# Development of a Secure Biometric Recognition System

**Rajesh Kumar Muthu**

**PhD**

**2016**

# Development of a Secure Biometric Recognition System

**Rajesh Kumar Muthu**

A thesis submitted in partial fulfilment
of the requirement of the
University of Northumbria at Newcastle
for the degree of
Doctor of Philosophy

Research undertaken in the Faculty of Engineering and Environment,
Northumbria University, United Kingdom

**April 2016**

# Abstract

Biometric based security systems are becoming an integral part of many security agencies and organisations. These systems have a number of applications ranging from national security, law enforcement, the identification of people, particularly for building access control, the identification of suspects by the police, driver's licences and many other spheres. However, the main challenge is to ensure the integrity of digital content under different intentional and non-intentional distortions; along with the robustness and security of the digital content.

This thesis focuses on improving the security of fingerprint templates to allow accurate comparison of the fingerprint content. The current methods to generate fingerprint templates for comparison purposes mostly rely on using a single feature extraction technique such as Scale Invariant Feature Transform (SIFT) or Fingerprint Minutiae. However, the combination of two feature extraction techniques (e.g., SIFT-Minutiae) has not been studied in the literature.

This research, therefore, combines the existing feature extraction techniques, SIFT-Harris: *Feature point detection is critical in image hashing in term of robust feature extraction, SIFT to incorporate the Harris criterion to select most robust feature points* and SIFT-Wavelet: *Wavelet based technique is basically used to provide more security and reliability of image, SIFT feature with efficient wavelet-based salient points to generate robust SIFT - wavelet feature that provides sufficient invariance to common image manipulations. The above said feature detector* are known work well on the natural images (e.g., faces, buildings or shapes) and tests them in the new context of fingerprint images. The results in this thesis demonstrate that new approach contributes towards the improvement of fingerprint template security and accurate fingerprint comparisons.

The fingerprint minutiae extraction method is combined *individually* with the SIFT-Harris method, SIFT-Wavelet method and the SIFT method, to generate the most prominent fingerprint features. These features are post-processed into perceptual hashes using Radial Shape Context Hashing (RSCH) and Angular Shape Context

Hashing (ASCH) methods. The accuracy of fingerprint comparison in each case is evaluated using the Receiver Operating Characteristic (ROC) curves.

The experimental results demonstrate that for the JPEG lossy compression and geometric attacks, including rotation and translation, the fingerprint template and accuracy of fingerprint matching improved when combinations of two different Feature extraction techniques are used, in contrast to using only a single feature extraction technique.

The ROC plots illustrates the SIFT-Harris-Minutiae, SIFT-Wavelet-Minutiae, SIFT-Minutiae perform better than the SIFT method. The ROC plots further demonstrate that SIFT-Harris-Minutiae outperform all the other techniques. Therefore, SIFT-Harris-Minutiae technique is more suitable for generating a template to compare the fingerprint content.

Furthermore, this research focuses on perceptual hashing to improve the minutiae extraction of fingerprint images, even if the fingerprint image has been distorted. The extraction of hash is performed after wavelet transform and singular value decomposition (SVD). The performance evaluation of this approach includes important metrics, such as the Structural Similarity Index Measure (SSIM) and the Peak Signal-to-Noise Ratio (PSNR). Experimentally, it has confirmed its robustness against image processing operations and geometric attacks.

To my father

**Late Mr. M. Muthu**

and

My mother

**Mrs. M. Rani**

# Acknowledgement

The research was carried out in the Faculty of Engineering and Environment at the University of Northumbria. I would like to express my sincere gratitude to the university for providing me with a studentship to perform the research. I would also like to thank VIT University, India for providing sponsorship throughout my research.

My special thanks go to my supervisors Prof. Ahmed Bouridane and Dr. Fouad Khelifi for providing me with their continuous support, guidance and encouragement, and for giving me the opportunity to undertake the study under their supervision.

I would also like wish to express my sincere gratitude to Prof. Fary Ghassemlooy, Professor and Head of the Northumbria Communication Research Lab for his inspiration and support whilst carrying out my research at the University of Northumbria.

In addition, I would like to convey my sincere thanks to Dr. Richard Binns, Head of the Department of Physics and Electrical Engineering and to Ms. Karen Vacher, Office of Postgraduate Research, for their support with my teaching and with the research.

Finally, special thanks must go to my wife Dr. Rani and my beautiful daughter Muthusri for their constant support, patience and encouragement throughout this work.

# Publications

1. Muthu, R., Bouridane, A., & Khelifi, F. (2014**).** Minutiae Based Fingerprint Image Hashing. *International Conference on Control Decision and Information Technologies,* 2014.

2. Herald, S. Muthu, R. Khelifi, F. Ali, A.Vickers, P. & Bouridane, Tanougast, C. (2013). Progress in Data Encryption Research.

3. Muthu, R., Bouridane, A., & Khelifi, F. (2013). Securing Biometric Recognition systems. *4th European Workshop on Visual Information Processing,* 2013.

4. Muthu, R., Bouridane, A., & Khelifi, F. (2013). Minutiae Ranking and Its Application to Fingerprint Recognition. *International Journal of Applied Engineering Research*, *8*(19), 2013.

5. Muthu, R., Bouridane, A., & Khelifi, F. (2013). Image Feature Extraction Techniques for Biometric Recognition Systems-A Survey. *International Journal of Applied Engineering Research*, *8*(19), 2013.

6. Muthu, R., Bouridane, A., & Khelifi, F. (2013). Minutiae Ranking and Its Application to Fingerprint Recognition. *International Conference on Communications, Networking and Signal Processing,* 2013.

7. Muthu, R., Bouridane, A., & Khelifi, F. (2013). Image Feature Extraction Techniques for Biometric Recognition Systems -A Survey. *International Conference on Communications, Networking and Signal Processing,* 2013.

# Declaration

I declare that the work contained in this thesis has not been submitted for any other award and it is my own work.

Rajesh Kumar Muthu

# Contents

# List of Figures

# List of Tables

# List of Acronyms

| | | |
|---|---|---|
| AFIS | : | Automatic Fingerprint Identification Systems |
| AWGN: | | Additive White Gaussian Noise |
| ASCH | : | Angular Shape Context Hashing |
| CL | : | Constract Low |
| CH | : | Constract High |
| DCT | : | Discrete Cosine Transform |
| DFT | : | Discrete Cosine Transform |
| DWT | : | Discrete Wavelet Transform |
| DoG | : | Difference-of-Gaussian |
| EER | : | Equal Error Rate |
| FDoG | : | First Derivative of the Gaussian |
| FMT | : | Fourier- Mellin Transform |
| FPR | : | False Positive Rate |
| FP | : | Feature Points |
| HVS | : | Human Visual System |
| LSH | : | Locality-Sensitive Hashing |
| MCC | : | Minutiae Cylinder Code |
| PSNR | : | Peak Signal-to-Noise Ratio |
| RSCH | : | Radial Shape Context Hashing |
| ROC | : | Receiver Operating Characteristic |
| RLRD | : | Random Local Region Descriptor |

SIFT : Scale Invariant Feature Transform

SVD : Singular Value Decomposition

SSIM : Structural Similarity Index Measure

SURF : Speeded Up Robust Feature

SNR : Signal-Noise-Ratio

TPR : True Positive Rate

# Chapter 1

# Introduction

## 1.1 Biometric Recognition System

Identification of a personal identity in a digital environment can be established in three basic ways i.e. by *"something you know"* (e.g. password, PIN number etc), by *"something you carry"* (e.g. ID cards, keys etc) or *"something you are"* (e.g. fingerprints, face, iris etc). The security and recognition systems based on surrogate representations, for instance passwords and ID cards have been established to have a fundamental flaw, for example a password can be forgotten or guessed, an ID card can easily be lost or misplaced and they can all be very easily spoofed.

Biometric based recognition systems are being extensively used in a number of current and potential applications ranging from national security, law enforcement, the identification of people, particularly for building access control, the identification of suspects by the police, driver's licences and many other spheres. Therefore, current trends in the development of innovative security systems, particularly pertaining to the identification and verification of an individual, places considerable emphasis on biometric based solutions for the reason that with biometric identification systems the key is the user and in most cases very difficult to forget. Biometric technologies can be defined as *"automated methods for verifying or recognizing the identity of a person based on a physiological and /or behavioural characteristic"* [1]. Figure 1.1 signifies commonly used biometric traits including fingerprints, face, iris, palm print, signature and voice [2],[3].

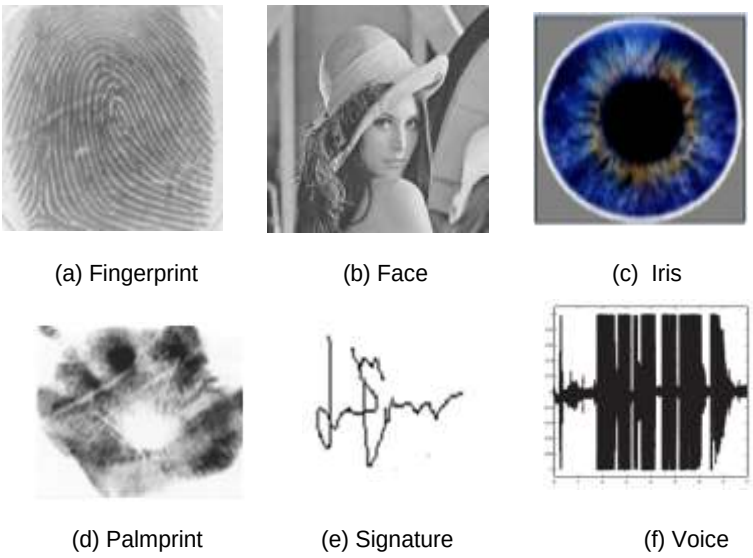



Figure1.1: Example of some commonly used biometric traits

### 1.1.1 System Operation

A biometric system, regardless of the algorithms, consists of four major modules: Sensor Module, Feature Extraction, Matching Module and Decision Module [4].

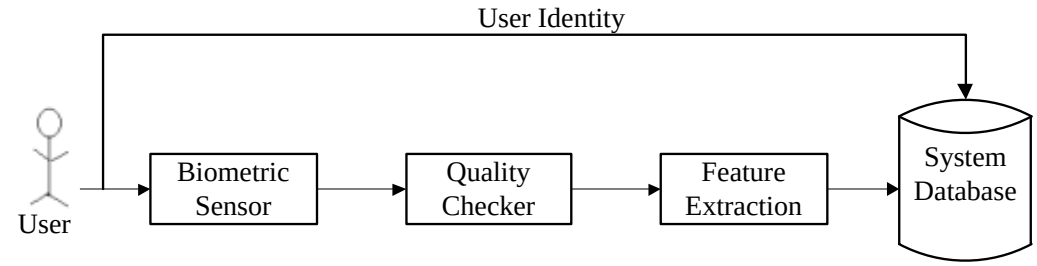
- The *Sensor Module* captures the biometric data of a user. For example, a fingerprint sensor that captures the fingerprint impression of a user.

- The *Feature Extraction Module,* where the captured data is processed to extract feature sets. For example, the position and orientation of minutiae in a fingerprint image would be computed in the feature extraction module of a fingerprint system.

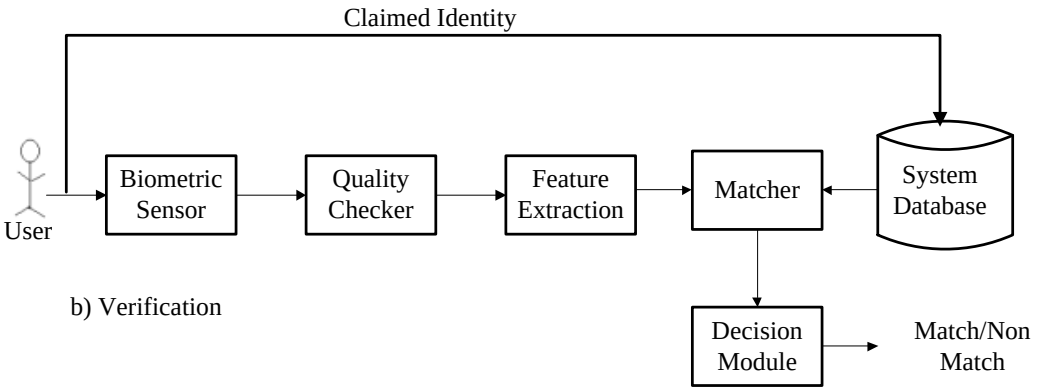
- The *Matching Module* compares the feature sets against those in the system database by generating a matching score. For instance, the number of matching minutiae between the query and the template can be computed as a matching score.

- The *Decision Module*, where the user's claimed identity is either a match or non-match, if the match score is greater than the system threshold and if not declares a non-match.

A biometric authentication system is essentially a pattern recognition system that recognizes a person by determining the authenticity of biometric traits. A biometric system operates in three main stages: (i) Enrollment: the system collects biometric data from a user and features extracted from the data is stored as a biometric template, (ii) Verification: the system authenticates a person's identity by comparing the captured biometric data with previously enrolled biometric reference template pre-stored in the system. It conducts one-to-one comparison to confirm whether the claim of identity by the individual is true. (iii) Identification: the system recognizes an individual by searching the entire enrollment template database for a match. It conducts one-to-many comparisons to establish if the individual is present in the database and if so, returns the identifier of the of the enrollment reference that matched [5][6]. Figure 1.2 illustrates the enrollment, verification, and identification stage of a biometric recognition system




a) Enrollment




b) Verification

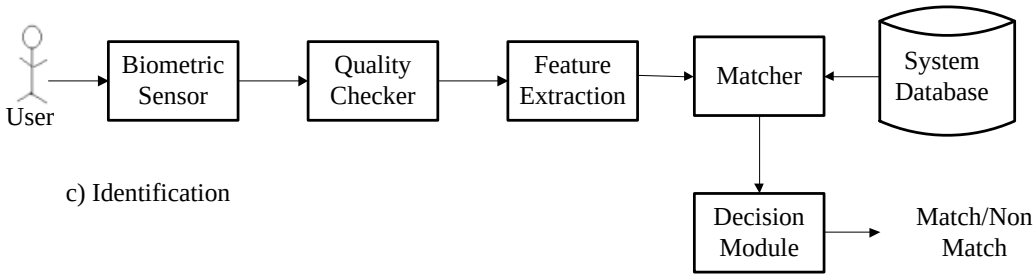



Figure 1.2: (a) Enrollment, (b) verification, and (c) Identification stage of a biometric recognition system.

## 1.2 System Vulnerabilities

A biometric system is vulnerable to different types of attacks that can compromise the system's security. The various factors that affect the security of the system typically belong to one of four categories: intrinsic failures, administrative attacks, non-secure infrastructure and access to biometric data [7], [8].

- ***Intrinsic failures:*** It is a security lapse due to an incorrect decision made by the biometric system. The sensor may fail to acquire the biometric data of the user due to limits in sensing technology or environmental conditions. The variation in the imaging condition captured biometric data and thus, the features extracted usually exhibit considerable inter-user similarity and intra-user variations. e.g., the face images of two identical twins are very similar to each other and this may lead to an incorrect decision when verifying the identity of one of the twins. The error rate at which the biometric verification system incorrectly matches two unrelated biometric templates is called the *'false accept rate'.* Conversely, it may also fail to match two biometric templates extracted from the same biometric due to significant intra-user variations. These kinds of errors are measured using the *'false reject rate'* system.

- ***Administration attacks***: This refers to all vulnerabilities due to improper administration of the biometric system. The function of the system can be

abused by an attacker by colluding with or coercing a system administrator to allow the individual to enrol or be accepted as a genuine user.

- ***Non–secure infrastructure:*** where an adversary can manipulate the biometric infrastructure in the hardware, software and the communication channels between the various modules.
- ***Access to biometric traits****:* An adversary covertly captures the biometric data of the legitimate user and uses the data to create physical artefacts. Hence, if the system is not capable of distinguishing between a live biometric and an artificial spoof, an adversary can circumvent the system by presenting spoofed traits.

As such biometric systems are prone to vulnerability at different points in the system [9] (Figure 1.3). These attacks are intended to either circumvent the security provided by the system or to change the normal functioning of the system:

(i) A fake biometric trait such as an artificial finger may be presented at the sensor

(ii) Illegally intercepted data may be resubmitted to the system.

(iii) The feature extractor may be replaced by a Trojan horse program that produces predetermined feature sets.

(iv) Legitimate feature sets may be replaced with synthetic feature sets.

(v) The matcher may be replaced by a Trojan horse program that always outputs high scores, thereby defying the system security

(vi) The template stored in the database may be modified or removed. Alternately, a new template may be introduced in the database.

(vii) The data in the communication channel between various modules in the system may be altered.

(viii) The final decision output by the biometric system may be overridden.

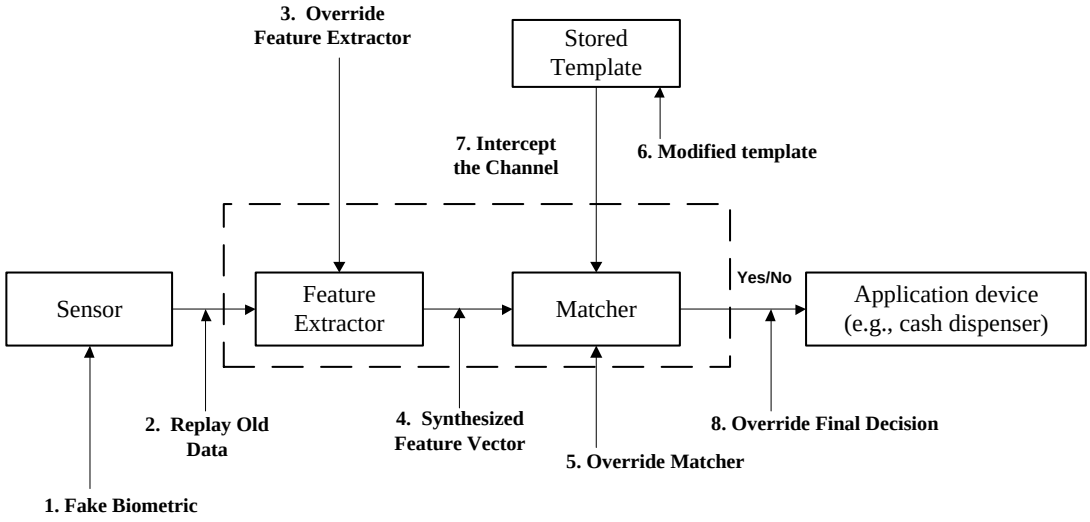



Figure1.3: Vulnerabilities in a biometric recognition system [8].

## 1.3 Fingerprint Representation

Amongst all biometric traits, fingerprints are the oldest serving, most successful and popular modality to identify a person. Fingerprints consist of a regular texture pattern composed of ridges and valleys. In a fingerprint the focussed feature points are the minutiae. i.e., ridge endings and ridge bifurcation [1] (Figure 1.4). The spatial distribution of these minutiae points is said to be unique for each finger and thus, the collection of minutiae points in a fingerprint is primarily employed for matching two fingerprints. A good quality fingerprint consists of between 20 to 70 minutiae [10], all of which are not genuine and prominent. The minutiae of the fingerprint image are usually represented as a 3 –tuple $(x, y, \theta)$, where $x$ and $y$ are the coordinate of the minutiae and $\theta$ is the angle (Figure 1.5).

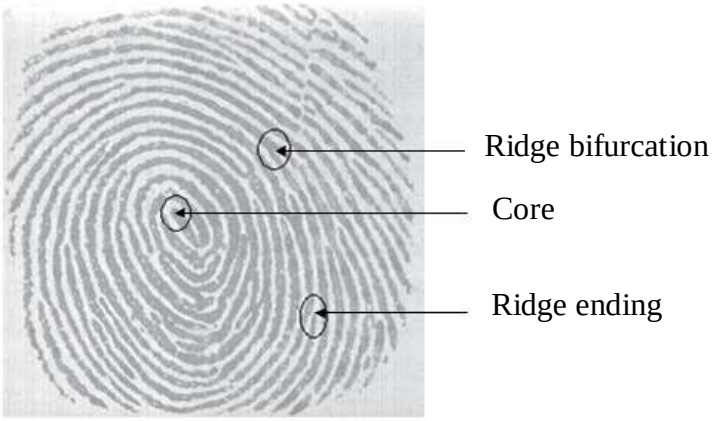
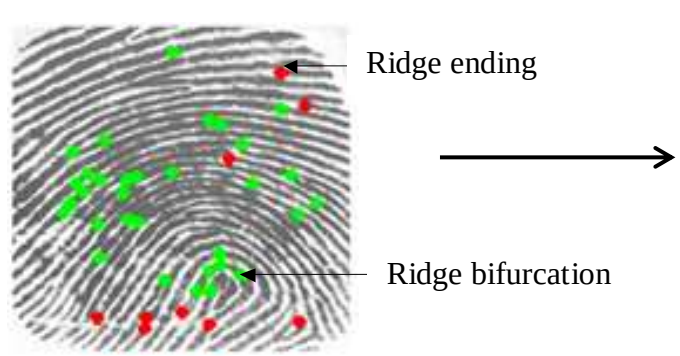



Figure 1.4: A fingerprint image with core and minutiae points marked on it. The global structure is the ridge pattern along with the core and delta points. Local structures are characterized by minutiae points [4].




| X | y | θ |
|---|---|---|
| 114 | 135 | 90 |
| 90 | 113 | 80 |
| 167 | 161 | 110 |
| 128 | 66 | 120 |

Minutiae of Fingerprint Image

Fingerprint Template (Minutiae)

Figure 1.5: Minutiae of fingerprint template

(a) (b) (c)

(d) (e)

(f) (g)

Figure 1.6: Example of fingerprint system application: (a) Border passage system using the fingerprint system. (b) Fingerprint identification system in an ATM machine. (c)Walt Disney World use the fingerprint recognition system for annual and seasonal pass holders to access the park. (d) Fingerprint – based point of sale. (e) Fingerprint - based door lock. (f) The fingerprint system is used in time and attendance applications (g) Fingerprint verification on a mobile phone [4].

### 1.3.1 Fingerprint Minutiae Extraction

Most Automatic Fingerprint Identification Systems (AFIS) (Figure1.6) are based on minutiae matching. A minutiae based fingerprint recognition system undergoes three main stages, namely pre-processing, minutiae extraction and post-processing [1], [2]. The pre-processing stage consists of image enhancement, image binarization and image segmentation. Thinning and minutiae marking is completed at the minutiae extraction stage, and finally, the removal of false minutiae in the post-processing stage. Figure 1.7 illustrates minutiae extraction of the fingerprint image.

