Vijila C., Sathesh A. (2010). Performance Analysis of Spatial and Frequency Domain Multiple Data Embedding Techniques towards Geometric Attacks. *International Journal of Security (IJS)*, 4(3), pp. 28-37.
- Martinez, A.M., Kak, A.C. (2001). PCA versus LDA. *IEEE Transactions on Pattern Analysis and Machine Intelligence* 23(2), pp. 228-23.
- Mathivadhani, D., Meena, C. (2010). A comparative study on fingerprint protection using watermarking techniques. *Global Journal of Computer Science and Technology* 9(5), pp. 98-102.
- Moon, D., Kim, T., Jung, S.H., Chung, Y., Moon, K., Ahn, D., Kim, S.K. (2005). Performance evaluation of watermarking techniques for secure multimodal biometric systems. In: Hao, Y., Liu, J., Wang, Y.-P., Cheung, Y.-m., Yin, H., Jiao, L., Ma, J., Jiao, Y.-C. (eds.) *CIS 2005. LNCS (LNAI) 2005 3802*, pp. 635–642.
- Morizet, N., Amiel, F., Hamed, I., Ea, T. (2007). A Comparative Implementation of PCA Face Recognition Algorithm. *Electronics, Circuits and Systems. ICECS 2007. 14<sup>th</sup> IEEE International Conference*, pp. 865-868.
- Navas, K.A., Sasikumar, M., Sreevidya, S. (2007). A Benchmark for Medical Image Watermarking. In: *14th International Workshop on Systems, Signals and Image Processing, 2007 and 6th EURASIP Conference focused on Speech and Image Processing, Multimedia Communications and Services*.
- Neerja., & Walia E., (2008). Face Recognition Using Improved Fast PCA Algorithm. *Image and Signal Processing, 2008. CISP '08. Congress on, Sanya, Hainan*, 554-558.
- Noore, A., Singh, R., Vatsa, M., Houck, M.M. (2007). Enhancing security of fingerprints through contextual biometric watermarking. *Forensic Science International* 169 2007, pp. 188–194.
- Obied, A. (2009). How to Attack Biometric Systems in Your Spare Time. *Non refereed paper*.

ORL. The Database of Faces.

<http://www.cl.cam.ac.uk/research/dtg/attarchive/facedatabase.html>; 2002 [accessed 12.03.12].

Pankanti, S., Yeung, M.M. (1999). Verification watermarks on fingerprint recognition and retrieval. *Electronic Imaging'99 International Society for Optics and Photonics*.

Park, K.R., Jeong, D.S., Kang, B.J., Lee, E.C. (2007). A study on iris feature watermarking on face data. in: *Proceedings of the ICANNGA 2007, Lecture Notes in Computer Science*, vol. 4432, pp. 415–423.

Passport Canada. Rules for Canadian passport photos. <http://www.ppt.gc.ca/info/photos.aspx>. [accessed 17.08.12].

Pearson, K. (1901). On Lines and Planes of Closest Fit to Systems of Points in Space. *Philosophical Magazine* 6, pp. 559-572.

Peterson, G. (1997). Arnold's cat map survey. *Math 45- Linear Algebra, Fall 1997*, pp. 1-7.

Petitcolas, F., Anderson, R., Kuhn, M. (1999). Information Hiding – A Survey. *Proceedings of the IEEE* 87(7), pp. 1062–1078.

Phillips, P.J., Moon, H., Rizvi, S.A., Rauss, P.J. (1997). The FERET Evaluation Methodology for Face recognition Algorithms. in *Proceedings, IEEE Conference on Computer Vision and Pattern Recognition*, pp. 137-143.

Phillips, P.J., Rauss, P., Der, S. (1996). FERET (Face REcognition Technology) Recognition Algorithm Development and Test Report. U.S. Army Research Laboratory ARL-TR-995.

Poljičak A., Mandić L., & Kurečić M.S., (2012). Improvement of the watermark detector performance using image enhancement filters. *2012 19th International Conference on Systems, Signals and Image Processing (IWSSIP)*, Vienna, 68-71.

Poljicak, A., Mandic, L., Agic, D. (2011). Discrete Fourier Transform - Based Watermarking Method with an Optimal Implementation Radius. *Journal of Electronic Imaging* 20(3), pp. 033008-1 - 033008-8.