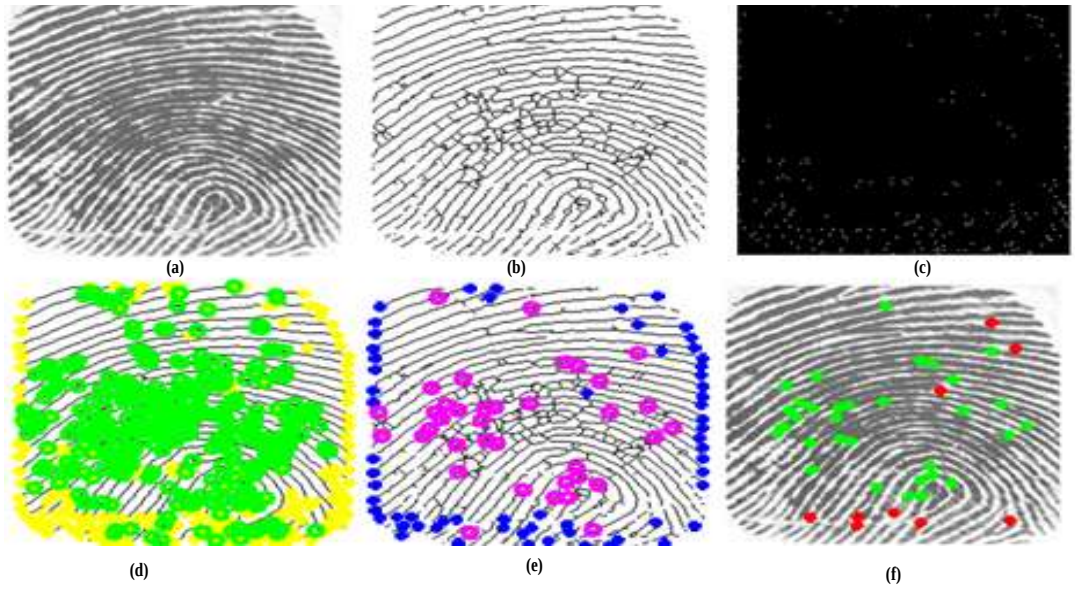



Figure 1.7: Minutiae extraction of the fingerprint image: (a) Fingerprint image. (b) Thinned image. (c) Minutiae extraction. (d) Minutiae and its spurious. (e) Removal of false minutiae. (f) Final minutiae of fingerprint image.

## 1.4 Perceptual fingerprint image hashing

Biometric template security is an important and emerging research, given that unlike passwords and tokens, compromised biometric templates cannot be revoked and reissued. The main challenge is to ensure the integrity of digital content under different intentional and non-intentional distortions environment together with the robustness and security of the data content [7], [8], [11], [12]. Recently, a few methods have been proposed for biometric template security. These methods can be categorized into two classes: Transformed based systems and biometric

cryptosystems [7]. These approaches offer a positive solution to the problem of user authentication, although they are limited. In addition, existing approaches are also not robust enough for geometric operations and slight variations in the template can significantly decrease the performance.

Alternatively, image hashing, a scheme that generates a unique, compact, resilient and secure signature for each image, has been widely applied in image content verification and content authentication.

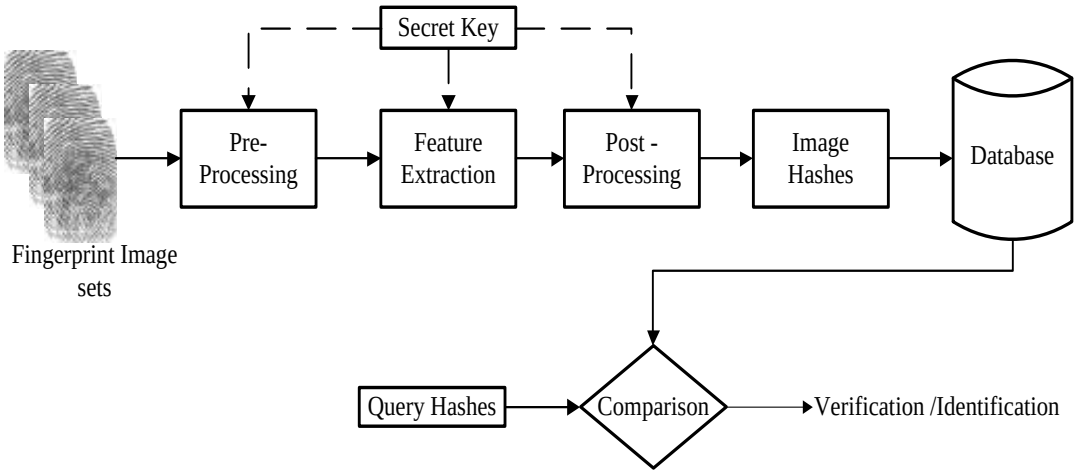



Figure 1.8: Perceptual hashing for fingerprint image authentication

A perceptual hashing system for fingerprint image authentication, as illustrated in Figure 1.8, generally consists of three main stages: pre-processing, feature extraction and post-processing. An image hash can be constructed by extraction and post processing appropriate image features to form a compact representation that can be used for the authentication and integrity of the data [13]. Interestingly another advantage of a hash based image authentication scheme is that it can also be used to handle key issues like tamper detection, security and robustness. The robustness of an image hashing arises from robust feature extraction and the compression, which mainly contributes to the compactness of the final hash. To increase the security of a traditional hash function and prevent unauthorized access, a secret key is incorporated in the feature extraction, the compression or both to make the hashes unpredictable.

Most of hashing algorithms incorporate a pseudorandomization relying on a secret key into the compression step [14][15][16] to further enhance the security, as indicated by the dashed line in Figure 1.8. The key is owned by the owner, and the hash generation is a pseudorandom process rather than a completely random one for fingerprint identification. The incoming query hash corresponding to the query image is compared with the hashes in the database.

The approach to perceptual hashing is extended to apply and demonstrate the three way check [17] to protect the biometric template as shown in Figure 1.9.

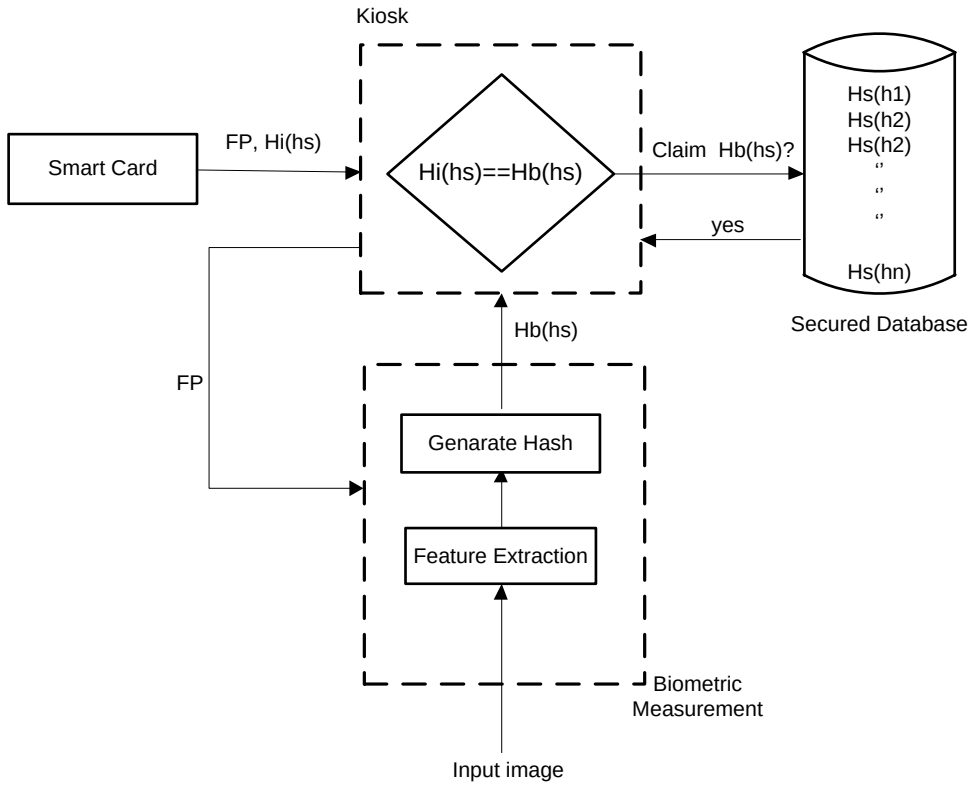



Figure1.9: Architecture for the three way check for the template Protection through Perceptual hashing.

The architecture for the three way check for the template protection through perceptual hashing explains the biometric template in the form of a selected feature point (FP). Furthermore, the hash template $(\mathrm{FP}, \mathrm{H_i}\ (\mathrm{h_s}))$ is stored in the smartcard/e-passport and the reference hash template $H(h_s)$ is stored in a secured database. The

three way check is performed by matching the hashed template form, the smartcard database and biometric measurements i.e. $(\mathrm{H_i}\,(\mathrm{h_s}) = H(h_s) = H_b(h_s))$

The three way check proceeds as follows:

- The Kiosk, which is the border control authority that reads the information feature points (only selected/limited points) and the hashed template from the smart card/e-passport sends the feature points to the biometric measurements. This results in the output of the feature point combining with the FP to generate the $H_b(h_s)$ hash template, which is given to the Kiosk.

- The Kiosk then validates the received hash template of $\mathrm{H_i}\,(\mathrm{h_s})$ and the biometric measurement hashed template $H_b(h_s)$ with the database hash template $H(h_s)$, to check the authenticity of the owner i.e. Authenticity:$(\mathrm{H_i}\,(\mathrm{h_s}) = H(h_s) = H_b(h_s))$ otherwise it is not authentic.

### 1.4.1 Properties of perceptual image hashing.

Given an image *I* and its perceptually similar copy with minor distortion $I_d$. Let $\epsilon, \tau$ be two positive values that satisfy $\epsilon > 0, \tau < 1$. The image hashing function $H_k(.)$ depends on the secret key *k*. The desirable properties of a perceptual fingerprint image hashing function $H_k(.)$ are as follows:

- ***One-way function:*** Preferably, the hash generation should be noninvertible

$$I \rightarrow H_k(.) \tag{1.1}$$

- ***Compactness:*** The size of the hash signature $H_k(I)$ should be much smaller than that of the original image *I*.

$$Size(H_k(I)) \ll Size\ (I) \tag{1.2}$$

- ***Perceptual Robustness:*** The robustness property requires for any pair of perceptually similar images have similar hashes even if they undergo content-preserving operations. This is for image identification proposes. An example is illustrated in Figure 1.10 (a) to (i), which includes the original image and its distorted copies under distortions such as rotation, median filter, Gaussian blur, Gaussian noise, JPEG compression, motion blur, translation and average

filter. The perceptual robustness of image hashing guarantees that these images will have very similar hashes.

$$(H_k(I)) \approx \left(H_k(I_d)\right) \geq 1 - \epsilon,\ 0 \leq \epsilon < 1. \quad (1.3)$$

- ***Visual Fragility:*** Perceptually distinct images (Figure 1.11) should have different hashes.

$$(H_k(I)) \neq \left(H_k(I')\right) \geq 1 - \tau,\ 0 \leq \tau < 1. \quad (1.4)$$

- ***Unpredictability:***

$$(H_k(I));\ f_h(1) \approx f_h(0) \approx 0.5 \quad (1.5)$$

Where $f_h(x)$ is the probability mass function for $h$. With this property the hash values should be approximately equally distributed. Security is an important concern for image hashing. Pseudo-randomisation techniques are incorporated into the image hash generation process to enhance the security of image hashes by using secrete keys.

(a) Original fingerprint Image (b) Rotation (c) Median filter

(d) Gaussians blur (e) Gaussian Noise f) JPEG Lossy compression

(g) Motion Blur (h) Translation (i) Average Filter

Figure 1.10: Examples of fingerprint images under different content preserving operations (perceptually insignificant modifications).

Figure 1.11: Examples of perceptually different images

## 1.5 Aim and Objectives

The aim of this research is to investigate and develop novel perceptual hashing techniques to secure biometric templates whilst maintaining the fingerprint recognition rate. In addition, a technique to improve minutiae extraction using perceptual hashing in fingerprint identification systems is also studied. The main objectives are as follows:

- To analyse the performance of state of the art techniques, SIFT, SIFT-Harris and to improve the feature extraction of fingerprint images.

- To develop a technique for fingerprint image hashing to improve the security of biometric templates, as well as to enhance or maintain the performance of the recognition system. Furthermore, the trade-off between robustness and the security of the hash will be addressed.

- To develop a method for minutiae extraction of fingerprint images using perceptual hashing that tolerates content-preserving manipulation. Furthermore, evaluate the imperceptibility against the content preserving operations using standard metrics such as SSIM and PSNR.

## 1.6 Thesis Contribution

The fingerprint image hashing and the related security issues are improved in this thesis by focusing on robust feature extraction techniques. The following are the three important contributions of this thesis:

- A new, robust, SIFT-Harris-Minutiae feature extraction technique that includes orientation and descriptor in the minutiae of fingerprint images using SIFT-Harris feature points for improving robustness against image processing operations including JPEG lossy compression and geometric attacks such as rotation and translation.
- A new, robust, SIFT-Wavelet-Minutiae feature extraction technique for improving robustness to the median filter, Gaussian blurs and rotation attacks. The ROC plots demonstrate that this new technique is suitable for generating a secured fingerprint template.
- A new robust perceptual hashing solution, based on wavelet transform and singular value decomposition (SVD) to enhance the fingerprint image and to provide good balance of robustness and imperceptibility. Additionally, this approach retains the maximum minutiae of the fingerprint image, even if the image is distorted.

## 1.7 Organisation of the thesis

This thesis comprises seven chapters, which are outlined below:

Chapter 1 presents a brief introduction on perceptual fingerprint image hashing, including the original contribution of the research.

Chapter 2 discusses the literature review in relation to biometric systems, which includes the minutiae based fingerprint system, the feature extraction and image hashing scheme, and template protection techniques.

Chapter 3 discusses the basic characteristics of transform domain: Discrete Fourier Transform, Discrete Cosine Transform and Fourier-Mellin Transform and Discrete Wavelet Transform. The transform domain technique are the most challenging part

of the image hashing in the feature extraction stage, the extracted feature are invariant to image processing operation and geometric attacks.

Chapter 4 highlights the state of the art feature extraction processes, which include the end-stopped wavelet, and the SIFT, SURF and SIFT-Harris methods.

Chapter 5 presents the proposed framework for minutiae based fingerprint image hashing. The method is combined *individually* with the SIFT-Harris, SIFT-Wavelet, SIFT. The accuracy of fingerprint comparison in each case is evaluated using the ROC curves. Further, the ROC plots demonstrate accuracy of fingerprint matching improved when combinations of two different feature extraction techniques are used, in contrast to using only a single feature extraction technique.

Chapter 6 presents the proposed technique to improve minutiae extraction of fingerprint images using perceptual hashing. The imperceptibly and performance of the minutiae extracted are discussed in detail.

Chapter 7 discusses the conclusion and suggests areas for future research in biometric recognition systems.

# Chapter 2

# Review of Secure Biometric Systems

Biometric recognition is often considered to enhance identity verification. The use of biometric recognition also introduces new challenges in protecting the privacy of the subject and increases the security of the verification system. The literature review discusses three major categories: the minutiae based fingerprint system, the feature extraction and image hashing scheme, and template protection techniques.

## 2.1 Minutiae Based Fingerprint System

Fingerprint is a popular biometric modality, which is used extensively in several applications for person recognition, providing uniqueness and an acceptable performance. A minutiae based fingerprint system involves three basic steps: pre-processing, feature extraction and matching. This system requires storing minutiae sets in the database. However, several projects have established that the fingerprint impression can be reconstructed from minutiae information.

More recently, several researchers have addressed the concept of fingerprint template solution. Moujahdietat [19] proposed a new approach to fingerprint template by constructing a new representation of minutiae based on spiral curves. Liang et al [20] demonstrated a robust fingerprint indexing scheme using a minutiae neighborhood structure and low order Delaunay triangles. This algorithm was able to search a fingerprint database more efficiently and methodically for various fingerprints.

Jin et al [21] proposed a fingerprint template protection method that transforms a set of minutiae points into bit-string using the polar grid based 3 -tuple quantization technique that offers a reasonable recognition rate. Moreover, Liu et al [22] utilised a random local region descriptor (RLRD) to generate a fixed-length feature vector. In this case, the RLRD features are extracted from a set of randomly and uniformly generated directional points from the image of a fingerprint. Additionally, Feng et al [23] suggested two descriptors: a texture based descriptor, which captures the orientation and frequency information of minutiae and a minutiae-based descriptor matching algorithm. The combined descriptors provide high discriminating ability.

Cappelli et al [24] described a template privacy protection technique for minutiae cylinder code (MCC), which provides diversity, revocability and irreversibility for the MCC descriptors with respect to the original minutiae, with the aim of improving recognition accuracy while reducing the size of the template. Tulyakov et al [25] [26] presented a method of symmetric hashing of the fingerprint minutiae, aimed at protecting the original fingerprint and minutiae location from the attacker; whereas Sutcu et al [27] proposed a scheme which employs a robust one–way transformation that maps the geometrical configuration of the minutiae points into a fixed-length code vector. Moreover, Shuai et al [28] recommended locality-sensitive hashing (LSH) based fingerprint indexing using reduced SIFT points.

Xu et al [29] [30] approached the spectral minutiae representation as a fixed-length feature vector to represent the minutiae set. In addition, Feng et al [31] presented a novel fingerprint-matching algorithm that matches both the minutiae and the ridges. This approach is used to find promising initial minutiae pairs. For each initial minutiae pair, a ridge matching process was performed, which incrementally matched the remaining minutiae and ridges.

Additionally, Jain et al [32] described a hierarchical matching system that utilized features at all three levels, namely, level 1 (pattern), level 2 (minutiae points) and level 3 (pores and ridge contours). A relative reduction of 20% is observed in the Equal Error Rate (EER: The rate at which both acceptance and rejection errors are equal. In general, the device with the lowest EER is the most accurate) of the matching system, when level 3 features are employed in combination with level 1 and level 2 features. Using a different method, Ahn et al [33] proposed an interesting alignment-free feature transformation approach. The purpose of this technique is to extract some special geometrical information from minutiae triplets to construct the secure template.

Lee et al [34] suggested a method for generating cancellable fingerprint templates without alignment, in addition to a method for producing changing functions. To generate the templates for each minutiae, a rotational and translation invariant value is computed from the orientation information of the neighbouring local region surrounding the minutiae. The invariant value is used as the input for two changing

functions that output two values for the translational and rotational movements of the original minutiae, respectively, in the cancellable template.

Chang et al [35] proposed a point pattern matching to solve the problem of optimal matches between a two-point pattern under geometrical transformation and spurious points pattern. To increase the reliability and robustness of minutiae matching, Jiang et al [36] recommended a fingerprint minutiae matching by using both the local and global structures of the minutiae. However, the system determines the identity of a user by comparing the match score to a threshold value set by the administrator.

Luo et al [37] introduced ridge information into the process of fingerprint matching and used a changeable sized box in the matching process; whilst Bhowmick et al [38] presented a method to assign a score value to each of the extracted minutiae, based on several topographical properties. The score associated to the minutiae signifies its genuineness and prominence. Furthermore, Jain et al [39] advocate the design and implementation of an on-line fingerprint verification system, which operates in two stages, such as minutiae extraction and minutiae matching. To find the correspondence between minutiae in the input image and the stored template, an alignment based elastic matching algorithm is employed.

## 2.2 Feature Extraction and Image hashing Techniques

In the design requirements for fingerprint image hashing, the robustness of the image hashing arises from robust feature extraction and compression, which mainly contributes to the compactness of the final hash. The hash should be capable of dealing with various image processing and geometric attacks, as long as two similar images possibly generate near similar hash value, otherwise the hash value differs with a perceptually different image. The following literature discusses the various feature extractions and image hashing schemes.

Monga et al [40] established a '*nonnegative matrix factorization',* which is robust against a significant class of attacks; including blurring, minor additive noise and compression, although it suffers from changes in brightness and large geometric transforms. Furthermore, Han et al [21] and Wu et al [41] presented an in-depth

review and analysis on content based image authentication; whereas Kim et al [42] proposed a novel scheme to detect unauthorized copies of an image using DCT coefficients.

Venkatesan et al [43] explained a novel image indexing technique called *'image hash function'*. This algorithm uses randomized strategies for a non-reversible compression of images into random binary strings and is robust against limited attacks. Lefèbvre et al[44] employ random transform for feature extraction and principle component analysis to reduce the hash length, nevertheless, its robustness for texture image is limited. Additionally, Swaminathan et al [45] advocated an algorithm for image hashing based on Fourier transformed controlled randomization, though, the algorithm suffers from known attacks, for instance additive noise.

Khelifi et al [46] introduced virtual watermark detection using an optimum multiplicative watermark detector. It uses a pseudo-randomly generated pattern to extract the hash bits. These researchers [47] also presented an analysis of the security of a perceptual image hash based on non-negative matrix factorization and reveal that the use of a secret key combined with image dependent keys can enhance security. Moreover, Kozat et al [48] explain singular value decomposition for image hashing; however, this algorithm, although it is robust is limited.

Recently, Monga et al [14] suggested an image hashing algorithm using visually significant feature points and performed a performance evaluation and tradeoffs between geometric invariance and robustness against classical attacks.

Also, Lv et al [16] created new image hashing algorithm using a local feature point with SIFT to detect robust feature points and incorporate Harris criterion to select the most stable points that are less vulnerable to image processing attacks.

More recently, Badrinath et al [49] advocated an efficient indexing scheme for a palmprint identification system, which makes use of a fusion of votes obtained through strategy-based geometric hashing and a SURF (speeded-up robust feature) score. Moreover, Tuytelaars et al [50] presented an overview of feature detector, such as corner (via Harris, SUSAN: *Smallest Univalue Segment Assimilating*

*Nucleus)*, Blob (via Hessian) and a salient region (via MSER: Maximally Stable Extremal Regions). The overview exposes the property of feature points and their invariant under significant geometric transforms.

Lowe D.G [51] illustrated a method for extracting distinctive invariant features from images which can be used to perform reliable matching between different views of an object. The algorithm used is SIFT, as it transforms image data into scale invariant coordinates relative to local features.

Ahmed et al [13] recommended a hash-based image authentication scheme, which concentrates on various issues like tamper detection, security and robustness. A secret key is used at the feature extraction stage to randomly modulate image pixels, in order to create a transformed feature space. The hash based scheme offers good robustness against JPEG compression, and low and high-pass filtering. In addition, Koval et al [52] proposed two classes of robust-hashing techniques: Random-Based Hashing and Content-Based Hashing systems, and perform security analysis for each class to demonstrate how security issues arise.

## 2.3 Template Protection Techniques

Template protection is a collective term for a variety of methods that aim to preserve privacy and enhance the secure storage of biometric data. Jain et al [7] presented an overview of biometric template protection schemes and categorize them into a transformation-based approach and biometric cryptosystems [7] [8] as shown in Figure 2.1. The functions used in transformation approaches can distort or randomize biometric data so that the original data cannot be reconstructed from transformed templates. The biometric cryptosystems can be embedded or generate secrets from the biometric data.