Pradhan, C., Saxena, V., Bisoi, A.K. (2012). Imperceptible Watermarking Technique using Arnold's Transform and Cross Chaos Map in DCT Domain. *International Journal of Computer Applications* 55(15), pp. 50-53.



- Putte, T., Keuning, J. (2000). Biometrical fingerprint recognition: don't get your fingers burned. *IFIP TC8/WG8.8, Fourth Working Conference on Smart Card Research and Advanced Applications*, pp. 289-303.
- Ramkumar, M. (2000). Data Hiding in Multimedia - Theory and Applications. *New Jersey Institute of Technology, Newark*.
- Rao, K.R., Yip, P. (1990). Discrete Cosine Transform: algorithms, advantages. applications. *Aademic Press, USA*.
- Ratha, N.K., Connell, J.H., Bolle, R.M. (2000). Secure data hiding in waveletcompressed fingerprint images. *Proceedings of ACM Multimedia*, pp. 127-130.
- Ratha, N.K., Connell, J.H., Bolle, R.M. (2001). An analysis of minutiae matching strength. *In Proc. AVBPA 2001, Third International Conference on Audio- and Video-Based Biometric Person Authentication*, pp. 223-228.
- Ross, A., Shah, J., Jain, A.K. (2005). Toward Reconstructing Fingerprints from Minutiae Points. *Proc. Int'l Soc. Optical Eng. (SPIE), Biometric Technology for Human Identification II*, pp. 68-80.
- Salahi, E., Moin, M.S., Salahi, A. (2008). A new visually imperceptible and robust image watermarking scheme in contourlet domain. *Proceedings of the IIHMSP*.
- Sangeeta, J., Anjali, B. (2010). Robust Digital Image-Adaptive Watermarking Using BSS Based Extraction Technique. *International Journal of Image Processing (IJIP) 4(1)*, pp. 77-88.
- SANS Institute, (2014). Password Construction Guidelines. <http://www.sans.org/security-resources/policies/general/pdf/password-construction-guidelines>. [accessed 16.06.15]
- Sharma, P.K., Rajni. (2012). Information security through image watermarking using least significant bit algorithm. *The Second International Conference on Computer Science, Engineering and Applications (CCSEA)*, pp. 61-67.
- Shaw, Peter J.A. (2003). Multivariate statistics for the environmental sciences. *London: Arnold*.
- Sherlock, B.G., Monro, D.M. (1993). A Model for Interpreting Fingerprint Topology. *Pattern Recognition 26*, pp. 1047-1055.

- Shih, F. (2008). Digital Watermarking and Steganography. *In: Fundamentals and Techniques*. CRC Press.
- Shoemaker, C. (2002). Hidden Bits: A Survey of Techniques for Digital Watermarking. *Independent Study*.
- Singh, A.P., Mishra, A. (2010). Wavelet Based Watermarking on Digital Image. *Indian Journal of Computer Science and Engineering* 1(2), pp. 86-91.
- Škorić B. (2010). Security with noisy data. *Information Hiding*, pp. 48-50.
- Sridhar, K., Sattar, S.A., Mohan, M.C. (2014). Comparison of Digital Watermarking with Other Techniques of Data Hiding. *International Journal of Computer Science and Information Technologies (IJCSIT)*, Vol. 5 (1), pp. 350-353.
- Sukthankar, G. (2000). Face recognition: a critical look at biologically-inspired approaches. Carnegie Mellon University, Pittsburgh, PA, Technical Report: CMURITR-00-04 2000.
- Support, M. IBM SNA Formats Bit Ordering is Opposite of Intel Convention. <http://support.microsoft.com/kb/130861>. [accessed 23.10.12].
- Syed A.A. (2011). Digital Watermarking. EE 5359 Multimedia Processing Report.
- Syverson, P. (1994). A taxonomy of replay attacks. *in Proceedings of the Computer Security Foundations Workshop (CSFW97)*, pp. 187–191.
- Thampi, S.M., Jacob, A.J. (2011). Securing biometric images using reversible watermarking. *International Journal Of Image Processing* 5(4), pp. 382.
- Tian, J. (2003). Reversible data embedding using a difference expansion. *IEEE Trans. Circuits Syst. Video Technol.* 13, pp. 890–896.
- TÜViT. EAL2 certification report for authentication engine of VOICE.TRUST server version 4.1.2.0. 2005; Certification Report TUVIT-DSZ-CC-9224.
- Tzouveli, P., Tsapatsoulis, N., Ntalianis, K., Kollias, S. (2002). Automatic face region watermarking using qualified significant wavelet trees. *Proceedings of 9th International Workshop on Systems, Signal and Image Processing, Control Systems Centre Manchester, United Kingdom (November , 2002)*, pp. 101–103.
- U.S. Information Assurance Directorate. U.S. government biometric verification mode protection profile for basic robustness environments. 2007; Version 1.1.