The biometric template protection scheme has the following properties:

- *Diversity:* where the secure template must not allow cross-matching across the database, by ensuring the privacy of the user.

- *Revocability:* revokes a compromised template and reissues a new one based on the same biometric data.

- *Security:* prevents an adversary from creating a physical spoof of the biometric trait from a stolen template.

- *Performance:* the biometric template scheme should not degrade the recognition performance of the (True Positive Rate and False Positive Rate) biometric system.

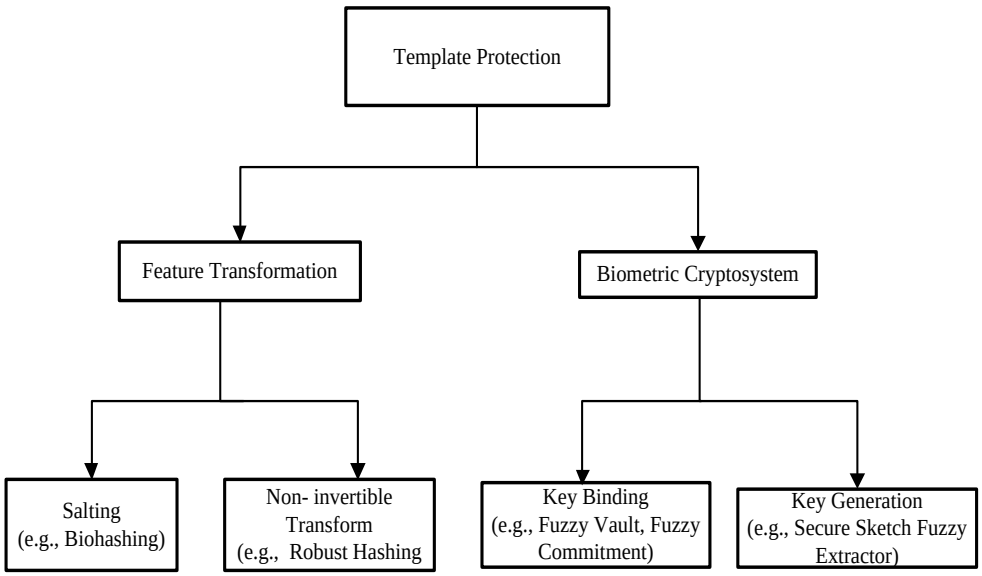



Figure 2.1: Template protection Schemes [5].

Ratha et al [9] outlined the inherent strengths of biometrics-based authentication in identifying weak links in systems by pointing to possible attacks in a generic biometric system. Furthermore, Nagar et al[11] explained that the matching performance and security of a fingerprint fuzzy vault is improved by incorporating a minutiae descriptor. However, Tuyls et al [53] proposed template protection for fingerprint based authentication, where the algorithm is based on helper data consisting of two parts. The first part identifies the reliable components with a high

signal to noise ratio in the Gabor-filtered fingerprint, whilst the second part allows for noise correction on the quantized representation.

Breebaart et al [54] and Rane [55] described the requirements for the standardization of architecture in biometric data storage and processing, which satisfy the conditions of renewability (are properties that allow a system to recover after the auxiliary data and/or the pseudonymous data have been compromised by an attacker), irreversibility, unlinkability (are the property possessed by two or more biometric references between auxiliary data and pseudonymous data pairs by virtue of which they cannot be linked to each other or to the individual from whom they were derived), confidentiality and integrity. Sun et al [56] presented a key-mixed template, which mixes a user's template with a secret key to generate another form of template, in order to prevent the biometric template stored in the database from experiencing backend attacks, snooping and tampering assaults.

In addition, Roberge et al[57] proposed a biometric encryption algorithm for the connection and retrieval of digital keys, which can be used as a method in the secure management of cryptographic keys. Sutcu et al [58] examine the storage of a face biometric template by applying a secure sketch algorithm, and noted the performance and the security of the secure sketch method. In addition, Brindha V.E [59] attempts to improve template security by combining a dorsal hand vein biometric with cryptography to generate a fuzzy vault. Sutcu et al [60] proposed a geometric transformation for securing minutiae based fingerprint templates. This method is a robust one-way transformation that maps the geometrical configuration of the minutiae points into a fixed-length code vector.

Mirmohamadsadeghi et al [61] established a new technique to protect fingerprint minutiae based on a MCC. This is a hybrid technique, combining a transformation and a user key, which provides diversity, revocability, and irreversibility for MCC descriptors with respect to the original minutiae of the fingerprint image. In addition, Prasad et al [62] described an alignment free method for generating the cancellable template, which use neighbouring relations around every reference minutiae.

Finally, Jain et al[63] provide a theoretical framework, which includes template security requirements, protection approaches and various fingerprint template protection schemes in detail. Table 2.1 explains the different techniques to transform fingerprint features for template protection schemes.

Table 2.1: Different methods used to transform fingerprint features for template protection [63].

| **Technique** | **Features** | **Transformation** | **Final Representation** |
|---|---|---|---|
| Spectral minutiae [29] | Minutiae | Fourier transform of 2D-delta functionsat minutiae locations | Vector |
| BioPhasor [64] | FingerCode | Nonlinear | Vector |
| Biometric encryption [65] | Fingerprint image | Apply a secure filter | Vector |
| Minutiae indicator [66] | Minutiae | Minutiae locations marked as '1' | Vector |
| Histogram of minutiae triplets [67] | Minutiae | Hashing the histogram of minutiae triplet features | Vector |
| Cuboid based minutiae Aggregates [68] | Minutiae | Minutiae aggregate selection from random local regions | Vector |
| Symmetric hash [26] | Minutiae as complex numbers | Set of order invariant functions for minutiae | Minutiae |
| Cancelable fingerprints [67] | Minutiae | Image folding | Minutiae |
| Alignment free cancellable fingerprint [34] | Minutiae orientation field | Transform minutiae according to surrounding orientation field | Minutiae |
| Minutiae structures [68] | Minutiae | Local minutiae structures | Minutiae |

## 2.4 Summary

In this chapter, a brief review on securing template protection and its technique are discussed in detail. In relation to the proposed research work, the literature was carried out on three main categories, which were discussed: minutiae based fingerprint templates, feature extraction image hashing and template protection. This research focuses on improving the security of fingerprint templates to allow accurate comparison of the fingerprint content. The current methods to generate fingerprint templates for comparison purposes mostly rely on using a single feature extraction technique such as SIFT or Fingerprint Minutiae. However, the combination of two feature extraction techniques (e.g., SIFT-Minutiae) has not been studied in the literature. The results in this thesis demonstrate that new approach contributes towards the improvement of the fingerprint template and accuracy of fingerprint matching improved when combinations of two different feature extraction techniques are used, in contrast to using only a single feature extraction technique.

In the next chapter, the basic characteristics of transform domain techniques are presented. These techniques are based on the manipulation of the orthogonal transform of image rather than the image itself. Transform domain techniques are suited for processing the image according to the frequency content. The principle behind this domain methods of image enhancement consists of the computing a 2-D discrete unitary transform of the image, for instance the 2-D DFT manipulating the transform coefficients by an mathematical operator and then performing the inverse transform. The orthogonal transform of the image has two components magnitude and phase. The magnitude consists of the frequency content of the image. The phase is used to restore the image back to the spatial domain. The usual transform domain enables operation on the frequency content of the image, and therefore high frequency content such as edges and other subtle information can easily be enhanced.

# Chapter 3

## Image Representation in the Transform Domain

With the increasing demand of enhanced security in our daily lives, reliable personal identification through biometric is currently active research. An individual can be identified effectively using biometric modalities such as fingerprint, palm-print and face. Recently many researchers have proposed several promising methods for biometric image identification using transform domains: Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT) and Fourier-Mellin Transform (FMT) and Discrete Wavelet Transform (DWT).

Kapil Rathor [71] proposed a method to improve the recognition rates of iris images by localizing the image between the inner and the collaretee boundary. 2-D DFT is used for finding the collaretee boundary. Imtiaz et al [72] presented a spectral feature extraction algorithm for palmprint recognition. In this method, the entire image is segmented into several spatial modules and the task of the feature extraction is carried out using 2-D Fourier transform within those spatial modules and shown good recognition accuracy and computational complexity.

Amornraksa et al [73] presented a fingerprint recognition method based on the DCT features. Applying the DCT transform to a discrete fingerprint image, the DCT features used for fingerprint matching resulting in higher recognition rates and a lower complexity. Imtiaz et al [74] proposed a DCT-based palm-print recognition scheme, where the dominant spectral features are extracted separately from each of the narrow-width band resulting from image segmentation operation. These feature extraction scheme offers two advantages: first, it captures local variations that exist in the palmprint images, which plays an important role in discriminating different persons. Second, it utilizes a very low dimensional feature space for the recognition task, which ensures lower computational burden. Badrinath et al [75] extracted the feature using 1-D DCT coefficients to design an efficient palm print based recognition system.

Singh et al [76] proposed a novel rotation-invariant and degraded partial palmprint recognition method, which combines the features of the FMT and Modified Phase –

Only correlation. Additionally, Prungsinchai et al [77] presented an efficient secure and robust perceptual image hashing technique based on the Fourier-Mellin Transform. It has been shown this method is robust against signal processing operation and geometric attacks. It has also been shown that FMT based features outperform SVD, wavelet and NMF based hashing under geometric distortions.

Ekinci et al [78] presented a novel Daubechies-based kernel Principal Component Analysis (PCA) method by integrating the Daubechies wavelet representation of palm images and the kernel PCA method for palmprint recognition. Yang et al [79] combine fingerprint, palmprint and hand geometry for person identity verification. In this multimodal system, wavelet transform is employed to extract feature from fingerprint, palmprint and hand-geometry. The Feature fusion and match score together are used for identification.

In the following section, the most widely used transform domain techniques are reviewed.

## 3.1 Discrete Fourier Transform (DFT)

The Fourier Transform is an important image processing tool which is used to decompose an image into its sine and cosine components. The Fourier transform of $x(t)$ is defined as

$$X(f) = \int_{-\infty}^{+\infty} x(t)\, e^{-i2\pi ft}\, dt \tag{3.1}$$

Where the independent variable $t$ represents time, the transform variable $f$ represents ordinary frequency. In the Fourier domain signal, each point represents a particular frequency contained in the time domain signal. The signal $x(t)$ can be reconstructed from *X(f)* by the inverse transform

$$x(t) = \int_{-\infty}^{+\infty} X(f)\, e^{-i2\pi ft}\, df \tag{3.2}$$

The interpretation of $X(f)$ is aided by expressing it in polar coordinate form as

$$X(f) = |X(f)|e^{i\Phi(f)} \tag{3.3}$$

Where $|X(f)|$ and $\Phi(f)$ represent the amplitude and the phase of $X(f)$, respectively.

Let $x(t) \Leftrightarrow X(f)$ are a Fourier transform pair. Some important properties of the Fourier transform are

- Linearity

$$ax_1(t) + bx_1(t) \Leftrightarrow aX_1(f) + bX_2(f) \tag{3.4}$$

- Convolution

$$x_1(t) * x_2(t) \Leftrightarrow X_1(f)X_2(f) \tag{3.5}$$

- Scaling

$$x(at) \Leftrightarrow \frac{1}{|a|}X\left(\frac{f}{a}\right) \tag{3.6}$$

- Modulation

$$x(t)e^{-i2\pi f_0 t} \Leftrightarrow X(f - f_0) \tag{3.7}$$

- Parseval's theorem

$$\int_{\Re}|x(t)|^2 = \int_{\Re}|X(f)|^2 \tag{3.8}$$

The DFT is the sampled Fourier Transform and therefore, it does not contain all frequencies forming an image, but only a set of samples that are large enough to perfectly describe the spatial domain image. The number of frequencies corresponds to the number of pixels in the spatial domain image, i.e. the image in the spatial and Fourier domain are of the same size [80].

For a square image size N x N, the two-dimensional DFT is given by

$$F(k,l) = \sum_{i=0}^{N-1}\sum_{j=0}^{M-1} f(i,j)e^{-i2\pi\left(\frac{ki}{N}+\frac{lj}{M}\right)} \tag{3.9}$$

where $= 0 \ldots\ldots \mathrm{N} - 1\ ;\ l = 0 \ldots\ldots \mathrm{M} - 1$

$f(i,j)$ is the image in the spatial domain and the exponential term is the basis function corresponding to each point $F(k,l)$ in the Fourier space. Equation (3.9) can be interpreted as: the value of each point $F(k,l)$ is obtained by multiplying the spatial image with the corresponding base function and summing up the result. The basis functions are sine and cosine waves with increasing frequencies, i.e. *F(0,0)* represents the DC-component of the image which corresponds to the average brightness and *F(N-1, M-1)* represents the highest frequency.

Similarly, the inverse Fourier transform is given by

$$f(i,j) = \frac{1}{NM}\sum_{k=0}^{N-1}\sum_{l=0}^{M-1} f(k,l)e^{i2\pi\left(\frac{ki}{N}+\frac{lj}{M}\right)} \tag{3.10}$$

where $i = 0 \ldots\ldots \mathrm{N}-1,\ j = 0 \ldots\ldots \mathrm{M}-1$

## 3.2 Fourier-Mellin Transform (FMT)

The Fourier-Mellin transform is a important tool for pattern recognition, reconstruction and image database retrieval, because its resulting spectrum is invariant in rotation, translation and scaling .

Let $f$ denote a function representing a grey level image defined over a set of $\mathbb{R}^2$. The standard Fourier-Mellin transform of $f$ is given by

$$\forall(k,v) \in \mathbb{Z}\times\mathbb{R}, M_f\,(k,v) = \frac{1}{2\pi}\int_0^{\infty}\int_0^{2\pi} f(r,\theta)\, r^{-iv} e^{-ik\theta}\,\mathrm{d}\theta\,\frac{dr}{r} \tag{3.11}$$

where $f(r,\theta)$ is the polar coordinates representation of a 2-D function.

$f$ is assumed to be summable over $\mathbb{R}_+^* \times \mathbb{S}^1$ under the measure $\mathrm{d}\theta\,\frac{dr}{r}$, i. e.

$$\int_0^{\infty}\int_0^{2\pi} \left|f(r,\theta)\, r^{-iv} e^{-ik\theta}\right|\mathrm{d}\theta\,\frac{dr}{r} = \int_0^{\infty}\int_0^{2\pi} \frac{1}{r} f(r,\theta)\mathrm{d}\theta dr < \infty \tag{3.12}$$

Since $f$ is positive. For $\forall(k,v) \in \mathbb{Z} \times \mathbb{R}$. $\mathbb{Z}^1$ denotes the additive group of integers, $\mathbb{R}$ denotes the additive group of the real line. $\mathbb{R}_+^*$ the multiplicative group of positive and nonzero numbers, $\mathbb{S}^1$ the unit circle of the plane $\mathbb{R}^2$ . All these groups are locally compact and commutative. The direct product $\mathbb{R}_+^* \times \mathrm{S}^1$ forms a locally compact and commutative group under the following law: $(\alpha,\theta)\mathrm{o}(\rho,\psi) = (\alpha\rho, \theta + \psi)$[81].

The FMT could be divided into main three steps, which result in the invariance to rotation, scaling and translation attacks:

- *The Fourier Transform (FT):* It converts the original image in spatial domain onto spectrum domain. The magnitude of Fourier transform itself is the translation invariant.

- *The Cartesian to Log-Polar Coordinates:* The conversion to log-polar coordinates converts the scale and rotation differences to vertical and horizontal offsets that can be measured.

- *The Mellin Transform:* A second FT, called the Mellin Transform (MT) gives a transform-space image that is invariant to rotation, scaling and translation.

## 3.3 Discrete Cosine Transform (DCT)

The discrete cosine transform attempts to decorrelate the image data. After decorrelation each transform coefficient can be encoded independently without losing compression efficiency [82].

The most common DCT definition of a 1-D sequence of length N is

$$C(u) = \alpha(u) \sum_{x=0}^{N-1} f(x) \cos\left[\frac{\pi(2x+1)u}{2N}\right] \tag{3.13}$$

For u= 0, 1,…..*N-1*. Similarly, the inverse transformation is defined as

$$f(\mathrm{x}) = \sum_{u=0}^{N-1} \alpha(u) C(u) \cos\left[\frac{\pi(2x+1)u}{2N}\right] \tag{3.14}$$

For $x$ = 0, 1,…..*N-1.* In both equation (3.13) and (3.14) $\alpha(u)$ is defined as

$$\alpha(u) = \begin{cases} \sqrt{\frac{1}{N}} & for\ u = 0 \\ \sqrt{\frac{2}{N}} & for\ u \neq 0 \end{cases} \tag{3.15}$$

The 2-D DCT is a direct extension of the 1-D case and is given by

$$C(u,v) = \alpha(u)\alpha(v) \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} f(\mathrm{x},\mathrm{y})\ \cos(\frac{\pi(2i+1)u}{2N})\cos(\frac{\pi(2i+1)v}{2N}) \tag{3.16}$$

For $u, v$ = 0, 1, 2…..*N-1.* The inverse transform is defined by

$$f(\mathrm{x},\mathrm{y}) = \sum_{u=0}^{N-1} \sum_{v=0}^{N-1} \alpha(u)\alpha(v) C(u,v)\ \cos\left(\frac{\pi(2i+1)u}{2N}\right)\cos\left(\frac{\pi(2i+1)lv}{2N}\right) \tag{3.17}$$

For x, y = 0, 1, 2…..*N-1.* The main advantages of the DCT are that it gives a real output image and that it is a fast transform. A major use of the DCT is in image compression. Indeed, after performing a DCT it is possible to discard the coefficients representing high frequency components that the human eye is not very sensitive to. Thus, the amount of data can be reduced, without seriously affecting the way an image appears to the human eye.

## 3.4 Discrete Wavelet Transform (DWT)

The wavelet decomposition is a mathematical tool allowing the study of signals and signal generating processes characterised by a non-stationary behaviour. It accounts for the evolution in time of the frequency content of a signal [80]. A signal $x(t)$ can

often be better analysed, described, or processed if expressed as a linear decomposition by

$$x(t) = \sum_{j,k} a_{j,k}\, 2^{\frac{j}{2}} \psi(2^j t - k) \tag{3.18}$$

Where the two-dimensional set of coefficients $a_{j,k}$ is called *discrete wavelet transform* (DWT) of $x(t)$. Note that the basis functions $\psi_{j,k}(t) = 2^{\frac{j}{2}}\psi(2^j t - k)$ are generated from a single function $\psi(t)$ called *"mother wavelet"* by changing two parameters *j* and *k*. The location of the wavelet moves in time or space, as the index *k* changes. This allows the expansion to explicitly represent the location of events in time or space and enables a representation of detail or resolution. A more precise way of indicating how the $a_{j,k}'s$ are calculated can be written using the inner products as

$$x(t) = \sum_{j,k} \langle \psi_{j,k}(t), x(t) \rangle \psi_{j,k}(t) \tag{3.19}$$

### 3.4.1 Multiresolution Analysis

The multiresolution formulation of wavelet systems is designed to represent signals where a single event is decomposed into finer and finer details. As described earlier for the wavelet, a set of scaling function is defined in terms of integer translated of the basic scaling function $\varphi$(t) by

$$\varphi_k = \varphi(t - k);\ k \in Z, \varphi \in L^2 \tag{3.20}$$

`The subspace of $L^r\Re$ spanned by these function is defined as

$$V_0 = \overline{Span_k(\varphi_k(t))} \tag{3.21}$$

A two-dimensional family of functions is generated from the basic scaling function by scaling and translation by

$$\varphi_{j,k}(\mathrm{t}) = 2^{j/2}\varphi(2^j t - k) \tag{3.22}$$

whose span over $k$ is

$$V_j = \overline{Span_k(\varphi_k(t))} \tag{3.23}$$

This means that if $x(t) \in V_j$, then it can be expressed as

$$x(t) = \sum_k a_k \ \varphi(2^j t - k) \tag{3.24}$$

For j>0, the span can be larger since $\varphi_{j,k}$ is narrower and is translated in smaller steps, the basic requirement of multi resolution analysis is

$$V_0 \subset V_1 \subset V_2 \ldots\ldots\ldots \subset L^2 \tag{3.25}$$

Hence, the spaces $V_j$ satisfy a natural scaling condition

$$x(t) \in V_j \Leftrightarrow x(2t) \in V_{j+1} \tag{3.26}$$

The important features of a signal can be better described by also using a set of wavelet functions $\psi_{j,k}$(t) that span the differences between the successive spaces $V_j$. Let us denote the orthogonal complement of $V_j$ in $V_{j+1}$ as $W_j$. It follows

$$V_1 = V_0 + W_0 \tag{3.27}$$

Which extends to

$$V_n = V_0 + W_0 + W_1 + \cdots + W_{n-1} \tag{3.28}$$

Therefore, a signal $x(t) \in V_n$ can be expressed as

$$x(t) = \sum_k a_k \ \varphi(t-k) + \sum_{j=0}^{n-1} \sum_k d(j,k)\, \psi_{j,k}(\mathrm{t}) \tag{3.29}$$

Equation (3.29) represents a decomposition of $x(t)$ with n resolutions (or scales). The first summation gives a function that is a low resolution or coarse approximation of $x(t)$. For each increasing index $j$ in the second summation, a higher or finer resolution is added, which adds increasing detail. This is somewhat analogous to a Fourier series where the higher frequency terms contain the detail of the signal. From Equation (3.25) it can be observed that if a function $\varphi(t)$ is in $v_{j-1}$, it is also in $V_j$,

which is the space spanned by $\varphi(2^j t)$. This means $\varphi(2^{j-1}t)$ can be expressed in terms of a weighted sum of shifted $\varphi(2^j t)$

$$\varphi(2^{j-1}t) = \sum_n h(n)\ 2^{j/2}\varphi(2^j t - n) \tag{3.30}$$

Similarly, since $W_{j-1} \subset V_j$, $\varphi(2^{j-1}t)$ can be expressed as

$$\varphi(2^{j-1}t) = \sum_n g(n)\ 2^{j/2}\varphi(2^j t - n) \tag{3.31}$$

Assume a signal $x(t) \in V_j$ which can therefore be written as

$$x(t) = \sum_k a_{j-1,k} 2^{\frac{j-1}{2}} \varphi\left(2^{j-1}t - k\right) + \sum_k d_{j-1,k} 2^{\frac{j-1}{2}} \varphi\left(2^{j-1}t - k\right) \tag{3.32}$$

where

$$a_{j-1,k} = \langle x(t), 2^{\frac{j-1}{2}} \varphi\left(2^{j-1}t - k\right)\rangle = \int_{-\infty}^{\infty} x(t), 2^{\frac{j-1}{2}} \varphi\left(2^{j-1}t - k\right) dt \tag{3.33}$$

and

$$d_{j-1,k} = \langle x(t), 2^{\frac{j-1}{2}} \varphi\left(2^{j-1}t - k\right)\rangle = \int_{-\infty}^{\infty} x(t), 2^{\frac{j-1}{2}} \varphi\left(2^{j-1}t - k\right) dt \tag{3.34}$$

From equation (3.30) and (3.32) one can deduce

$$a_{j-1,k} = \sum_m h(m-2k)\, a_{j,k} \tag{3.35}$$

and

$$d_{j-1,k} = \sum_m g(m-2k)\, a_{j,k} \tag{3.36}$$

The last two equations represent a digital filtering process followed by a down sampling (also called decimating) by a factor of 2. The down sampling takes a signal $x(n)$ as an input and produces an output $(n) = x(2n)$ . These equations shows that the scaling and wavelet coefficients at different levels of scale can be obtained by convolving the expansion coefficients at scale $j$ by the time reversed recursive coefficients $h(-n)$ and $g(-n)$ then down sampling to give the expansion coefficients at the next level of $j$-1. In other words, the scale $j$ coefficients are filtered by two FIR digital filters with coefficients $h(-n)$ and $g(-n)$. Subsequently, the down –sampling gives the next coarser scaling and wavelet coefficients. These structures implement Mallat's algorithm [83] and have been developed in filter bank, quadrature mirror filters, conjugate filters, and perfect reconstruction filter bank in the literature [84]. Mallat, Daubechies, and others showed the relation of wavelet coefficient calculation and filter banks. The implementation of Equation (3.35) and (3.36) is illustrated in Figure 3.1. where the down –pointing arrows denote a down sampling by two and other boxes denote convolution by $h(-n)$ or$g(-n)$. This splitting, filtering, and decimation can be repeated on the scaling coefficients to give the two-scale structure in Figure 3.2.