- U.S. Information Assurance Directorate. U.S. government biometric verification mode protection profile for medium robustness environments. 2007; Version 1.1.
- UK CESG. Biometric device protection profile (BDPP). 2001; Draft issue 0.82.
- Vatsa, M., Singh, R., Mitra P., Noore, A. (2004a). Digital watermarking based secure multimodal biometric system. *in: Proceedings of IEEE International Conference on Systems, Man, and Cybernetics*.
- Vatsa, M., Singh, R., Mitra, P., Noore, A. (2004b). Comparing robustness of watermarking algorithms on biometrics data. *Proceedings of the Workshop on Biometric Challenges from Theory to Practice - ICPR Workshop 2004*, pp. 5-8.
- Vatsa, M., Singh, R., Noore, A. (2005). Improving biometric recognition accuracy and robustness using DWT and SVM watermarking. *IEICE Electronics Express* 2(12), pp. 362–367.
- Vatsa, M., Singh, R., Noore, A. (2007). Feature based RDWT watermarking for multimodal biometric system. *Image and Vision Computing*.
- Vatsa, M., Singh, R., Noore, A., Houck, M.M., Morris, K. (2006). Robust biometric image watermarking for fingerprint and face template protection. *IEICE Electronics Express* 3(2), pp. 23-28.
- Vetterli, M.a.K. (1995). Wavelets and Subband Coding. *Signal Processing Series*. Prentice Hall.
- Viola P., Jones M.J. (2004). Robust real-time face detection. *International Journal of Computer Vision* 57, pp. 137–154.
- Wang Z., Conrad A., Rahim H., Simoncelli E. (2004). Image Quality Assessment: From Error Visibility to Structural Similarity. *IEEE Trans. Image Processing* 13 (4).
- Wang, F.H., Pan, J.-S., Jain, L.C. (2009). Intelligent Techniques. *In: Wang, F.-H., Pan, J.-S., Jain, L.C. (eds.) Innovations in Digital Watermarking Techniques. Studies in Computational Intelligence, Springer, Heidelberg, vol. 232*, pp. 27–44.
- Weilong, C., Meng J.E., Shiqian W. (2005). PCA and LDA in DCT Domain. *Journal of Pattern Recognition Letters* 26, pp. 2474-2482.

- Wiskott, L., Fellous, J.M., Krüger, N., Malsburg, CVD. (1997). Face Recognition by Elastic Bunch Graph Matching. *IEEE Transactions on Pattern Analysis and Machine Intelligence* 19, pp. 775- 779.
- Wu, L., Deng, W., Zhang, J., He D. (2009). Arnold transformation algorithm and anti-Arnold transformation algorithm. *Proc. of 1st International Conference on Information Science and Engineering (ICISE2009)*, pp. 1164–1167.
- Wu, X., Zhang, D., Wang, K., Huang, B. (1998). Palmprint classification using principle lines. *Pattern Recognition* 2004 37(10), pp. 1987-1998.
- Yadav, R., Kamaldeep, Saini, R., Nandal, R. (2011). Biometric template security using invisible watermarking with minimum degradation in quality of template. *International Journal On Computer Science & Engineering* 2011 3(12), pp. 3656-3668.
- Yan, J., Liu, L. (2010). An information hiding algorithm based on RDWT for fingerprint biometric system. *2<sup>nd</sup> International Conference on Signal Processing Systems (ICSPS)* 3(V3), pp. 597 -599.
- Zebbiche, K., Khelifi, F. (2008). Region-based watermarking of biometric images: Case study in fingerprint images. *International Journal of Digital Multimedia Broadcasting* (March 2008).
- Zeng, W., Liu, B. (1999). A statistical watermark detection technique without using original images for resolving rightful ownerships of digital images. *IEEE Transactions on Image Processing* 8(11), pp. 1534-1548.
- Zhang, Z. (2011). Improving security for facial image using fragile digital watermarking, face analysis, modeling and recognition systems. InTech 2011. <http://www.intechopen.com/books/face-analysis-modeling-and-recognition-systems/improving-security-forfacial-image-using-fragile-digital-watermarking>; 2011 [accessed 12.03.12].
- Zhao, W., Chellappa, R., Phillips, P.J., Rosenfeld, A. (2003). Face recognition: a literature survey. *ACM Computing Surveys* 2003, pp. 399–458.