Figure 3.1: One-stage wavelet decomposition

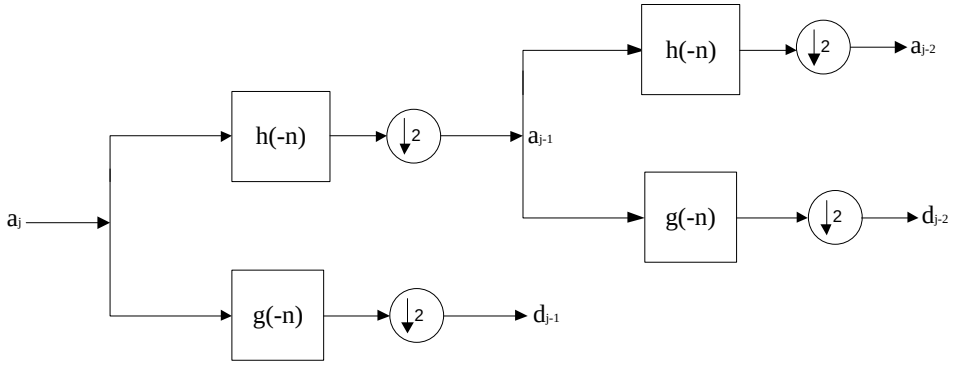



Figure 3.2: Two-stage wavelet decomposition

This Splitting, filtering, and decimation can be repeated on the original fine scale coefficients and can be made from a combination of the scale function and wavelet coefficients at a coarse resolution. This derived by considering a signal in the *j* scaling function space $x(t) \in V_j$, which can be expressed as given by Equation (3.32) or in terms of the scaling function at the same level j by

$$x(t) = \sum_k a_{j,k}\, 2^{j/2}\, \varphi(2^j t - k) \tag{3.37}$$

Substituting Equation 3.30 and 3.31into 3.32 gives

$$x(t) = \sum_k a_{j-1,k} \sum_n h(n)\; 2^{\frac{j}{2}} \varphi\left(2^j t - 2k - n\right) + \sum_k d_{j-1,k} \sum_n g(n)\; 2^{\frac{j}{2}} \varphi\left(2^j t - 2k - n\right) \tag{3.38}$$

Because all of these functions are orthogonal, multiplying the equation 3.37 and 3.38 by $\varphi\left(2^j t - k'\right)$

By integrating the coefficient can be rewritten as:

$$a_{j,k} = \sum_m a_{j-1,k}\; k(k-2m) + \sum_m d_{j-1,k}\; g(k-2m) \tag{3.39}$$

The final equation is actually evaluated by up-sampling the (*j*-1) scale coefficient sequence $a_{j-1,k}$, which means double its length by inserting zeros between each term, then convolving it with the scaling filter $h(n)$. The same procedure is performed to the (*j*-1) level wavelet coefficient sequence $d_{j-1,k}$ and the results are added to produce the *j* level scaling function coefficients $a_{j,k}$.This structure is illustrated in Figure3.3. This process can be continued to any level by combining the appropriate scale wavelet coefficients.

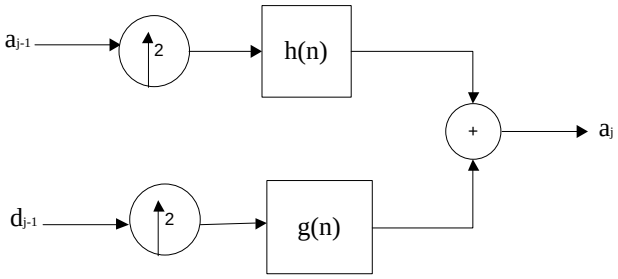



Figure 3.3: One-stage wavelet reconstruction

The resulting two-scale tree is shown in Figure 3.4

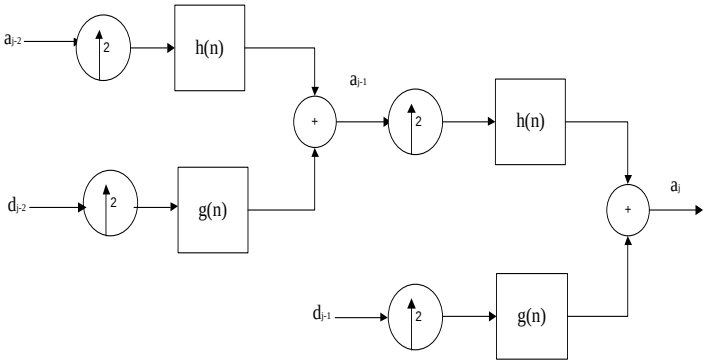



Figure 3.4: Two-stage wavelet reconstruction.

## 3.4.2 Properties

In practical application, wave bases can judiciously be chosen to fit the behaviour of the data to be analysed. An excellent choice of the wavelet bases can optimise signal processing algorithms. Indeed, a wavelet basis that produces more coefficients with a magnitude closed to zero is preferred more in data compression, since theses coefficients require less bits to encode. The most relevant criteria are the number of vanishing moments, the size of the support and regularity.

The number of vanishing moments is related to the smoothness or differentiability of $\varphi(t)$ and $(t)$. The size of the support measure the interval in

time in which the wavelet takes non-zero values. Regularity is defined ill terms of zeros of the frequency response function of the scaling filter $h(n)$ thus, indicating how fast the Fourier transform magnitude drops off, as the frequency progresses to infinity. This is particularly related to the frequency localisation of the decomposed signal.

The size of the wavelet support increases with the number of vanishing moments. The wavelet regularity is important to reduce the artefacts. The choice of an optimal wavelet in image compression is thus the result, of a trade-off between the number of vanishing moments and artefacts. Some useful properties of the wavelet transform can be summarised as follows:

- They can represent smooth functions
- They can represent singularities
- The basis functions are local. This makes most coefficient-based algorithms naturally adaptive to inhomogeneities in the function.
- They have the unconditional basis property for a variety of function classes implying that if one does not know much about a signal (for instance, a signal with a non-stationary behaviour), the wavelet basis is usually a reasonable choice.
- They are computationally inexpensive with a complexity *O (N)* compared to a Fourier transform, which is *Nlog(N)* or an arbitrary linear transform which is $O(N^2)$.

### 3.4.3 2-D wavelet transform

For 2-D data such as images, the most commonly used algorithm for wavelet decomposition uses separable one-dimensional wavelets and scaling functions.

This kind of two-dimensional DWT leads to a decomposition of approximation coefficients at level *j* in four components: the approximation at level

$j$—1($a_{j-1}$), and the details in three orientations (horizontal$d_{j-1}^{(h)}$, vertical$d_{j-1}^{(v)}$, and diagonal$d_{j-1}^{(d)}$), Figure 3.5 describes the basic decomposed steps for images.

An example of a one stage decomposed image of "Lena" is illustrated by Figure3.6. In a similar way, the reverse process can be used to obtain the original 2-D signal.

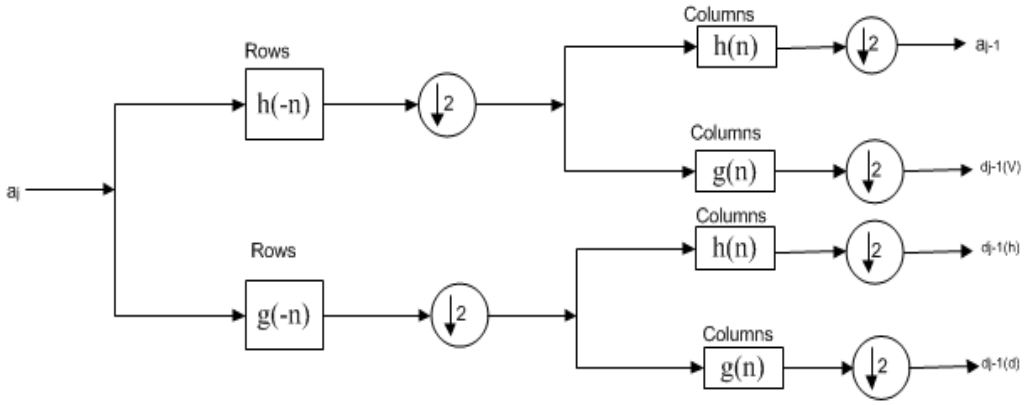
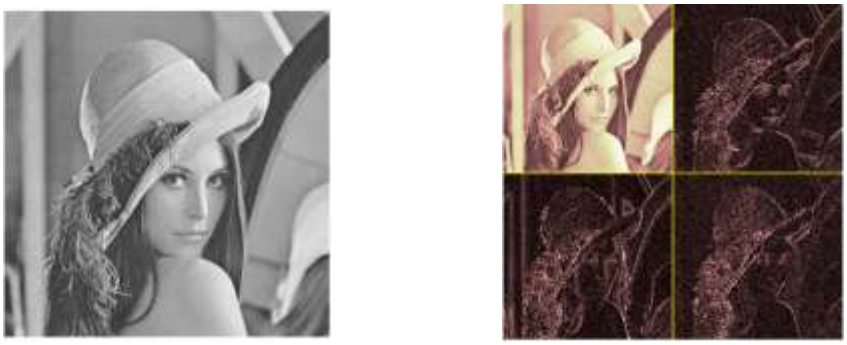



Figure 3.5: One-stage 2-D wavelet decomposition



(a) Original Image (b) Decomposed Image

Figure 3.6: One-stage 2-D wavelet decomposition of "Lena".

## 3.5 Summary

In this chapter, the basic characteristics of transform domain: Discrete Fourier Transform, Discrete Cosine Transform and Fourier-Mellin Transform and Discrete Wavelet Transform, are reviewed. These techniques are very promising, within biometric and image processing. The transform domain technique are the most challenging part of the image hashing in the feature extraction stage, the extracted

feature are invariant to image processing operation and geometric attacks. In next chapter, the recent state-of-the-art feature extraction techniques such as: end-stopped wavelets, SURF, SIFT, and SIFT-Harris are presented.

# Chapter 4

# Image Feature Extraction Techniques

## 4.1 Introduction

Recent research in biometric recognition systems has been performed to secure the biometric through hash based techniques. An image hash can be constructed by a set of features from images to form a compact representation that can be used for the authentication and integrity of the data. The selection of a feature extraction technique is a key step in any biometric recognition system and all pattern recognition systems. The recognition process analyses the spatial geometry of the distinguishing feature of the image. Different methods exist to extract the identifying features of an image, although in general they can be classified into three approaches: Feature-based approaches, Appearance-based approaches and Hybrid approaches

- ***Feature-based approaches***: This approach is based on the properties of individual appendages located on a biometric trait, such as eyes, nose and mouth on a face, wrinkles lines for a palm print, eye lashes for an iris, etc, as well as their relationships with each other.

- ***Appearance-based approaches*:** These are based on information theory concepts and seek a computational model that describes a biometric image. This works by extracting the most relevant information contained in the image without dealing with the individual appendages.

- ***Hybrid approaches*:** This approach uses both holistic feature and local features. Modular eigenfaces and component-based feature can be given as examples.

Once a raw image is properly pre-processed (i.e., enhancement, formatting, segmentation, etc), the feature extraction algorithm can then be used to extract the relevant features. The feature extraction algorithms can be classified into two groups: Global Feature Extractors and Local Feature Extractors.

- ***Global Feature Extractors***: Aim to locate usable features from the raw data at the overall image level. They process the image as a whole and attempt to extract the features, e.g. the Gabor wavelet-based approach for iris and fingerprint recognition.

- ***Local Feature Extractors***: Focus on the block of image data. These algorithms work on small windows within the images and extract the relevant features, e.g. minutiae extraction.

The feature points should be largely invariant under perceptually insignificant distortions. The feature extraction techniques discussed in terms of robustness to content-preserving operations include rotation, translation and other variations. The state of the art feature extraction techniques: End Stopped Wavelets [14], SIFT [51], SURF [15] and SIFT-Harris [16] are approached to solve problems in the image based biometric, including fingerprint, face, etc.

## 4.2 End-Stopped Wavelets

Psychophysical studies have identified the presence of certain cells, called hypercomplex or end stopped cells, in the primary visual cortex. Two types of end-stopped cells have being identified. The single end-stopped cells respond strongly to extremely robust image features, for instance corner like stimuli and points of high curvature. The second type of end-stopped cells responds strongly to a linear segments or curved lines. The term end-stopped comes from the impressive sensitivity of these cells to end-points of linear structures, and moreover, Bhattacharjee et al [85] construct ‘‘end –stopped’’ wavelets to capture this behaviour. The construction of the wavelet kernel or basis function combines two operations. Firstly, linear structures having a certain orientation are selected. These linear structures are then processed to detect line-ends (corners) and or high curvature points. Morlet wavelets can be used to detect linear structures having a specific orientation. In the spatial domain, the 2-D Morlet wavelet is given as [85];

$$\psi_M(X) = \left(e^{j\mathrm{k}_0.\mathrm{X}} - e^{-\frac{1}{2}|\mathrm{k}_0|^2}\right)\left(e^{-\frac{1}{2}|\mathrm{X}|^2}\right) \tag{4.1}$$

where X = $(x, y)$ represents 2-D spatial coordinates, and $K_0 = (K_0, K_1)$ is the wave-vector of the mother wavelet, which determines the scale-resolving power and angular-resolving power of the wavelet. The frequency domain representation $\psi_M(K)$ of a Morlet wavelet is

$$\hat{\psi}_M(K) = \left(e^{-\frac{1}{2}|\mathrm{k}-\mathrm{k}_0|^2} - e^{-\frac{1}{2}|\mathrm{k}_0|^2}\right)\left(e^{-\frac{1}{2}|\mathrm{k}|^2}\right) \tag{4.2}$$

Here, $K$ represents the 2-D frequency variable $(\mathcal{U}, \mathcal{V})$. The Morlet function is similar to the Gabor function, although with an extra correction term $e^{-\frac{1}{2}(|\mathrm{k}|^2+|\mathrm{X}|^2)}$ to make it an admissible wavelet. The orientation of the wave-vector determines the orientation tuning of the filter. A Morlet wavelet detects linear structures orientated perpendicular to the orientation of the wavelet.

In two dimensions, the end points of the linear structures can be detected by applying the first derivative of the Gaussian (FDoG) filter in the direction parallel to the orientation of the structures in question. The first filtering stage detects lines having a specific orientation and the second filtering stage detects end-points of those particular lines. These two stages can be combined into a single filter to form an "end-stopped" wavelet (Figure 4.1). For example, the end-stopped wavelet and its 2-D Fourier transform is as follows:

$$\psi_E(x, y) = \frac{1}{4} y e^{-\left(\frac{x^2+y^2}{1}+\frac{k_0}{1}(k_0-2jx)\right)} \tag{4.3}$$

$$\hat{\psi}_E(\mathcal{U}, \mathcal{V}) = 2\pi\left(e^{-\frac{(u^2-k_0)+(v^2)}{2}}\right)\left(jve^{-\frac{u^2+v^2}{2}}\right) \tag{4.4}$$

Equation (4.4) shows $\hat{\psi}_E$ as a product of two factors. The first factor is a Morlet wavelet orientated along the axis. The second factor is a FDoG operator applied along the frequency axis $\mathcal{V}$, i.e., in a perpendicular direction to the Morlet wavelet. Hence, this wavelet detects line ends and high curvature points in the vertical direction.

(a) (b) (c)

Figure 4.1: Behaviour of the end-stopped wavelet on a synthetic image. (a) Synthetic L-shaped image. (b) Response of a Morlet wavelet. (c) Response of the end-stopped wavelet[14].

Monga et al [14] recommend a feature extraction technique that computes a wavelet transform based on an end-stopped wavelet obtained by applying the FDoG operator to the Morlet wavelet

$$\psi_E(x, y, \theta) = (FDoG)o\big(\psi_M(x, y, \theta)\big) \tag{4.5}$$

and orientation tuning is given by $\theta = \tan^{-1}((k_1/k_0))$.

The orientation range $[0,\pi]$ need be divided into M intervals and the scale parameter $\alpha$ be sampled exponentially as $\alpha^i, i \in Z$. This results in a wavelet family

$$(\psi_E\left(\alpha^i(x, y, \theta_k)\right), \alpha \in \mathcal{R}, i \in Z \tag{4.6}$$

Where $\theta_k = k\pi/M$ , $k = 0, \ldots \ldots M - 1$.

The wavelet transform is

$$W_i(x, y, \theta) = \iint f(x_1, y_1)\ {\psi_E}^* \times \left(\alpha^i(x - x_1, y - y_1, \theta)\right) dx_1 dy_1 \tag{4.7}$$

Monga's feature detection method preserves significant image geometry feature points of an image as: (1) Computes the wavelet transform for each image location (2) Identifies significant features by looking for local maxima of the magnitude of the wavelet coefficients in a preselected neighbourhood. (3) Thresholding to eliminate spurious local maxima in featureless region of the image. These feature detection methods have two free parameters: integer scale $i$ and real threshold T. The threshold is used to select a fixed number of feature points from the image and

an image feature vector is formed by collecting the magnitudes of the wavelet coefficients at the selected feature points.

### 4.2.1 Experimental Results

In this novel work, Hausdorff distance is used to characterize the robustness and discriminability of the feature points.

**a) *Hausdorff Distance*** [87]

Given two finite points sets A=$\{a_1, a_2, a_3, a_4 \ldots\ldots a_p\}$ and B=$\{b_1, b_2, b_3, b_4 \ldots\ldots b_p\}$, the Hausdorff distance is defined as

$$H(\mathrm{A}, \mathrm{B}) = \max\left(h(\mathrm{A}, \mathrm{B}), h(\mathrm{B}, \mathrm{A})\right) \tag{4.8}$$

$$\text{Where} \quad h(\mathrm{A}, \mathrm{B}) = \max_{a \in A} \min_{b \in B} \|A - B\| \tag{4.9}$$

and $\|.\|$ is the underlying norm on the points of A and B. The function $h$ (A, B) is called the directed Hausdorff distance from A to B. $h$ (A,B) in effect rank each point of A based on its distance to the nearest point on B and subsequently uses the largest ranked point as the distance. The Hausdorff distance $H$ (A, B) is the maximum of $h$ (A, B) and $h$ (B, A).

***b) Result and Analysis***

The algorithm is tested on a fingerprint image (Figure 4.2) database of 100 images from FVC2004/DB1_A [88]. The similarity of the feature point hash to the original and identical images are evaluated through the Hausdorff distance against distortion of the JPEG compression with the quality factor 10%, Additive white Gaussian Noise (AWGN) of Signal-Noise Ratio (SNR) 10%, Rotation $1^0$ ~ $15^o$, a median filter of window size 3x3, and low pass filter as mentioned in Table 4.1. Table 4.2 tabulates the quantitative deviation as the Hausdorff distance between the hash values of the original and manipulated images for various attacks. The deviations are less than 0.3 values except for large rotation (greater than $10^o$) and AWGN of SNR (more than 10%).

Figure 4.2: Fingerprint images from FVC2004/DB1_A database

Table 4.1: Different Attacks used to assess the End Stopped Feature point

| **Attack** | **Parameters** |
|---|---|
| **Image Processing Operations**<br>JPEG lossy compression<br>Additive white Gaussian Noise (AWGN)<br>Median filtering<br>Low pass filtering | <br>Quality Factor =10<br>Standard deviation $\sigma = 10$<br>Window size 3x3<br>/ |
| **Geometric Distortion**<br>Rotation | <br>Degree $1^0 \sim 15^0$ |

Table 4.2: Hausdorff Distance between features of original and Attacked Image (For 32 Feature Points)

| Attack | 00_1 | 01_1 | 02_1 | 03_1 |
|---|---|---|---|---|
| JPEG,QF=10 | 0.2524 | 0.2294 | 0.1205 | 0.1669 |
| AWGN,$\sigma = 10$ | 0.8522 | 0.3151 | 0.3546 | 0.2577 |
| Rotation $1^0$ | 0.1587 | 0.1196 | 0.1620 | 0.1371 |
| Rotation $2^0$ | 0.2356 | 0.1856 | 0.1884 | 0.1654 |
| Rotation $3^0$ | 0.2065 | 0.1935 | 0.1729 | 0.1811 |
| Rotation $4^0$ | 0.2743 | 0.2254 | 0.2803 | 0.1742 |
| Rotation $5^0$ | 0.2827 | 0.2221 | 0.2768 | 0.2183 |
| Rotation $10^0$ | 0.2698 | 0.3341 | 0.3204 | 0.2913 |
| Rotation $15^0$ | 0.3490 | 0.4066 | 0.3892 | 0.3926 |
| Median Filter (3x3) | 0.2092 | 0.0983 | 0.1116 | 0.1852 |
| Low pass Filter | 0.0649 | 0.0372 | 0.0435 | 0.0444 |

## 4.3 Speeded-Up Robust Features [SURF]

SURF method has have been used in general object recognition and other machine vision applications for a number of years. The feature vectors are formed by means of local patterns around key points detected using scaled up filter size. These extracted feature vectors are established to be distinct and robust to noise and geometric and photometric deformations of image [40]. The major steps for SURF feature vectors are determined by key-point detectors and descriptors.