## Appendix A - List of watermarking techniques on biometrics and their application domains

No.	Authors	Research Title	Year	Cover Image	Watermark data	Algorithm	Watermarking techniques	Application	Comments
1	Behera, Govindan	Improved multimodal biometric watermarking in authentication systems based on DCT and phase congruency model	2013	Face	Fingerprint, Demographic data	DCT, PSO	Robust	Multimodal Biometric Authentication	No face detection module
2	Bedi et al.,	Multimodal biometric authentication using PSO based watermarking	2012	Face	Fingerprint	DCT, PSO	Robust	Multimodal Biometric Authentication	No face detection module

3	Zutao Zhang	Improving security for facial image using fragile digital watermarking, face analysis, modelling and recognition systems	2011	Face	Watermark scrambled by chaotic systems	LSB	Fragile	Image Tampering	Facial image database
4	Ma et al.,	Block pyramid based adaptive quantization watermarking for multimodal biometric authentication	2010	Face	Fingerprint	QIM, Adaboost region selection	Robust	Multimodal Biometric Authentication	Imperceptibility of face image is not important as long as the face feature can be extracted
5	Li et al.,	Protecting biometric templates using authentication watermarking	2010	Face	Eigenvalue face information	Salient region based	Semi Fragile	Biometric template protection, Image Tampering	Facial image database
6	Yan and Liu	An information hiding algorithm based on RDWT for fingerprint biometric system	2010	Face	Fingerprint	RDWT	Robust	Biometric template protection	Imperceptibility of face image is not important as long as the face feature can be extracted

7	Hoang et al.,	Remote multimodal biometric authentication using bit priority-based fragile watermarking	2008	Face	Fingerprint	Amplitude modulation, priority level of bits sequence	Fragile	Multimodal Biometric Authentication	No face detection module
8	Hoang et al.,	Remote multimodal biometric authentication using bit priority-based fragile watermarking	2008	Face	Fingerprint	Amplitude modulation, priority level of bits sequence	Fragile	Multimodal Biometric Authentication	No face detection module
9	Salahi et al.,	A new visually imperceptible and robust watermarking scheme in Contourlet Domain	2008	Face	Logo	CT	Robust	Biometric data protection	No face detection module
10	Vatsa et al.,	Feature based RDWT watermarking for multimodal biometric system	2007	Face	Voice	RDWT	Robust	Multimodal Biometric Authentication	Imperceptibility of face image is not important as long as the face feature can be extracted

11	Park et al.,	A study on Iris feature watermarking on face data	2007	Face	Iris	Transform domain, Adaboost region selection	Robust	Multimodal Biometric Authentication	Imperceptibility of face image is not important as long as the face feature can be extracted
12	Vatsa et al.,	Digital watermarking based secure multimedia biometric system	2004	Face	Iris template	Modified Correlation, Modified 2D DCT	Robust	Biometric template protection	No face detection module
13	Chung et al.,	Hiding biometric data for secure transmission	2005	Fingerprint, Face	Fingerprint, Face	Dual watermark	Robust	Template protection	No face detection module
14	Moon et al.,	Performance evaluation of watermarking techniques for secure multimodal biometric systems	2005	Fingerprint, Face	Fingerprint, Face	Robust and Fragile WM technique	Semi Fragile	Multimodal Biometric Authentication	No face detection module



15	Chen and Chang	A Digital Watermarking Scheme for Personal Image Authentication Using Eigenface	2005	Personal Image (Face)	Eigenvalue face information	SHA-1 SEQUENCE, DCT	Robust	copyright protection	Not Biometric Authentication System
16	Tzouveli et al.,	Automatic Face Region Detection Using Qualified Significant Wavelet Trees (QSWT) technique	2002	Real life images (Face)	Logo	QSWT, DWT	Robust	Copyright protection	Not Biometric Authentication System
17	Bahsal, Sehgal, Bedi	Securing fingerprint images using a hybrid technique	2012	Fingerprint	Face	Neural Network – PSO	Robust	Biometric data protection	
18	Sabu and Ann	Securing biometric images using reversible watermarking	2011	Fingerprint	Text	LSB, Different Expansion, Rotational Replacement of LSB	Reversible Watermarking	Biometric data protection	