***a) Key-Point Detectors***

SURF detection based on Hessian Matric [89] leads to the use of integral images, which drastically reduces the computation time. In addition, integral images fit in the more general framework of boxlets [90]. The entry of an integral image $I_\Sigma(p)$ at a location $p = (x, y)$ represents the sum of all pixels in the input image $I$ within a rectangular region by the origin and $p$.

$$I_\Sigma(p) = \sum_{i=0}^{x} \sum_{j=0}^{y} I(i,j) \tag{4.10}$$

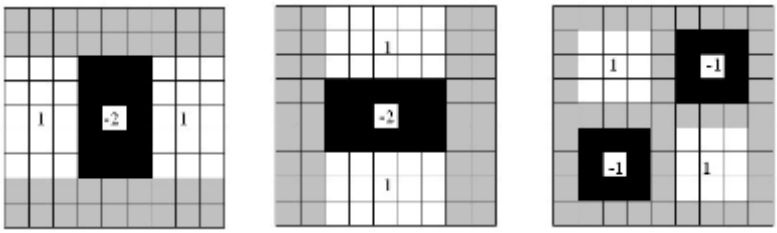
It can be said that Hessian-based detectors are more stable and repeatable than their Harris-based counterparts. Given point $p = (x, y)$ in an image $I$, the Hessian matrix $H(p, \sigma)$ in $p$ at scale $\sigma$ is defined as follows:

$$H(p, \sigma) = \begin{bmatrix} L_{xx}(p, \sigma) & L_{xy}(p, \sigma) \\ L_{xy}(p, \sigma) & L_{yy}(p, \sigma) \end{bmatrix} \tag{4.11}$$

Where $L_{xx}(p, \sigma)$ is the convolution of the Gaussian second order derivative $\frac{\partial^2}{\partial x^2} g(\sigma)$ with the image $I$ in the point $p$, and similarly for $L_{xx}(p, \sigma)$ and $L_{xy}(p, \sigma)$. The second order Gaussian derivatives are approximated using box filters as shown in Figure 4.3 and image convolutions with box filters are computed rapidly using integral images. The determinant of Hessian matrix ΔH can be reduced to

$$\Delta H = D_{xx} D_{yy} - (w D_{xy})^2 \tag{4.12}$$

The response for each spot can be determined by assigning $w$ = 0.9 [15]. Furthermore, keypoints are localized in scale and image space by applying non-maximum suppression in a 3x3x3 neighbourhood.




$x$-direction $y$-direction $xy$ direction

Figure 4.3: Approximation of the second order Gaussian partial derivative. (The grey regions are equal to zero)

***b) SURF Descriptor***

This stage consists of two sub steps. In the first sub step, a circular region is constructed around the extracted key-points and the dominant orientation of the circular region is computed using the Haar wavelets response in both $x$ and $y$ directions. The resulting maximum Haar wavelet response is considered to be the dominant orientation and is used to generate the key-point feature vector. The feature vectors of a key-point are measured relative to the dominant orientation and thus, the generated feature vectors are invariant to image rotations.

In the second sub step, a square region is constructed around each extracted key-point and aligned along the dominant orientation. This square region is partitioned into 16 sub-regions of size 4x4 and therefore, Haar wavelet responses are computed for each sub-region. The sum of the wavelet responses, *dx* and *dy*, for each sub-region are used as feature values. Further, absolute values $|dx|$ and $|dy|$ are summed up to obtain the polarity of the image intensity changes. Thus, the descriptor vector, *Des*, of the sub-image is given as

$$Des-\{\sum dx \sum dy \sum|dx| \sum|dy|\} \tag{4.13}$$

The SURF descriptor vector of the keypoint is formed by concatenating descriptor vectors of all sixteen 4x4sub-regions around a keypoint. In addition, it consists of 64 elements.

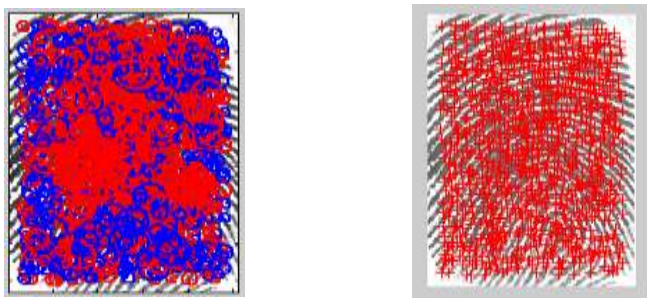
## 4.3.1 Experimental Results

SURF [15] focuses on the spatial distribution of gradient information within the local point neighbourhood. SURF is a rapid, scale and rotational invariant detector and descriptor. To verify the effectiveness of the SURF algorithm, the experiment conducted on fingerprint images and a face image of the same subject for known attacks of image processing and geometric operations as mentioned in Table 4.3. The result focuses on matching the two images (i.e., fingerprint and face) on various distortions with limited feature points. Figures 4.4 and 4.5 illustrate the feature

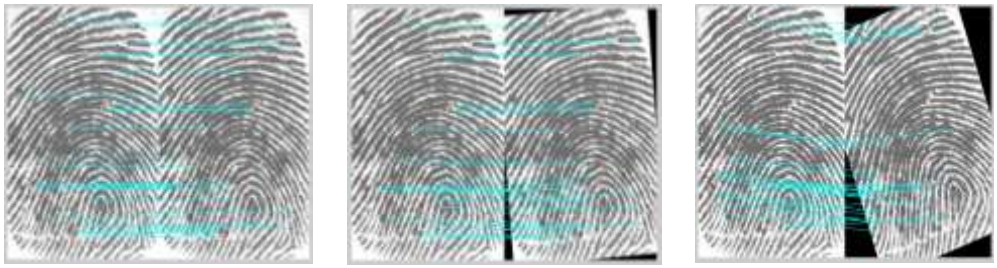
descriptors and matching of feature points (30 points) of the fingerprint image and face for various distortion like rotations (5degree, 20degree and 180degree), translation (25x25 window), histogram equalization, Median filter (5x5 window), JPEG (10%) and Additive White Gaussian Noise with a SNR of 0.065%. It was observed that descriptor vectors are matched between original and manipulated images for various attacks.

Table 4.3: Different Attacks used to assess the SURF Feature point

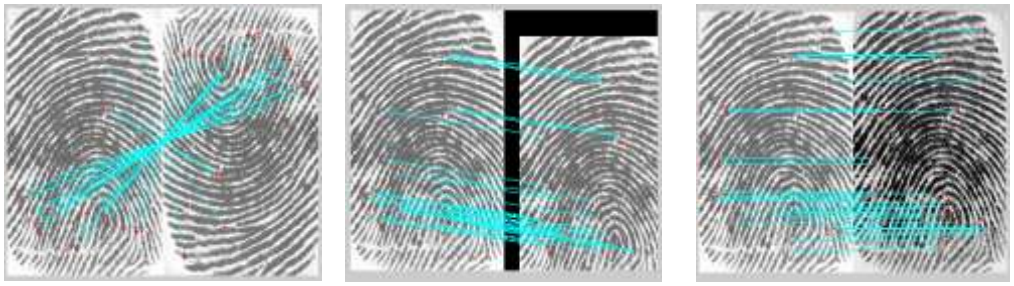
| **Attack** | **Parameters** |
|---|---|
| **Image Processing Operations**<br>JPEG lossy compression<br>Additive white Gaussian Noise<br>Median Filter<br>Histogram equalization | <br>Quality Factor =10<br>SNR of 0.065 %<br>Window size 5x5<br>/ |
| **Geometric Distortion**<br>Rotation<br>Translation | <br>Degree $0^0 \sim 180^0$<br>Window size 25x25 |



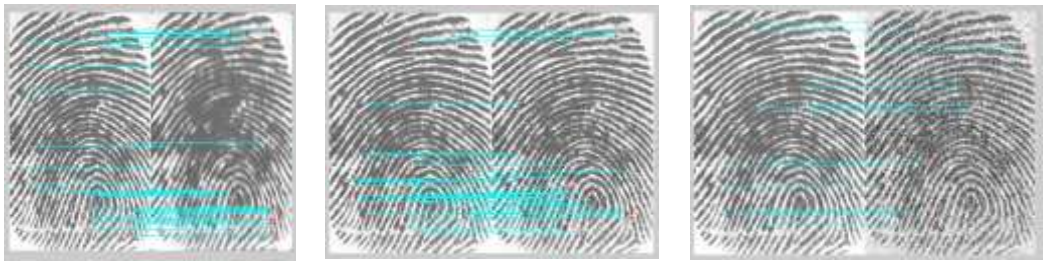
(a) Feature Descriptor (b) Feature Points (379 Points)



(c) Feature Points (d) 5 degree Rotation ( e) 20 degree Rotation

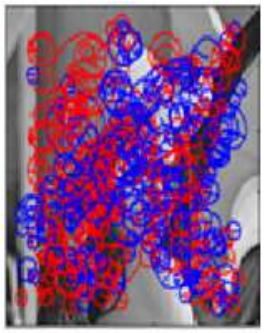


(f) 180 degree Rotation (g) Translate (25x25) (h) Histeq

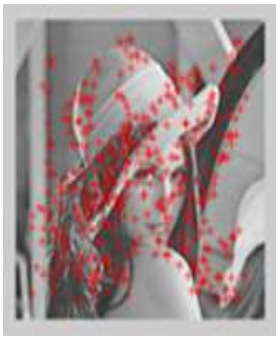


(i) Median Filter (5x5) j) JPEG (10%) (k) AWGN (0.065%)

Figure 4.4: Feature Descriptors and Matching of Feature Points (30Points) on Fingerprint Images of the same subject for different attacks: (a) Feature Descriptor (b) Feature Points (379 Points) (c) Feature Points (d) 5 degree Rotation e) 20 degree Rotation (f) 180 degree Rotation (g) Translate (25x25) (h) Histeq (i) Median Filter (5x5) j) JPEG (10%) (k) AWGN (0.065%).



(a) Feature Descriptor

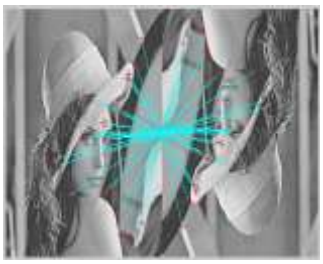


(b) Feature Points (379 Points)

(c) Feature Points

d) 5 degree Rotation

e) 20 degree Rotation



(f) 180 degree Rotation

(g) Translate (25x25)

(h) Histeq

(i) Median Filter (5x5)

j) JPEG (10%)

(k) AWGN (0.065%)

Figure 4.5: Feature Descriptors and Matching of Feature Points (30 Points) on Lena Images of the same subject for different attacks: (a) Feature Descriptor (b) Feature Points (379 Points) (c) Feature Points (d) 5 degree Rotation e) 20 degree Rotation (f) 180 degree Rotation (g) Translate (25x25) (h) Histeq (i) Median Filter (5x5) j) JPEG (10%) (k) AWGN (0.065%).

## 4.4 Scale Invariant Feature Transform [SIFT]

Local features, such as corners, blobs and regions, have been widely used for object detection, recognition and retrieval purposes in computer vision. The intrinsic advantages of these local features are their invariance under geometric operations. Among various local feature detectors and descriptors, SIFT was shown to provide a relatively optimal trade-off between robustness, unique and efficiency.

SIFT [51] mainly consists of the following steps to generate the set of an image feature: Scale-space extrema detection, keypoint localization, orientation assignment and keypoint descriptor.

***a) Scale-Invariant Points Detection and Localization***

Scale invariant local points are detected by searching for local extrema in the series of difference-of-Gaussian (DoG) image. The DoG is constructed by the convolution of a variable scale Gaussian function $G(x, y, \sigma)$, with an image $I(x, y)$ in the scale space of an image $L(x, y, \sigma)$.

$$L(x, y, \sigma) = G(x, y, \sigma) * I(x, y) \tag{4.13}$$

To efficiently detect stable keypoint locations in the scale space, using scale-space extrema in the DoG convolved with the image, $D(x, y, \sigma)$ with a nearby scale $k\sigma$ and $\sigma$ as

$$\begin{aligned} D(x, y, \sigma) &= L(x, y, k\sigma) - L(x, y, \sigma) \\ &= \big(G(x, y, k\sigma) - G(x, y, \sigma)\big) * I(x, y) \end{aligned} \tag{4.15}$$

Essentially, the DoG detector could be attributed to the detector for blob structures in the image content, as it provides a close approximation of the scale-normalized Laplacian of Gaussian.

$$G(x, y, k\sigma) - G(x, y, \sigma) \approx (k - 1)\sigma^2 \nabla^2 G \tag{4.16}$$

Substituting (4.16) into (4.15) and using a property of convolution to obtain

$$D(x, y, \sigma) \approx (k-1)\sigma^2\nabla^2 G * I(x, y)$$

$$= (k-1)\sigma^2\nabla^2 * \nabla^2 I(x, y) \quad (4.17)$$

where the Laplacian operator $\nabla^2 I(x, y)$ is used to detect edges and corners in the images. Equation (4.17) is DoG, is approximation of Laplacian of Gaussian and provides greater robustness against geometric transform of images compared with other gradient based feature points detectors such as Harris and Hessian, etc.

***b) Orientation Assignment and Descriptor Generation:***

The orientation of each key-point is determined by the peak of the orientation histogram formed by the gradient orientations within its neighbourhood. Based on the position, scale and orientation of each key-point, the corresponding descriptor with 128 dimensions based on gradient histogram within its 16x16 local neighbourhood is generated.

## 4.5 SIFT-Harris

DoG detector of SIFT provides a satisfying performance under geometric transforms; however, its robustness against attacks, like additive noise and blurring, is poor [16]. To extract robust local features, it is desirable to select the most stable key-points under various distortions and attacks. The Harris corner [91] could provide a stable detection performance with high repeatability and localization accuracy under various distortion and geometric transformations. Therefore, the Harris criterion is incorporated to select the most stable SIFT keypoints.

The Harris detector / criterion is based on the auto correlation matrix, which represents the gradient distribution within a local region of the selected point. The autocorrelation matrix M for image $I(x, y)$ is represented as

$$M = \sum_{x,y} w(x, y) \begin{vmatrix} I_x^2 & I_x I_y \\ I_x I_y & I_y^2 \end{vmatrix} \quad (4.18)$$

Where $w(x, y)$ is a window to determine the accumulated region, and $I_x$ and $I_y$ are the image gradients in $x$ and $y$ axis, respectively. Furthermore, there is alternative criterion to evaluate the corner points as;

$$H=\lambda_1\lambda_2 - K(\lambda_1 + \lambda_2)^2 = \det(M) - K(trace^2(M) \quad (4.19)$$

where $\lambda_{1,}\lambda_2$ are eigenvalues of autocorrelation matrix $M$ and $K$ is a coefficient ranging from 0.04 - 0.15 empirically. In this research work, $K = 0.06$ [16].

Given a set of SIFT points $= \{p_i(x, y, \sigma, \theta)\}_{i=1}^{N}$ , where $x$ and $y$ are coordinates and $\sigma, \theta$ are scale and orientation parameters, respectively. $H_i^{\sigma}(x, y)$ is the Harris response where $\sigma$ is the standard deviation of the Gaussian kernel window used to compute the auto-correlation matrix M and set the threshold $T$ to select the robust SIFT point as

$$T = \frac{\alpha}{N}\sum_{i=1}^{N} H_i^{\sigma}(x, y) \quad (4.20)$$

where α is an adjustable parameter to control the robust points selection and empirically α ∈ [0.1, 0.5]. Therefore, to control the robustness 0.5 is chosen as the default value.

### 4.5.1 Experimental Results

SIFT feature key points consist of local maxima or minima together with the gradient histogram. During matching, all the SIFT key points of the two images are compared. Intuitively, the SIFT algorithm is able to localize objects in an image, it can also help to determine whether two images contain identical content. Based on such consideration, the algorithms for SIFT and SIFT-Harris are tested on a natural image of size 256x256, between the original image and known distortion like Gaussian Noise ( var =0.005), Gaussian Blurr (var =0.5, 5x5 window), JPEG (QF =10%) as illustrated in Table 4.4.

Table 4.4 Comparison of keypoints Detectors on original and distorted Image

| **Attacks** | **SIFT** | | **SIFT-Harris** | |
|---|---|---|---|---|
| | Original Image Keypoints | Distoted Image Keypoints | Original Image Keypoints | Distoted Image Keypoints |
| Gaussian Noise (var =0.005) | 306 | 370 | 87 | 117 |
| Gaussian Blurr (var =0.5, 5x5) | | 353 | | 117 |
| JPEG (QF =10 %) | | 460 | | 148 |

Furthermore, an investigation is performed on the benefits of robust keypoints against content preserving manipulations for the purpose of content identification. In this analysis Hausdorff distance is used to measure the similarity between the coordinates of the two sets of features detected in the original and distorted images. Alongside this, Hausdorff is used to compare the state of the art feature detector SIFT-harris with end stopped wavelet detector in terms of robustness against content preserving manipulation, as shown in Table 4.5. The feature vector are coordinates of the top 20 detected stable keypoints. It is observed that the average Hausdorff distance for a keypoint detected by the SIFT-Harris detector are smaller than an end stopped wavelet.

Table 4.5 Average Hausdorff Distance between the coordinate for the top 20 keypoints detected in the original and manipulated copies using the SIFT-harris and End Stopped Detector.

| **Manipulation** | **SIFT Harris** | **End Stopped** |
|---|---|---|
| Gaussian Noise (Var =0.005) | 0.0039 | 0.0567 |
| Salt and pepper Noise (Var =0.01) | 0.0008 | 0.0902 |
| Speckle Noise (Var =0.01) | 0.0013 | 0.0066 |
| JPEG, QF =10 | 0.0021 | 0.0131 |

## 4.6 SIFT-Wavelet

Content Based Image Retrieval (CBIR) plays significant role in image processing and its mainly focus on describing the bottom information of images, such as color, texture, etc., These methods have some achievements but they have more difficulties to describe image scaling, rotation movement, affine and other features in detail. One of the appealing methods is to collect the salient points (feature points) using low-level characteristics such as Harris detector and SIFT. Salient points can also be detected on the wavelet domain. Wavelet based technique is basically used to provide more security and reliability of image. It decomposes an image into various resolutions which provide approximate and detail coefficients of image, which is then further processed for feature extraction and matching. In this proposed research we combined SIFT feature with efficient wavelet-based salient points to generate robust SIFT - wavelet feature that provides sufficient invariance to common image manipulations. The detail literature and the proposed block diagram are explained in section 5.4.2

## 4.7 Overview of Feature Detector

An invariant feature is an image pattern which differs from its immediate neighbourhood and is usually associated with a change in an image property, such as intensity, colour and texture. A good set of features holds the following properties:

- *Repeatability:* in which the feature extraction process should be repeatable and precise, so that the same features are extracted on two images showing the same object.

- *Distinctiveness:* is the intensity pattern underlying the feature variations, which can be distinguished and matched.

- *Locality:* allows the features invariant to reduce the probability of occlusion and model approximations of the geometric and photometric deformations between two images at different viewing conditions.

- *Quantity:* the number of detected features should be sufficiently large, so that a reasonable number of features are detected, even on small objects.

- *Accuracy*: the detected features should be accurately localized, both in image location, with respect to scale and possibly shape.

- *Efficiency:* the detection of features in a new image should allow for time critical applications.

Table 4.6 [49] provides an overview of the feature detector and has been grouped according to their invariance: rotation, similarity, affine and perspective. The Harris detector has rotational invariant features with the highest repeatability and localization accuracy. The Hessian detector locates blobs which are not as well localized and requires second-order derivatives to be computed. The SUSAN detector avoids computation of derivatives and is known for its efficiency; however, the absence of smoothing makes it more susceptible to noise.

In scale, invariant feature group Harris-Laplace has been shown to have high repeatability and localization accuracy inherited from the Harris detector. Hessian-Laplace is more robust than its single scale nature, which is due to blob-like structures that are better localized in scale than corners. In this invariant group, DoG and SURF detectors were designed for efficiency. The DoG detector performs extremely well in matching and image retrieval due to superior balance between spatial localization and scale estimation accuracy.

The affine invariant Harris and Hessian follows the invariance properties. In addition, the salient regions require computing of a histogram and its entropy for each regions candidate in the scale or affine space, which results in large computational costs. Thus, the edge based regions focus on corners formed by edge junctions and provides good localization accuracy and repeatability with a fewer number of detected features.

Intensity based regions use a heuristic method and find similar regions to the Maximally Stable Extremal Regions (MSER). Superpixels are typically based on segmentation methods, which are computationally expensive like normalized cuts. In

contrast to the superpixels, the MSER selects only the most stable regions, which results in high repeatability.

Binary Robust Independent Elementary Features (BRIEF) descriptors are relies on a relatively small number of intensity difference tests to represent an image patch as a binary string. BRIEF construction and matching for this descriptor much fast to yield higher recognition rates. The descriptor similarity can be evaluated using the Hamming distance, which is very efficient to compute, instead of the L2 norm as is usually done.

Binary Robust Invariant Scalable Keypoints (BRISK) tackles the classic Computer Vision problem of detecting, describing and matching image keypoints for cases without sufficient a priori knowledge on the scene and camera poses. BRISK relies on circular sampling pattern from which it computes brightness comparisons to form a binary descriptor string and offers the quality of high-end features in time demanding applications.

Fast Retina keypoint (FREAK) is a fast, compact and robust keypoint descriptor. A cascade of binary strings is computed by efficiently comparing pairs of image intensities over a retinal sampling pattern. FREAKs are general faster to compute with lower memory load and also more robust than SIFT, SURF or BRISK.