19	Yadav, Saini and Nandal	Biometric template security using invisible watermarking with minimum degradation in quality of template	2011	Fingerprint	Bit '0' or '1'	Spatial, Parity Checker Method	Robust	Biometric template protection	
20	Li et al.,	Sparse reconstruction based watermarking for secure biometric authentication	2011	Fingerprint,	Compact face feature	Robust WM, Blind - SSQIM	Robust	Multimodal Biometric Authentication	
21	Y. Cao et al.,	Robust biometric watermarking based on Contourlet transform for fingerprint and face protection	2010	Fingerprint	Face	CT, quantization	Robust	Biometric template protection	

22	Mathivadhani and Meena	A comparative study of fingerprint protection using watermarking techniques	2010	Fingerprint	Pseudorandom sequence generator	Zebbiche et al. algo (DCT, DWT), Vasta et al algo (DWT + LSB)	Robust	Biometric data protection	
23	Kim and Lee	Multimodal biometric image watermarking using two stage integrity verification	2009	Fingerprint	Face	Blind and SS approach	Robust	Multimodal Biometric Authentication	
24	Rajibul Islam et al.,	A secured fingerprint authentication system	2008	Fingerprint	Palmprint	DWT, Wu et al.	Robust	Biometric data protection	
25	Zebbiche et al.,	Region-based watermarking of biometric images: Case study in fingerprint images	2008	Fingerprnt	Pseudorandom sequence generator	DWT, DFT	Robust	Biometric data protection	Embed watermark in foreground or ridges area (ROI)

26	Zebbiche et al.,	An efficient watermarking technique for the protection of fingerprint images	2008	Fingerprint	Pseudorandom sequence generator	DCT, DWT	Robust	Biometric data protection	Embed watermark in foreground or ridges area (ROI)
27	Noore et al.,	Enhancing security of fingerprints through contextual biometric watermarking	2007	Fingerprint	Face, Demographic text data	DWT	Semi Fragile	Image tempering	
28	Zebbiche et al.,	Protecting fingerprint data using watermarking	2006	Fingerprint	Fingerprint minutiae	Wavelet	Robust	Biometric data protection	
29	Kim et al.,	Secure remote fingerprint verification using dual watermarks.	2006	Fingerprint	Pseudorandom sequence generator	Robust (Dugad et al.) and Fragile (Jain et al. )WM technique	Semi Fragile	Biometric data protection	

30	Vatsa et al.,	Robust biometric image watermarking for fingerprint and face template protection	2006	Fingerprint	Face template	DWT, LSB	Robust	Biometric template protection	
31	Vatsa et al.,	Improving biometric recognition accuracy and robustness using DWT and SVW watermarking	2005	Fingerprint	Face	Multi resolution DWT, SVM	Robust	Image tampering	
32	Ahmed and Moskowitz	Composite signature based watermarking for fingerprint authentication	2005	Fingerprint	Signature extracted from Fingerprint	Fourier Frequency Domain	Robust	Image Authentication	
33	Giannoula and Hatzinakos	Data hiding for multimodal biometric recognition	2004	Fingerprint	Voice, Iris	DWT	Robust	Multimodal Biometric Authentication	
34	Jain et al.,	Hiding fingerprint minutiae in images	2002	Fingerprint	Face	Robust WM technique	Robust	Biometric template protection	

35	Uludag et al.,	A spatial method for watermarking of fingerprint images	2001	Fingerprint	Watermark bit	Spatial	Robust	Biometric data protection	
36	Ratha et al.,	Secure data hiding in wavelet compressed fingerprint images	2000	Fingerprint	-	Wavelet compressed domain, Huffman algo	Robust data hiding	Data compression	
37	Yeung and Pankanti	Verification watermarks on fingerprint recognition and retrieval	1999	Fingerprint	Chaotic mixing	Invisible WM technique	Fragile	Image Verification	
38	Inamdar and Rege	Face features based biometric watermarking of digital image using singular value decomposition for fingerprinting	2012	General Image	Face	PCA, SVD	Robust	Fingerprinting	