Table 4.6: Overview of Feature Detector [50]

| Feature Extractor | Corner | Blob | Region | Rotation Invariant | Scale Invariant | Affine Invariant | Repeatability | Localization Accuracy | Robustness | Efficiency |
|---|---|---|---|---|---|---|---|---|---|---|
| Harris | ✓ | | | ✓ | | | +++ | +++ | +++ | + |
| Hessian | | ✓ | | ✓ | | | ++ | ++ | ++ | + |
| SUSAN | ✓ | | | ✓ | | | + | ++ | ++ | +++ |
| Harris-Laplace | ✓ | ✓ | | ✓ | | | +++ | +++ | ++ | + |
| Hessian-Laplace | ✓ | ✓ | | ✓ | ✓ | | +++ | +++ | +++ | + |
| DoG | ✓ | ✓ | | ✓ | ✓ | | ++ | ++ | ++ | ++ |
| SURF | ✓ | ✓ | | ✓ | ✓ | | ++ | ++ | ++ | +++ |
| Harris-Affine | ✓ | ✓ | | ✓ | ✓ | ✓ | +++ | +++ | + | + |
| Hessian Affine | ✓ | ✓ | | ✓ | ✓ | ✓ | +++ | +++ | +++ | + |
| Salient Regions | ✓ | ✓ | | ✓ | ✓ | ✓ | + | + | ++ | + |
| Edge-Based | ✓ | ✓ | | ✓ | ✓ | ✓ | +++ | +++ | + | + |
| MSER | | | ✓ | ✓ | ✓ | ✓ | +++ | +++ | ++ | +++ |
| Intensity Based | ✓ | | ✓ | ✓ | ✓ | ✓ | ++ | ++ | ++ | ++ |
| Superpixels | | | ✓ | ✓ | ✓ | ✓ | + | + | + | + |
| BRIEF | ✓ | ✓ | | ✓ | ✓ | | ++ | ++ | ++ | +++ |
| BRISK | ✓ | ✓ | | ✓ | ✓ | | ++ | ++ | ++ | +++ |
| FREAK | ✓ | ✓ | | ✓ | ✓ | | ++ | ++ | +++ | +++ |

## 4.8 Summary

In this chapter, the most recent state-of-the-art feature extraction techniques: end-stopped wavelets, SURF, SIFT, and SIFT-Harris are investigated for their perceptual robustness against various content-preserving manipulations. Based on geometric invariance of the SIFT keypoints, Harris criterion are incorporated to select the most stable feature points under the addition of noise and blurring. The performance of this feature detector is evaluated through Hausdorff distance to measure the similarity between the feature vector of the original and distorted images. The feature vectors are coordinates of the top 20 detected stable keypoints. The average Hausdorff distance of the keypoint detected by the SIFT-Harris detector are smaller than end stopped wavelets. Therefore SIFT-Harris is relatively more stable for geometric operations, especially for blurring operations and additive noise attacks. This chapter also discusses the overview of feature detectors by highlighting their respective strengths and weaknesses. In next chapter, we discuss implementation of robust minutiae based fingerprint image hashing. The fingerprint minutiae extraction method is combined *individually* with the SIFT-Harris, SIFT-Wavelet and the SIFT method, to generate robust features. The idea is to incorporate the orientation and descriptor in the minutiae of the fingerprint image. Shape context based hashing is used for fingerprint identification.

.

# Chapter 5

# Minutiae Based fingerprint Image Hashing

Due to recent developments in technologies, image data in digital format is used extensively in the world of the internet and ready to be accessed anytime, anywhere. The amount of image data information via digital devices has grown exponentially. Conversely, the digital nature of information allows individuals to manipulate and duplicate data easily without any change in quality. The power of the image manipulation software has made it possible to effortlessly modify digital multimedia data. Under this circumstance, integrity verification has become an important issue in the digital world. In the area of multimedia security, two types of approaches have been proposed to maintain the confidentiality of image data: watermarking and perceptual hashing. Watermarking is the ability to detect changes in the host image data, which can provide some form of guarantee that the image data has not been tampered with and has originated from the right source. Watermarking can be used in copyright verification or in content authentication for digital images. Furthermore, data embedding inevitability causes a slight distortion in the host image data.

In conjunction with watermarking, perceptual hashing is conventionally used for image content authentication. The main advantage of a perceptual hashing scheme is that the image data is not altered and not degraded visually. Perceptual image hashing is different from cryptographic hashing in that cryptographic hashes are extremely sensitive to single-bit changes of input data that will change the output dramatically.

Recently, perceptual image hashing has received considerable attention from many researchers. Most countermeasures proposed in the literature, generally focus on feature extraction to acquire robust feature to authenticate the image. In this research, we introduced a robust minutiae based fingerprint image hashing by combining state of the art feature points with the minutiae of fingerprint images, which are discussed in the following section 5.5.

## 5.1 Design criteria for image hashing

There are three important design criteria for an image hash function: robustness, fragility and unpredictability. Let $I$ denote the reference image (e.g., all natural images of a particular size). Likewise, $I'$ denote test image (an image visually identical or perceptually distinct). Assuming hash function $H(.)$, the system produces two hash values $h = H(I)$ and $h' = H(I')$ by using a key $K$.

$$\begin{cases} h = H(I;K) \\ h' = H(I';K) \end{cases} \tag{5.1}$$

The following requirements are considered:

*(i) Perceptual robustness:*

$$(H(I,K) \approx H(I',K)), \text{then } dist(h, h') < Th \tag{5.2}$$

*(ii) Distinct visually:*

$$(H(I,K) \neq H(I',K)), \text{then } dist(h, h') \geq Th \tag{5.3}$$

*(iii) Unpredictability of the hash:*

$$H(I);\ fh(1) = fh(0) = 0.5 \tag{5.4}$$

Where,

$fh(x)$ is the probability mass function for $h$.

In effect, *(i)* ensures the capability of the visually similar images distance between two hashes $h$ and $h'$ should be less than a threshold $Th$. Conversely, *(ii)* has the capability to differentiate between two images, which are visually distinct. The first requirement suggests that the distance between two hashes $h$ and $h'$ should be larger than a threshold $Th$. *(iii)* guarantee the unpredictability of the hash values, in addition to the key $K$ functions (pseudo-random number generator) used at final stages of the hash function.

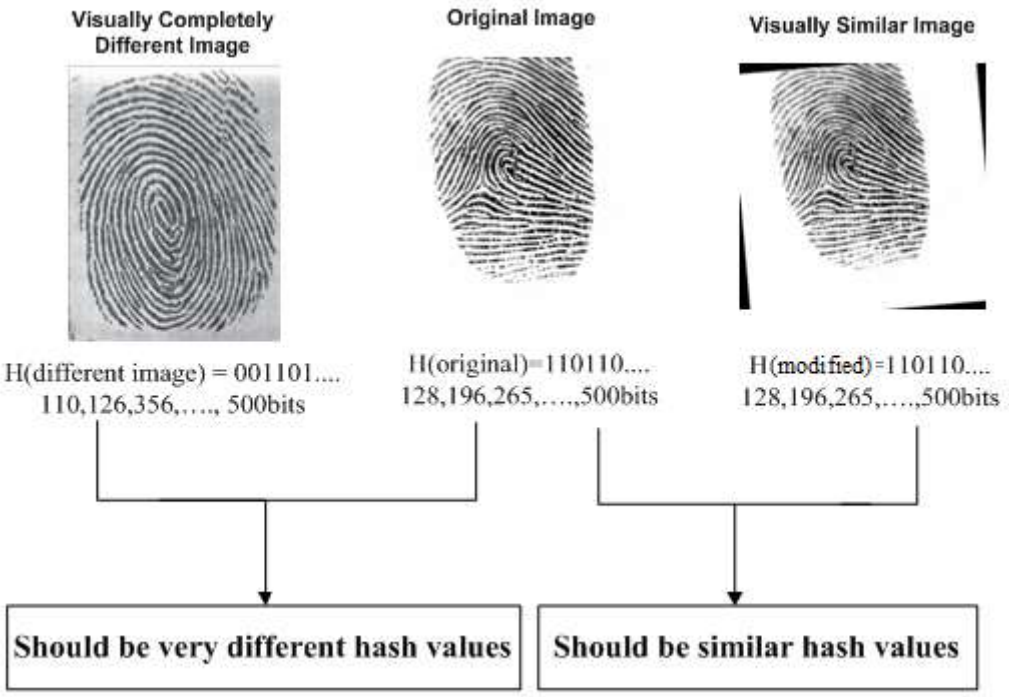



Figure 5.1: Design requirements for fingerprint image hashing

## 5.2 Perceptual Image Hashing Schemes

Perceptual image hashing has been introduced to generate a robust, unique, compact and secure feature and moreover, its hash values of the image. Based on the characteristics of images, the extracted features are unique and distinctive for content identification. The image hashes are perceptually similar to the content preserving operations as long as two images are similar to the Human Visual System (HVS). Similarly, a very different hash value for a perceptually different image is shown in Figure 5.1. Hence, feature extraction is a key step in the image hashing technique. The image hashing schemes are categorised into four types: Statistic-based schemes, Relation-based schemes, Coarse-representation-based schemes and Low-level feature-based schemes.

- ***Statistic-based schemes*** [43], [46], [47], [92]: This group of schemes extracts image features by calculating the image statistics in the spatial domain, such as the mean, variance, higher moments of image blocks and histogram.

- ***Relation-based schemes*** [90], [94]: This category involves approaches to extract image features by making use of some invariant relationships of the coefficients of the discrete cosine transform (DCT) or wavelet transform (DWT).

- ***Coarse-representation-based schemes*** [41], [48], [95]: In this category, the perceptual hash is calculated by making use of coarse information with regards to the whole image, for instance the spatial distribution of significant wavelet coefficients, the low-frequency coefficients of Fourier transform, and so on.

- ***Low level feature-based schemes***[14], [96]: The image features are extracted by detecting the salient image feature points. These methods first perform the DCT or DWT transform on the original image, and subsequently, makes use of the coefficients to generate a final hash value. However, the perceptual hash value is very sensitive to global as well as local distortions that do not cause perceptually significant image changes.

### 5.2.1 Perceptual Image Hashing Framework

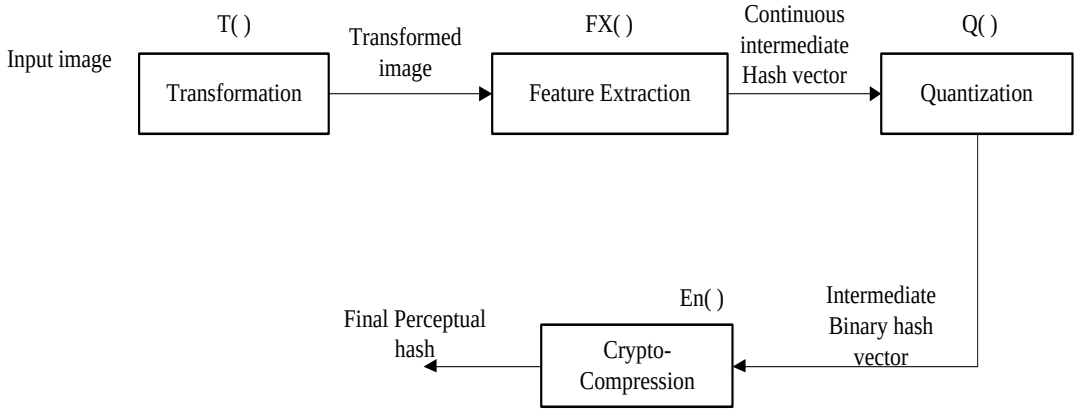



Figure 5.2: Pipeline stages for the perceptual hashing system

A perceptual hashing system consists of four pipeline stages: transform stage, feature extraction stage, quantization stage, and compression and crypto-compression stage, as illustrated in Figure 5.2. In the transformation stage, the input image undergoes special and /or frequency transformation to make all the extracted features depend on the image pixels or image frequency coefficients. In the feature extraction stage, the perceptual image hashing system extracts the image feature from the input image to generate the continuous hash vector. They, the continuous perceptual hash vector are quantized into the discrete hash vector in the quantization stage. In the third stage the discrete hash vector is converted into a binary perceptual hash string. Finally, the binary perceptual hash string is compressed and encrypted into a short and final perceptual hash in the crypto-compression stage.

## 5.3 Content-Based Image Identification

The concept behind image authentication is to extract the image characteristics (features) of the human perception for the authentication process. Typically, some applications will be performed by considering intentional (image processing, such as filtering, compression, cropping, resizing etc) and non–intentional (noise, channel errors) distortion to the images. The context-preserving manipulations only change the pixel values, which results in different levels of visual distortion in the image, but the contexts of the image, which carries the same visual message to the observer, are preserved. In contrast, malicious/content-changing manipulations consist of changing the content of the original image to a new one, which transmits a different visual message to the observer. One typical example of malicious modification is replacing some parts of the image with different contents. Perceptual hashes are expected to be able to survive acceptable content-preserving manipulations and reject malicious manipulations. Classification of content-preserving and content-changing manipulations is provided in Table 5.1.

Table 5.1: Content-Preserving and Content-Changing Manipulation

| Content –Preserving Manipulation | Content –Changing Manipulation |
|---|---|
| • Transmission errors<br>• Noise<br>• Compression and quantization<br>• Resolution reduction<br>• Scaling<br>• Rotation<br>• Cropping<br>• $\gamma$ Distortion<br>• Colour conversions<br>• Contract adjustment, changes of brightness, hue and saturation | • Removal of image objects<br>• Moving of image elements or changing their positions<br>• Adding new objects<br>• Changes of image characteristics: colour, textures.<br>• Changes to the image background: day time or location<br>• Changes of light conditions: shadow manipulation etc. |

## 5.4 Proposed Feature Extraction Techniques

The state of the art feature extraction techniques and the properties of feature detector are briefly discussed in chapter 4.

This research focuses on improving the security of fingerprint templates and accurate comparison of the fingerprint content. The generation of fingerprint templates, which in turn are used to compare fingerprint content (or their perceptual hashes) mostly rely on feature extraction techniques, such as SIFT, SIFT-Harris or Fingerprint Minutiae. However, a combination of the two (e.g., SIFT-Minutiae) has not been previously studied in the literature.

Firstly, the SIFT-Harris method is combined with the Fingerprint Minutiae extraction technique to determine the most prominent fingerprint features. These features are post-processed into perceptual hashes using shape content based perceptual hashing to plot the accuracy of fingerprint comparison using Receiver Operating Characteristic (ROC) curves.

Secondly, the SIFT-Wavelet is combined with the Fingerprint Minutiae extraction technique to determine the most prominent fingerprint features. These features are also post-processed using shape content based perceptual hashing techniques to plot the accuracy of fingerprint comparison using ROC curves.

Thirdly, the SIFT is combined with the Fingerprint Minutiae extraction method and post-processed using shape content based procedures to plot the accuracy.

### 5.4.1 SIFT-Harris-Minutiae Feature for Fingerprint Image Hashing

To design robust fingerprint hashing against various distortions, robust feature extraction is the most important step. We propose a method for extracting the robust minutiae of the fingerprint images, by combining the SIFT-Harris feature points with the minutiae of the fingerprint image, as demonstrated in Figure 5.3. Based on the position, scale and orientation of each keypoint in the SIFT-Harris, the corresponding descriptor with 128 dimensions based on the gradient histogram within its 16x16 local neighborhood is generated. Alongside the SIFT-Harris feature points ($SH_{FP}$), minutiae ($M_P$) are extracted with four tuple, such as $M_P=\{x,y,\theta,t\}$, where, (x,y) is the coordinate, $\theta$ is angle, and t is the type of minutiae (termination or bifurcation) respectively.

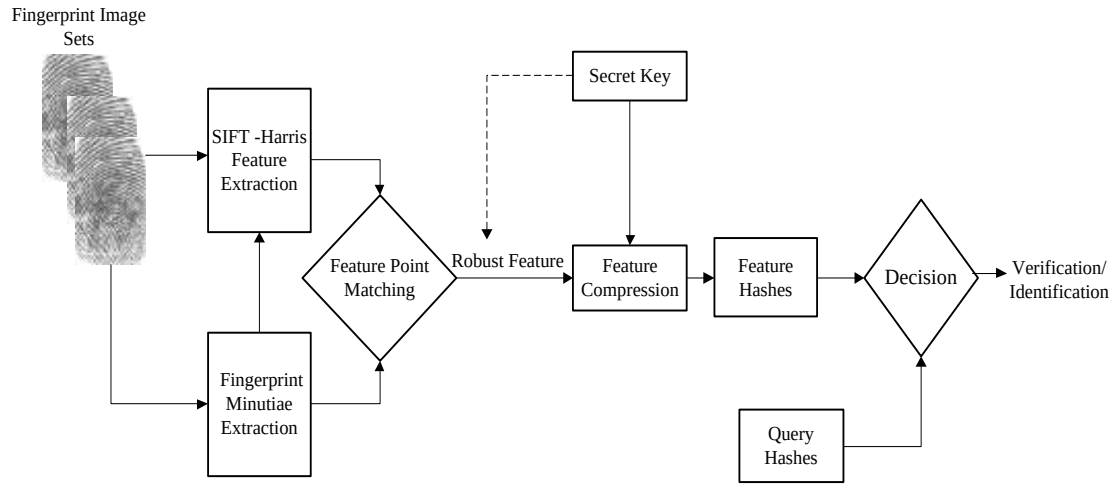



Figure 5.3: Proposed Robust SIFT-Harris- Minutiae based Fingerprint Image Hashing

The absolute radial distance between the position of the SIFT-Harris feature and the coordinates of the minutiae are computed. Most robust minutiae are detected if the relative difference of pixel values is within the threshold of ten pixel value [5]. Along with the detected point the corresponding orientation and descriptor are also identified. Hence, the proposed robust minutiae are represented by coordinates, orientation and descriptor respectively. This robust minutia of the fingerprint image is to be hashed, and the fingerprint identification is to be performed using hashed robust minutiae. Consequently, the detailed hashing technique is explained in section 5.5.

The robustness of the image hashing arises from robust feature extraction and the compression, which mainly contributes to the compactness of the final hash. To increase the security of a traditional hash function and prevent unauthorized access, a secret key is incorporated in either the feature extraction, compression or both to make the hashes unpredictable.

Most of the hashing algorithms incorporate a pseudorandomization relying on a secret key. Such a key is incorporated into the compression step [15] to further enhance the security, as indicated by the dashed line in Figure 5.3. The key is owned by the owner, and the hash generation is a pseudorandom process rather than a completely random one for fingerprint identification. The incoming query hash corresponding to the query image is compared with the hashes in the database.

### 5.4.2 SIFT-Wavelet -Minutiae Feature for Fingerprint Image Hashing

Recently, the wavelet based salient points detector and a combination of wavelet-SIFT features has been successfully used in several image recognition systems. Lin et al [97] presented an efficient salient-region extraction algorithm based on the significance of accumulated wavelet coefficients. This algorithm is robust for image processing operations like compression, filtering and geometric distortions. Lim [98], Sebe et al [99] explained the comparative analysis of scale-invariant feature extraction using different wavelet bases and highlight the advantages, whereas Loupias et al [100] recommended a salient point detector based on wavelet transform to detect global and local variations. In addition, Omidyeganeh et al [101]

introduced a robust face recognition system based on wavelet transform of the Scale Invariant Feature Transform (SIFT) features, and moreover, these combinations provide important performance efficiency in face recognition systems.

Recently, Kumar et al [102] suggested a new technique for robust colour image matching based on the combination of wavelet-colour SIFT features. Moreover, Wang et al [103] presented a parameter adjusted Gaussian Mixture Models using a salient feature patched to recognise an object in Caltech image database. These methods combine an effective combination of wavelet-based features and SIFT features. Thus, the extracted features are suitable for properties that are invariant to translation, scaling, rotation and illumination changes.

Halawani et al [104] evaluated and compared the non-linear kernel function around salient points with Monte-Carlo[105] function for the purpose of invariant content based image retrieval. Jian et al [106] proposed a wavelet based salient point detector to extract the visually meaningful region in an image and an annular segmentation algorithm based on salient region distribution is designed. Furthermore, Imamoglu et al., [107] introduced a novel saliency detection model by utilizing low-level features obtained from the wavelet transform domain.

Salient point detection in images is very useful for image processing application like image compression, object detection and object recognition. Tsai et al [108] suggested a hierarchical selection algorithm for selecting the most salient point to satisfy the representation of an image and to make an effective image retrieval system.

Though SIFT algorithms locate the salient points in a given image which are scale invariant there is a need to improve the robustness of those points. The most appropriate method for doing this is to prune the locations obtained by the SIFT to retain the most robust points, which remain unchanged for different types of attacks. Consequently, it is demonstrated [16] that the corner points in the SIFT locations are highly robust and retain the stable points.

*A)* **Wavelet Transform**

Wavelet [109] plays a significant role in many image processing applications. The computation of the wavelet transform of a 2-D image involves recursive filtering and sub-sampling. This operation results in four decomposed subband images referred to as low-low (LL, produces a approximation of the image), low-high (LH, containing horizontal information at a high frequency), high-low (HL, containing vertical information at a high frequency), and high-high (HH, containing diagonal information at a high frequency). Moreover, the wavelet transform can recursively decompose the LL band. The two level wavelet decomposition results, LH1, HL1, HH1, LH2, HL2, HH2 and an additional approximation image LL2 are revealed in Figure 5.4. In this particular research, we use the Haar wavelet [110], which is a simple orthogonal, compactly supported wavelet, which leads to a complete and non-redundant representation of the image.

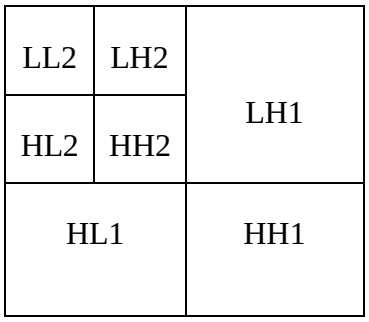



Figure 5.4: Second Level Wavelet Transform

***B) Proposed SIFT-Wavelet -Minutiae***

In our work we intend to use a wavelet image analysis tool to determine the robust points in the SIFT. This is completed by the motivation that four categories of coefficients; approximation coefficients, horizontal, vertical and diagonal coefficients can be utilized to localize the salient points. This method can be combined with the SIFT to select the robust points from the SIFT coefficients.

To explain the proposed method of selecting robust points from the SIFT output, let us consider that the selected images are decomposed by the L levels and represent

the coefficients obtained for every level, as $a_k$, $h_k$, $v_k$, $d_k$. Moreover, the relationship between the coefficients at every level can be illustrated as in Figure 5.5.

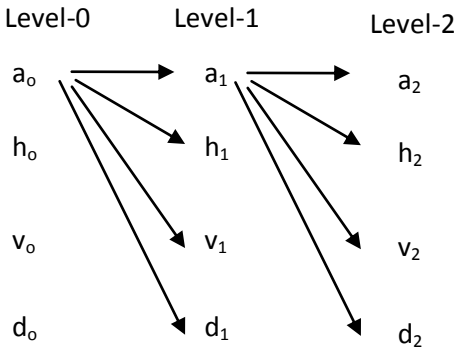



Figure 5.5: Image Decompose Level

It can be perceived that if the input image is of dimension N x N then at level 0 each of the coefficients will be of dimension N/2 x N/2. Furthermore, the computation 2 x 2 pixel group of the image contributes for a pixel in the set $\{a_k, h_k, v_k, d_k\}_{k=0}$. Based on image decomposition (Figure 5.5) it can be observed that when we compute the next level coefficients the results are contributed by a 4x4 pixel group of the image. When the decomposition is done progressively it can be shown that at $k_{th}$ level the contribution for a pixel of coefficients would be from a b x b pixel group from the input image, whereas $b=2^{(k+1)}$.

We propose to use the coefficient value obtained at a location at the $k_{th}$ level to determine the characteristics of the b x b pixel group of the original input image. If all the three coefficients $h_k$, $v_k$, $d_k$ are high at $k_{th}$ level in a given location then we assume that the corresponding b x b pixel group of original image is salient. The simple logic we applied is that a SIFT point in a salient bxb matrix of the original image will be considered salient and retained. The high energy in horizontal, vertical and diagonal directions imply that the point is a corner point and will be robust to attacks.

The SIFT-Wavelet is combined with the Fingerprint Minutiae extraction technique to determine the most prominent fingerprint features, as shown in Figure 5.6. The algorithm is similar to the SIFT-Harris-Minutiae as discussed in section 5.4.1.

The proposed robust minutiae are represented by coordinates, orientation and descriptor, respectively. The robust minutiae of the fingerprint image are also post-processed using shape content based perceptual hashing techniques to plot the accuracy of fingerprint comparison using ROC curves, as explained in section 5.6.

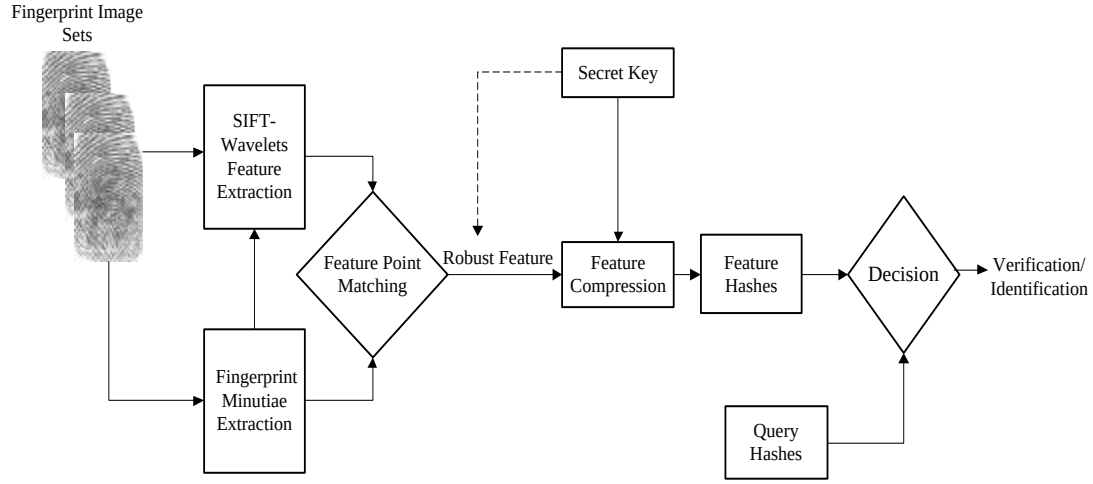



Figure 5.6: Proposed Robust SIFT-Wavelet- Minutiae Fingerprint Image Hashing

### 5.4.3 SIFT-Minutiae Feature for Fingerprint Image Hashing

Together with the SIFT-Harris-Minutiae and the SIFT-Wavelet-Minutiae, the performance of the SIFT-Minutiae combination was demonstrated. Without any thresholding to the SIFT keypoints the minutiae of the fingerprint image was combined to extract the most robust minutiae from the fingerprint images. The position, scale, orientation and descriptor of each keypoint in the SIFT and minutiae coordinate, angle and type are computed. The absolute radial distance between the positioned SIFT points and the coordinates of the minutiae are calculated. Based on the relative difference of the pixel the most robust minutiae are detected along with the orientation and descriptor. In addition, the SIFT-Minutiae combination is represented by the coordinates, orientation and descriptor respectively. This robust minutia from the fingerprint image is post-processed using shape content based procedures to plot the accuracy, as described in section 5.5.

## 5.5 Image Hashing Based On Shape Contexts

Roy et al [111] presented a technique to encode the geometric relationship between the SIFT points into a short vector, but the robustness is limited to attacks like rotation, cropping and compression. In [112], [113] the authors use the SIFT local feature points to detect image copies or near-duplicate copies by matching the high-dimensional local feature descriptors of keypoints. However, this is not possible in image hashing, where, the robust features are compressed into compact hash and match the hashes during the detection stage.

Lv et al [16] recommend using the shape contexts, which is a promising method to measure shape similarity for object recognition, so as to generate image hashes based on the robust local feature points that have been detected. The distribution of local feature points is composed of the content structure of images and considers this geometric structure as an abtract object. Furthermore, the use of a descriptor represents this structure as an unique signature. In the following sections, the basic concept of shape contexts and shape contexts based image hashings are described in detail.

### 5.5.1 Shape Contexts

Given a set of points P=$\{p_i\}_{i=1}^{N}$, which are sampled from the contour of an object, the shape context of point $p_i$ with respect to the reference point $p_c$ is defined in [114] as:

$$h_i(k) = \#\{p_i \neq p_c : (p_i - p_c) \in bin(k)\} \quad (5.5)$$

where $p_i \in P$ and $bin(k)$ are uniform in log-polar coordinates as shown in Figure 5.7 with the centre located at $p_c$. The shape context of each point is a coarse histogram, which represents the relative positions of other points to the reference point. It has been identified that this descriptor is highly robust to shape deformation and offers a globally discriminative characterization, which is effective in solving shape matching and transforming model estimation problems.

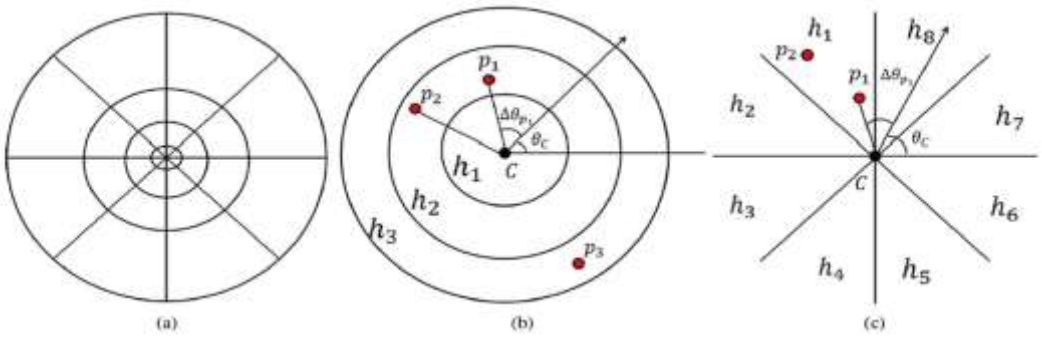



Figure 5.7: Diagram of the original shape contexts and the proposed shape contexts hashing: RSCH.ASCH. (a) Original Shape Contexts. (b) Radial Shape Contexts hashing (c) Angular shape Contexts hashing [16].

## 5.5.2 Shape Context Based Hashing

In our proposed approach, shape context based hashing [16] is used for fingerprint authentication and provides an excellent description of the geometric structure of a shape. We can embed the geometric distribution of robust feature points, as well as their descriptors into shape contexts to generate a compact image hash. The original shape context was designed to be computed for each point sampled from the object contours, which means that for N local feature points we have N shape contexts. In addition, it provides a rich descriptor to represent the shapes, although it has to be compressed to be used for hashing directly.

It can be observed in the image content authentication that all perceptually insignificant distortions and malicious manipulations on the image content would not lead to viewpoint changes. In addition, the centre of an image is generally preserved and relatively stable under certain geometric attacks. This encourages Lv et al [16] to generate shape contexts with the reference point in the centre and obtain a compact signature for the image. Another reason for avoiding computing shape context for each local feature point in the hashing is that the detection of keypoints cannot guarantee to yield exactly the same feature points when the image is under different attacks and manipulations. As a trade-off, Radial Shape Context Hashing (RSCH) and Angular Shape Context Hashing (ASCH) are used to generate hashes using shape contexts with respect to the central reference point.

Given a set of robust feature points $P = \{p_i(x, y)\}_{i=1}^{N}$and their corresponding descriptors $D = d_{pi}(\mathrm{x,y})\}_{i=1}^{N}$, the basic steps of RSCH and ASCH are as follows :

## A. Radial Shape Context Hashing (RSCH)

a. Given the coordinates of the central point $C$ = ($x_c$,$y_c$) and the required length of the hash L, construct bins $B = \{b(k)\}_{k=1}^{N}$of shape contexts with incremental $l$ =max ($x_c$,$y_c$)/L in the radial direction of the polar coordinates.

$$b(k) = \{p_i \in P: (k-1)l \leq \|p_i - C\| \leq kl\} \tag{5.6}$$

Where $\|p_i - C\|$is the relative distance between pi and the central point $C$.

b. Generate pseudorandom weights $\{\propto_k\}_{k=1}^{L}$ from the normal distribution N ($u, \sigma^2$) using a secret key. Each $\propto_k$ is a random vector with 128 dimensions to be consistent with the dimensions of the SIFT descriptors.

c. Let $H = \{h_k\}_{k=1}^{L}$ be the hash vector and thus, we have each component $h_k$ as

$$h_k = \sum_{p_i \in b(k)} w_{\left\lfloor \frac{L\Delta\theta_{pi}}{2\pi} \right\rfloor} \langle \propto_k, d_{pi} \rangle \tag{5.7}$$

Where $\Delta\theta_{pi}$= $(\theta_{pi} - \theta_c) \in (0,2\pi)$ is the relative difference in orientations between $p_i$ and the central point$C$. The weight w $[L\Delta\theta_{pi} / 2\pi] \in W = \{w_i\}_{i=1}^{L}$, is the set of random weights generated from uniform distribution U(0.5,1). This is to differentiate between the points located at different orientations of the same hash bin $b(k)$ along the radial direction.

## B. Angular Shape Context Hashing (ASCH)

a. Given the coordinates of the central point $C$=($x_c$,$y_c$) and the required length of the hash L, construct bins $B = \{b(k)\}_{k=1}^{N}$ of shape contexts with incremental $l = 2\pi/\mathrm{L}$ in the angular direction of the polar coordinates .

$$b(k) = \{p_i \in P: (k-1)l \leq (\theta_{pi} - \theta_c) \leq kl\} \tag{5.8}$$

Where $(\theta_{pi} - \theta_c) = \Delta\theta_{pi} \in (0,2\pi)$.

b. Generate pseudorandom weights $\{\propto_k\}_{k=1}^{L}$ from the normal distribution N($u, \sigma^2$) using a secret key. Each $\propto_k$ is a random vector with 128 dimensions to be consistent with the dimension of the SIFT descriptors.

c. Let $H = \{h_k\}_{k=1}^{L}$ be the hash vector, we have each component $h_k$ as

$$h_k = \sum_{p_i \in b(k)} w_{\left[\frac{L\|p_i - C\|}{\|C\|}\right]} \langle \propto_k, d_{pi} \rangle \tag{5.9}$$

Where $\|p_i - C\|$ is the same as referred to in section 5.5.2A and $\|C\| = \sqrt{x_c^2 + y_c^2}$ is the normalization factor. The weight $w_{[L\|P_i - C\|/\|C\|]} \in W = \{w_i\}_{i=1}^{L}$ is the set of random weights generated from the uniform distribution U(0.5,1). This is to differentiate between the points located at different orientations on the same hash bin $b(k)$ along the angular direction.

***Estimation of Central Orientation*** $\theta_{\mathrm{C}}$*:* The central orientation $\theta_{\mathrm{C}}$ is significantly important for both the ASCH and RSCH and moreover, is required as a reference direction to calculate the relative difference in orientation between the local feature point $p_i$ and the central point $C$. However, estimating based on local gradient distribution is not reliable due to different image processing attacks. Alternatively, Radon transform is used to estimate an accurate reference orientation for central point $C$.

Radon transform is the integral transform consisting of the integral of a function over straight lines. Given a 2-D function $f\ (x, y)$ and line $p$ with orientation $\theta$ as shown in figure5.8

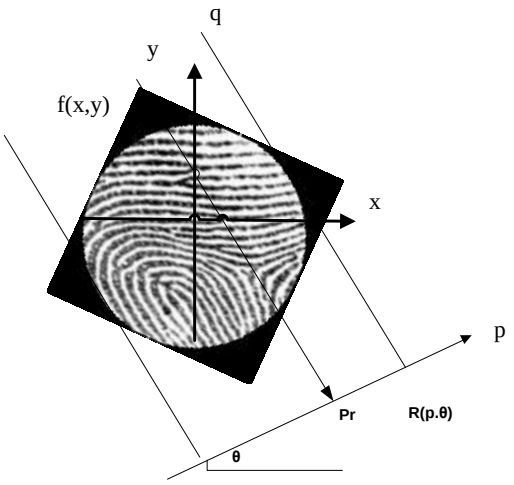



Figure 5.8 Radon transform $R(\mathrm{p},\theta)$ of a 2-D function $f\ (x,y)$

The Radon transform of $f\ (x,y)$ is the integral of the orthogonal projection to line $p$.

$$R_f\ (p,\theta)=\int_{-\infty}^{\infty} f(x,y)dq \tag{5.10}$$

Where $q$ is the orthogonal axis of line $p$.

$$x = pcos\theta - qsin\theta \tag{5.11}$$

$$y = psin\theta + qcos\theta \tag{5.12}$$

Based on Radon transform [16][17], the estimation of the reference orientation for the central point $C$ is as follows:

Step1) Select the circular neighborhood where the radius = 64 and denotes this region as a 2-D function $f\ (x,y)$. Subsequently, compute the radon transform of $f\ (x,y)$ from 0 to$2\pi$ and get $R_f\ (\mathrm{p},\theta)$, where $\theta \in (0,2\pi)$.

Step2) Choose a reference point $p_r$ on the $p$ axis neighborhood $\Omega \in \ [p_r - t, p_r + t]$ as shown in figure5.8.

The reference orientation $\theta_C$ are estimated by

$$\theta_C = \arg\max_{\theta} \sum_{p=p_r-t}^{p_r+t} R_f\,(p,\theta), \theta \in (0,2\pi)$$

(5.13)

Here $\theta_C$ is not the extract orientation of the central point $C$. However, it provides us with a reference orientation, which could be used to calculate the relative difference in orientations between $C$ and other keypoints.

## 5.6 Experimental Results

In this work, a Euclidean distance metric and Receiver Operating Characteristics (ROC) are chosen to distinguish the robustness and discriminability of the perceptual hashing scheme. These are:

***a) Euclidean Distance***

Let $S = \{s_i\}_{i=1}^{N}$ be the set of original images in the database. The corresponding hashes space $H(S) = \{H(s_i)\}_{i=1}^{N}$ where $H(s_i) = \{h_1(s_i), h_2(s_i), \ldots\ldots\ldots h_3(s_i)\}$ is the hash vector with length n for image $s_i$. Hence, we use Euclidean distance $D((h_1),(h_2))$ to measure the similarity between two hash vectors $H(s_1)$ and $H(s_2)$. Subsequently, given a query image Q, we generate its hash H(Q) and calculate its distance to each original image in the hash space H(S). The distance between two hashes is defined as the square root of the sum of the squares of the differences between the corresponding hash values. i.e., the distance between two hashes $h_1\ and\ h_2$ is given by

$$dist\big((h_1),(h_2)\big) = \sqrt{\sum_{i=1}\big(h_{1_i} - h_{2_i}\big)^2}$$

(5.14)

***b)Receiver Operating Characteristics (ROC)***

The ROC curve is used to evaluate the identification performance of the proposed robust minutiae based fingerprint image hashing technique. To plot the ROC curve, the $TPR\ (\tau)$ and $FPR\ (\tau)$ are defined as:

$$TPR\ (\tau) = Probability\ (D(H_k(I)), (H_k(I_d))) < \tau \quad (5.15)$$

$$FPR\ (\tau) = Probability\ (D(H_k(I)), (H_k(I^{'}))) < \tau \quad (5.16)$$

Where, $\tau$ is the identification threshold. The image $I_d$ is a modified version of *I* and $I^{'}$ is a distinct image of the original image *I*. ROC curves were generated by varying the threshold $\tau$ from the minimum to the maximum value of all the distances. TPR against FPR were plotted in ROC curves which suggest that the best possible performance should correspond to point in the top left corner (coordinate 0, 1) of the ROC space.

Table 5.2: Different Attacks used to assess the hashing performance

| **Attack** | **Parameters** |
|---|---|
| **Image Processing Operations**<br>JPEG lossy compression<br>Median filtering<br>Gaussian Blur | Quality Factor =10<br>Window size 3x3<br>Variance $\sigma = 0.5$, Window size 3x3 |
| **Geometric Distortion**<br>Rotation<br>Translation | Degree $5^0$<br>Variance $\sigma = 0.5$, Window size 5x5 |

***c) Result and Analysis***

The proposed technique was evaluated using 100 images in the FVC 2002/DB1_A database (Figure 5.9) [115] and we evaluated the perceptual robustness of the image hashing techniques, RSCH and ASCH against the known attacks, as mentioned in Table 5.2. The selected length of the hash vector for the RSCH and ASCH is L=20 [14]. The proposed robust feature extraction of fingerprint images, such as SIFT-Harris-Minutiae, SIFT-Wavelet-Minutiae and SIFT-Minutiae were compared to the

SIFT technique, as shown in Figure 5.10- 5.13(a-e). The results are discussed as follow:

Figure 5.9 Fingerprint images from FVC2002/DB1_A database.

***SIFT-Harris-Minutiae***: The advantage of generating hashes on robust feature points lie in the robustness against geometric transform, especially the rotation attacks. The location to extract robust feature are determined by detected keypoint, the corresponding hashes are invariant to rotation transform. The proposed fingerprint image hashing based on SIFT-Harris-Minutiae approaches can achieve better performance for JPEG lossy compression (QF=10%) and translation ( $\sigma = 0.5$, 5x5 window) attacks and exhibits good robustness against different attacks especially for median filtering (3x3 window), Gaussian blur ( $\sigma = 0.5$, 3x3 window) and a rotation (5 degrees) as shown in Figure 5.10. It can be seen that the shape contexts provide an outstanding description of the geometric structure of a shape and allows embedding the geometric distribution of robust minutiae feature points as well as their descriptors into a short hash vector. The result also demonstrates that ASCH relatively outperforms the RSCH. This leads that the distribution of feature points in the angular direction is better discriminated than in the radial direction [16].

***SIFT-Wavelet-Minutiae:*** Fingerprint image hashing based on an effective combination of wavelet based feature and SIFT feature along minutiae, to determine most prominent features for fingerprint image. The experimental result shows that

fingerprint image hashing based on SIFT-Wavelet minutiae are provides improved robustness for the median filtering (3x3 window) and Gaussian blur ( $\sigma = 0.5$, 3x3 window) and a rotation (5 degrees). However, through RSCH, its hash shown high sensitive to the JPEG lossy compression (QF=10%) and translation attacks ( $\sigma = 0.5$, 5x5 window) as shown in Figure 5.11. This is because of RSCH has less capacity in distribution of feature points in radial direction.

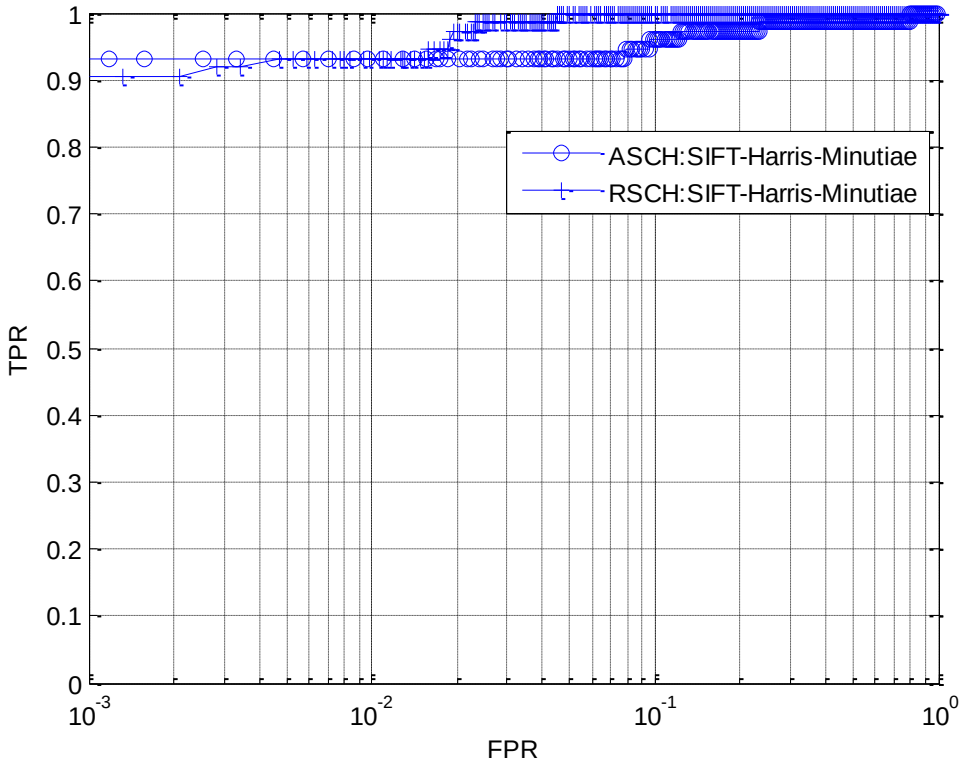
***SIFT-Minutiae:*** The SIFT combined with minutiae based hashing technique performs moderately well for median filtering (3x3 window), Gaussian blur ( $\sigma = 0.5$, 3x3 window), although it is highly susceptible to the JPEG lossy compression (QF=10%), rotation (5 degrees) and translation attacks ( $\sigma = 0.5$, 5x5 window) (Figure 5.12).

***SIFT:*** For the sake of comparison the SIFT was compared with the proposed technique. The performance is slightly affected by the median filtering (3x3 window), and highly sensitive to JPEG lossy compression (QF=10%), Gaussian blur ( $\sigma = 0.5$, 3x3 window), rotation (5 degrees) and translation attacks ( $\sigma = 0.5$, 5x5 window) (Figure 5.13). Alongside, To justify the research contribution of combined methods, experiment was performed on SIFT -Harris and SIFT-wavelet approach. The performances of these two approaches are highly competitive and resulted in Table 5.2.