39	M. Paunwala, S. Patnaik	DCT watermarking approach for security enhancement of multimodal system	2012	General Image	Iris, Fingerprint	DCT	Robust	Biometric template protection	
40	M. Qi et al.,	A novel image hiding approach based on correlation analysis for secure multimodal biometrics	2010	General Image	Palmprint, iris	Correlation Analysis, Partial Least Squares (PLS), PSO	Robust	Biometric data protection	
41	George Varbanov and Peter Blagoev	An improving model watermarking with iris biometric code	2007	General Image	Logo, Iris biometric code	DWT	Robust	Biometric template protection	Hashing iris code before embedding process
42	Geetha et al.,	Geometric Attack Invariant watermarking with biometric data – applied on offline handwritten signature	2011	Handwritten signature	Face	DCT, SVD	Robust	Ownership protection	

43	Jutta Hammerle-Uhl et al.,	Experimental Study on the Impact of Robust Watermarking on Iris Recognition Accuracy	2010	Iris	Binary values	LSB, DCT, DWT	Robust	Biometric data protection	
44	Bartlow et al.,	Protecting iris images through asymmetric digital watermarking	2007	Iris	Voice feature vector	Asymmetric technique	Robust	Multimodal Biometric Authentication	
45	Hui et al.,	Study on Implementation of a Fingerprint Watermark	2009	Lena Image	Fingerprint characteristics	Spatial Domain, DCT	Robust	Copyright protection	



# FORM UPR16

## I. RESEARCH ETHICS REVIEW CHECKLIST



A. Please include this completed form as an appendix to your thesis (see the Postgraduate Research Student Handbook for more information)

<b>Postgraduate Research Student (PGRS) Information</b>				<b>Student ID:</b> UP630277	
<b>PGRS Name:</b>		Mohd Rizal Bin Mohd Isa			
<b>Department:</b>		ENG	<b>First Supervisor:</b>		Dr. Salem Aljareh
<b>Start Date:</b> (or progression date for Prof Doc students)		1 OCT 2011			
<b>Study Mode and Route:</b>		Part-time <input type="checkbox"/>	MPhil <input type="checkbox"/>	MD <input type="checkbox"/>	
		Full-time <input checked="" type="checkbox"/>	PhD <input checked="" type="checkbox"/>	Professional Doctorate <input type="checkbox"/>	

<b>Title of Thesis:</b>	WATERMARKED FACE RECOGNITION SCHEME - ENHANCING THE SECURITY WHILE MAINTAINING THE EFFECTIVENESS OF BIOMETRIC AUTHENTICATION SYSTEMS
<b>Thesis Word Count:</b> (excluding ancillary data)	37, 824

If you are unsure about any of the following, please contact the local representative on your Faculty Ethics Committee for advice. Please note that it is your responsibility to follow the University's Ethics Policy and any relevant University, academic or professional guidelines in the conduct of your study

Although the Ethics Committee may have given your study a favourable opinion, the final responsibility for the ethical conduct of this work lies with the researcher(s).

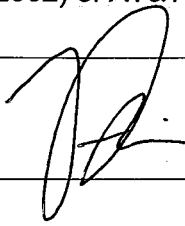
### UKRIO Finished Research Checklist:

(If you would like to know more about the checklist, please see your Faculty or Departmental Ethics Committee rep or see the online version of the full checklist at: <http://www.ukrio.org/what-we-do/code-of-practice-for-research/>)

a) Have all of your research and findings been reported accurately, honestly and within a reasonable time frame?	YES <input checked="" type="checkbox"/> NO <input type="checkbox"/>
b) Have all contributions to knowledge been acknowledged?	YES <input checked="" type="checkbox"/> NO <input type="checkbox"/>
c) Have you complied with all agreements relating to intellectual property, publication and authorship?	YES <input checked="" type="checkbox"/> NO <input type="checkbox"/>
d) Has your research data been retained in a secure and accessible form and will it remain so for the required duration?	YES <input checked="" type="checkbox"/> NO <input type="checkbox"/>
e) Does your research comply with all legal, ethical, and contractual requirements?	YES <input checked="" type="checkbox"/> NO <input type="checkbox"/>

### Candidate Statement:

I have considered the ethical dimensions of the above named research project, and have successfully obtained the necessary ethical approval(s)

<b>Ethical review number(s) from Faculty Ethics Committee (or from NRES/SCREC):</b>		
If you have <i>not</i> submitted your work for ethical review, and/or you have answered 'No' to one or more of questions a) to e), please explain below why this is so:		
I have not applied for ethical review because the experiments for this research were tested using the 'Our Database of Faces (ORL, 2002) of AT&T Laboratories Cambridge University		
<b>Signed (PGRS):</b>		<b>Date:</b> 22/08/2016