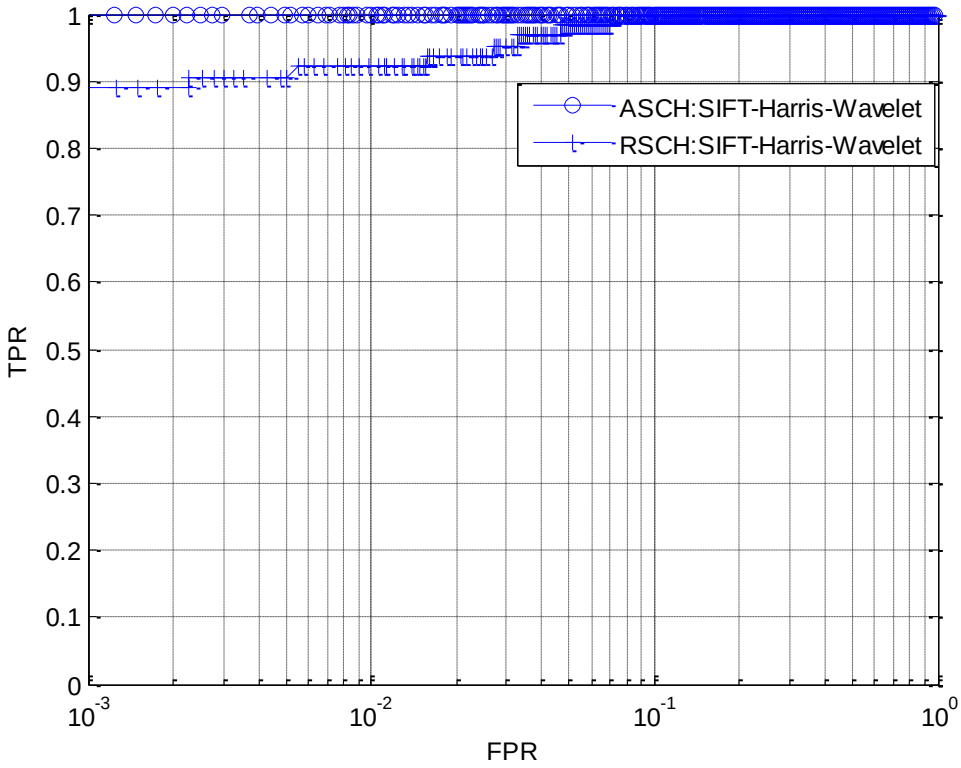
The advantage of generating hashes based on the robust minutiae of fingerprint image lies in the robustness against geometric distortions like rotations and translations. Furthermore, the hashing techniques ASCH and RSCH perform better for identification accuracy. Also, we have observed that Angular shape context hashing relatively outperforms Radial shape context hashing (Table 5.2), which indicates that the distribution of feature points in the angular direction is better discriminative capacity than the distribution in the radial direction. However, image hashing using feature points still has limitations on considering the distortions of additive noise and blurring large scale.

Table 5.3: Summary of proposed fingerprint image hashing technique

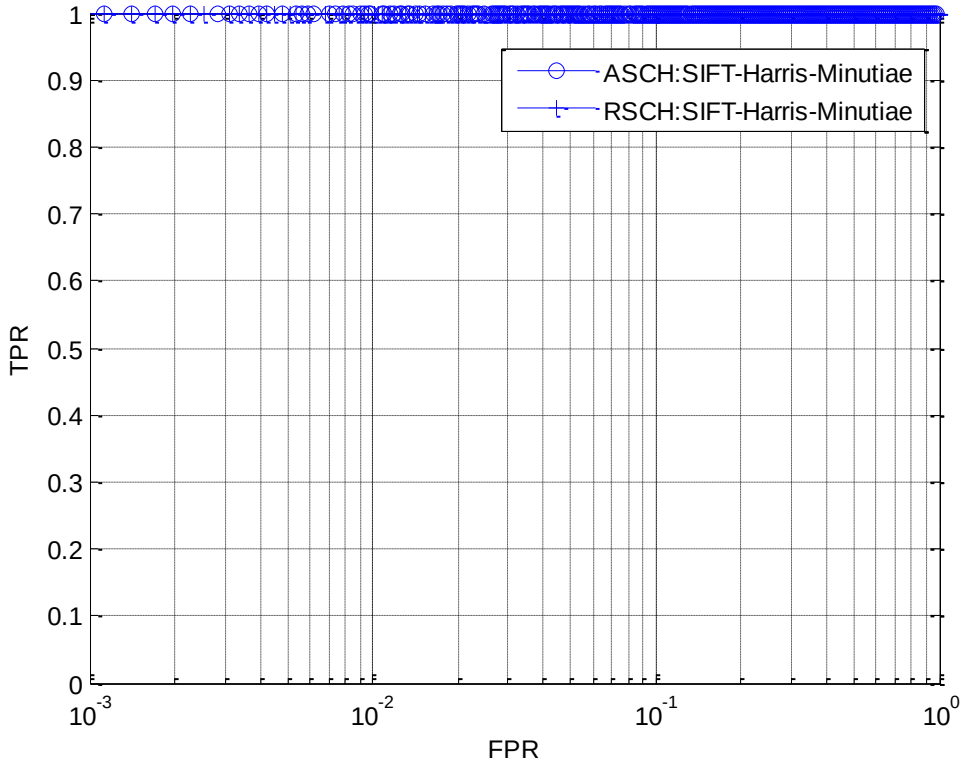
| Performance Evaluation of Fingerprint Image Hashing Technique | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Attacks | SIFT- Harris - Minutiae | | SIFT- Wavelet- Minutiae | | SIFT- Minutiae | | SIFT | | SIFT- Harris[16] | | SIFT- Wavelet | |
| | ASCH | RSCH | ASCH | RSCH | ASCH | RSCH | ASCH | RSCH | ASCH | RSCH | ASCH | RSCH |
| JPEG lossy Compression QF=10% | Good | Good | Good | Low | Good | Low | Moderate | Low | Good | Moderate | Moderate | Low |
| Median filtering 3x3 | Better | Good | Better | Moderate | Better | Moderate | Moderate | Low | Good | Good | Good | Moderate |
| Gaussian Blur $\sigma$=0.5, 3x3 | Better | Better | Better | Better | Moderate | Moderate | Moderate | Low | Better | Moderate | Good | Good |
| Rotation $5^0$ | Better | Good | Good | Moderate | Moderate | Low | Low | Low | Good | Good | Moderate | Moderate |
| Translation $\sigma$=0.5, 5x5 | Good | Good | Good | Low | Low | Low | Low | Low | Good | Moderate | Good | Low |



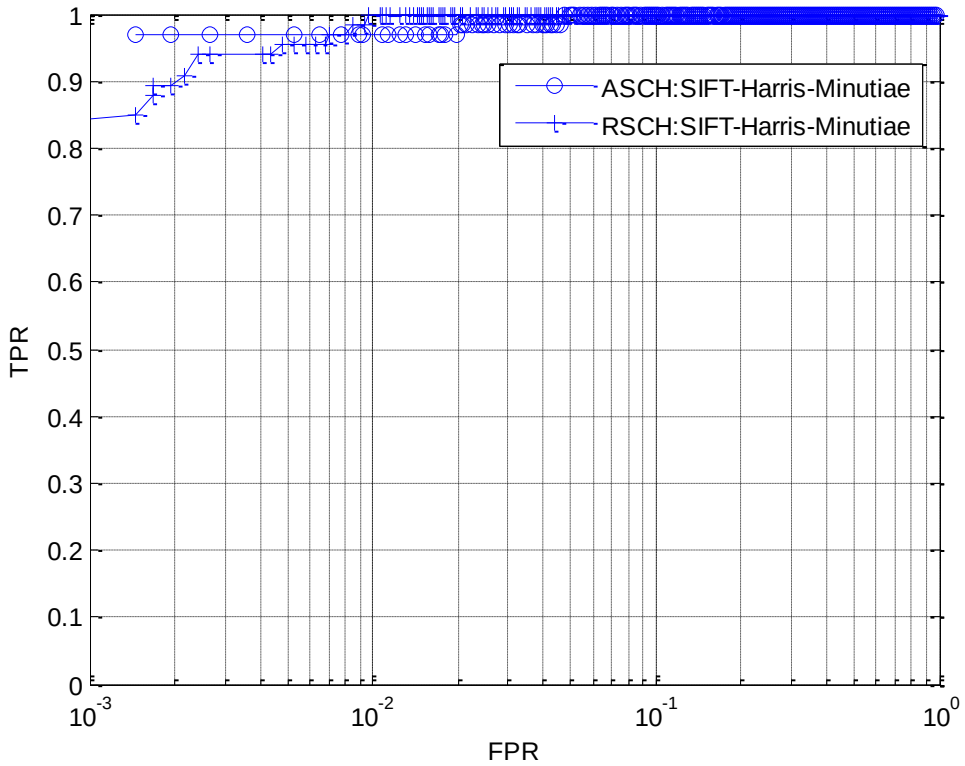

(a) ROC curves under JPEG lossy compression



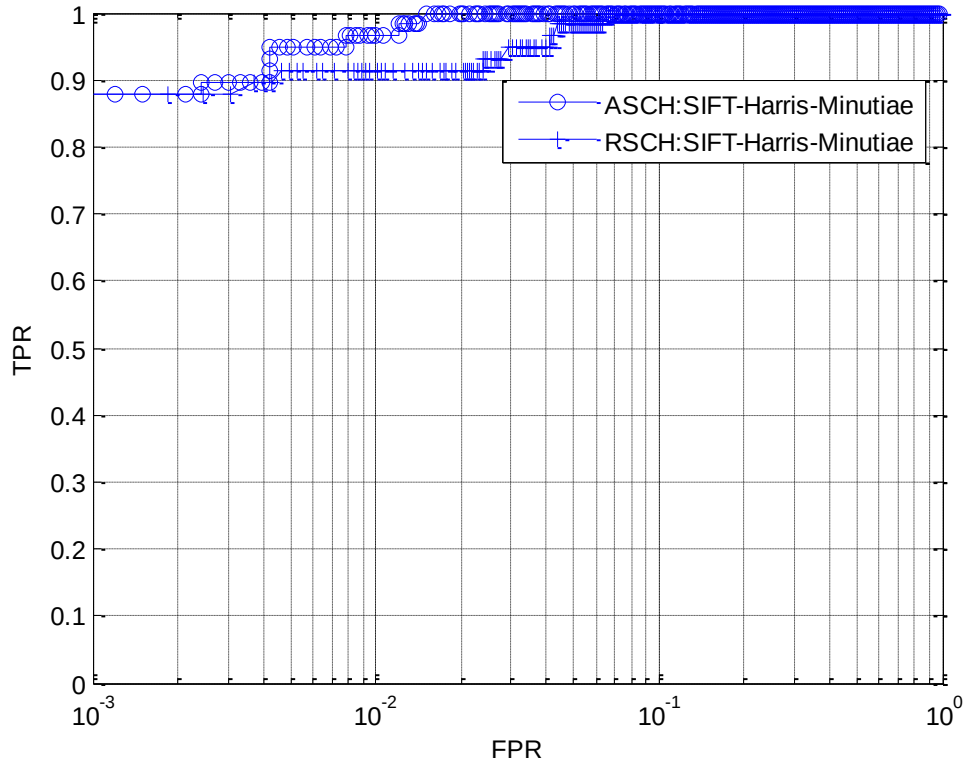

(b) ROC curves under median filter




(c) ROC curves under Gaussian blur

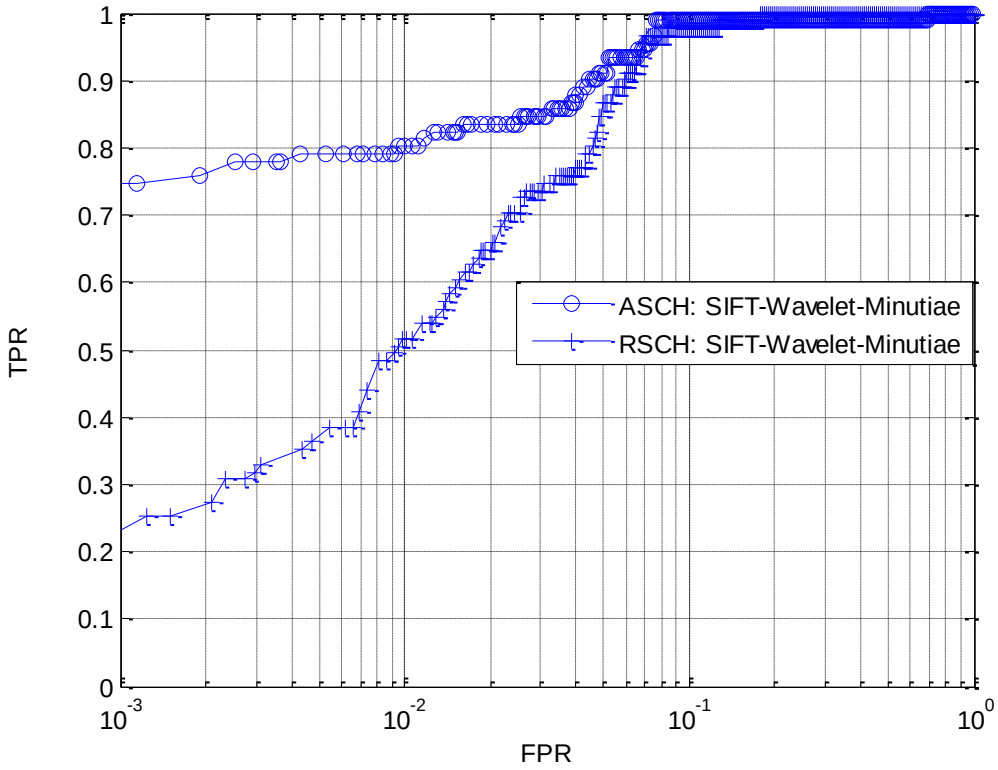



(d) ROC curves under rotation

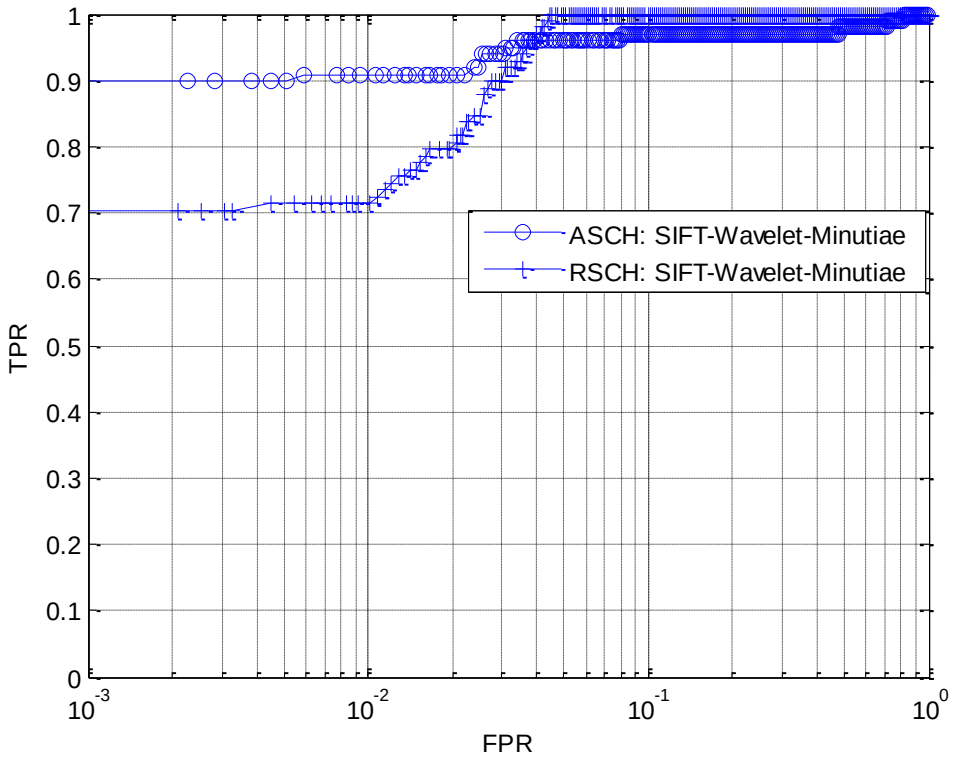



(e) ROC curves under translation

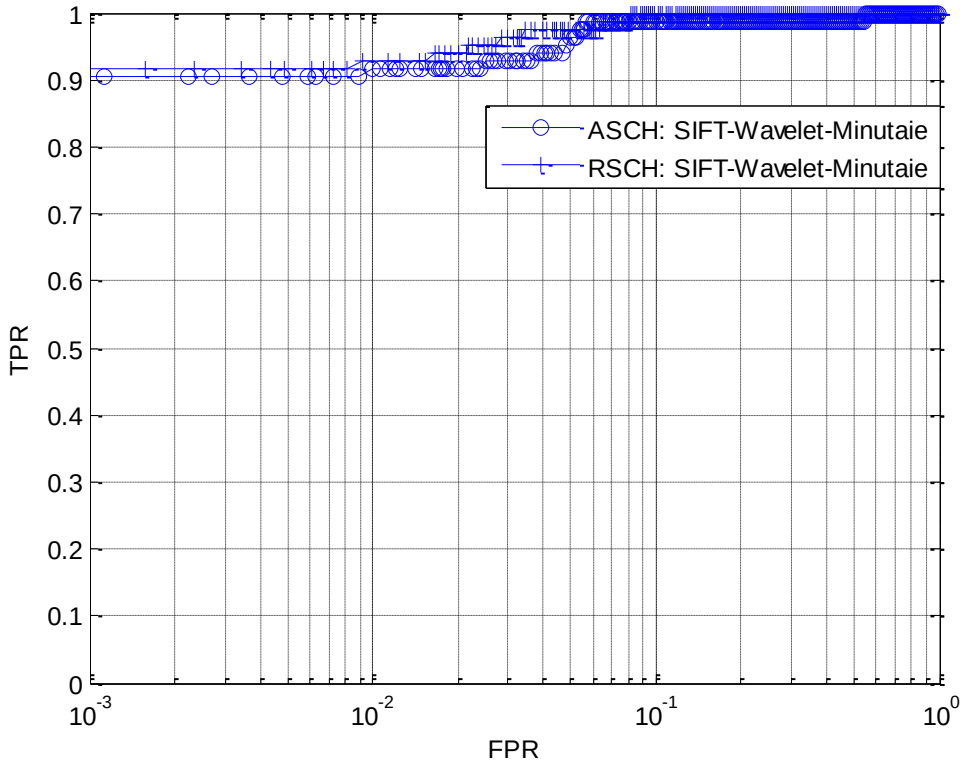
Figure 5.10: ROC curves for the proposed robust minutiae of the fingerprint image (SIFT-Harris-Minutiae) using the shape context based image hashing technique, (a) ROC curves under JPEG lossy compression (b) ROC curves under median filter (c) ROC curves under Gaussian blur (d) ROC curves under rotation (e) ROC curves under translation



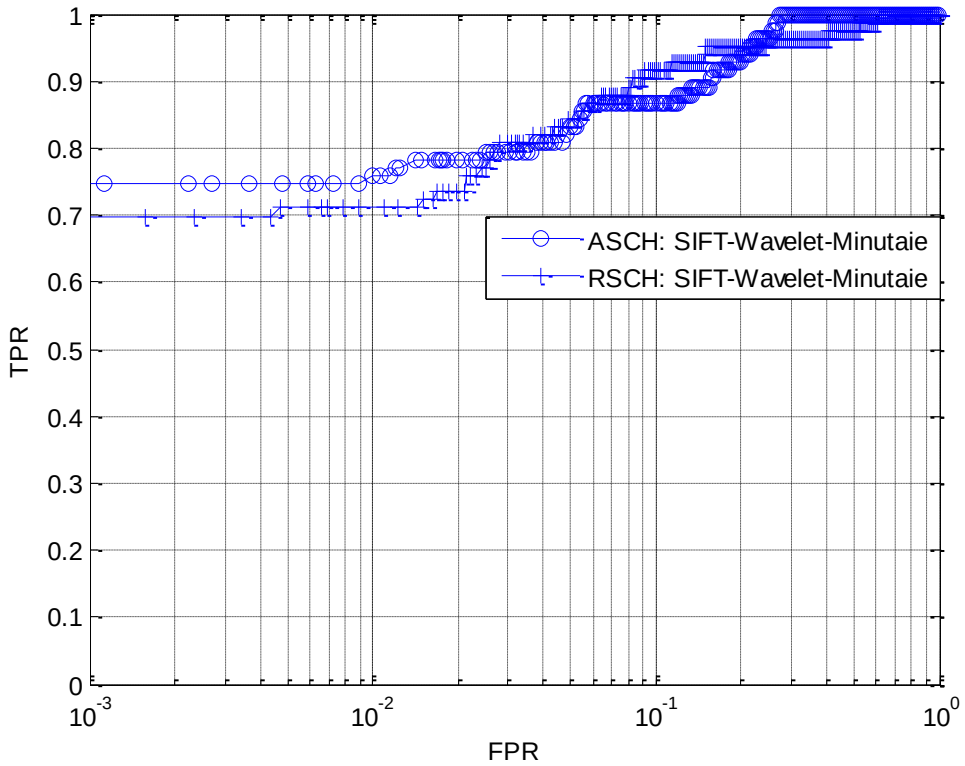

(a) ROC curves under JPEG lossy compression



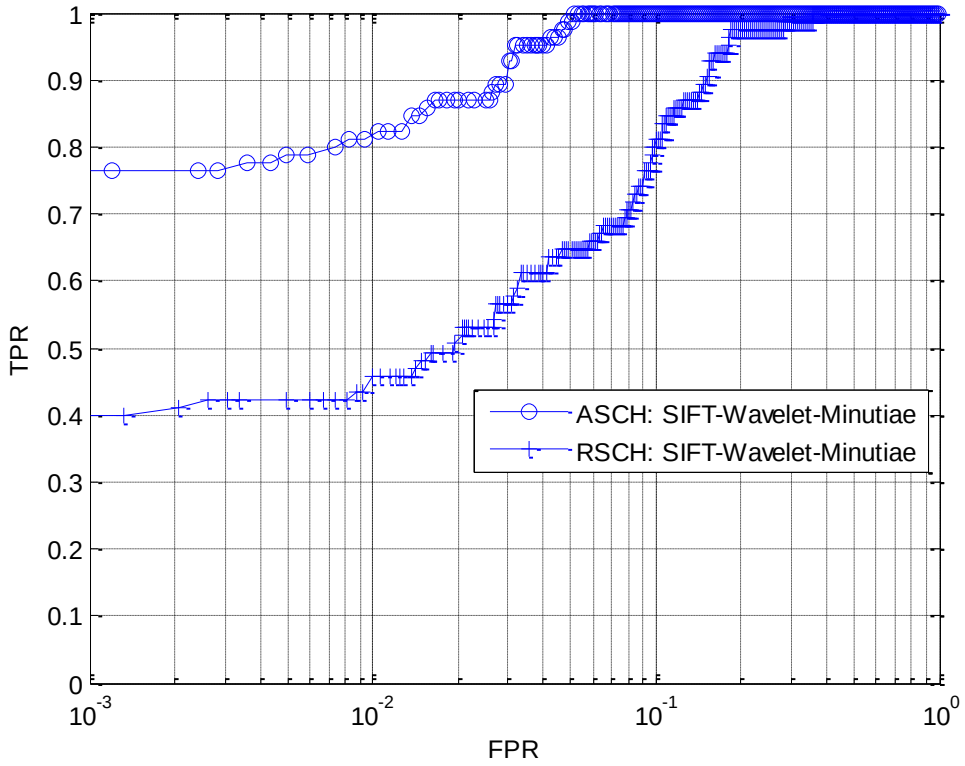

(b) ROC curves under median filter




(c) ROC curves under Gaussian blur

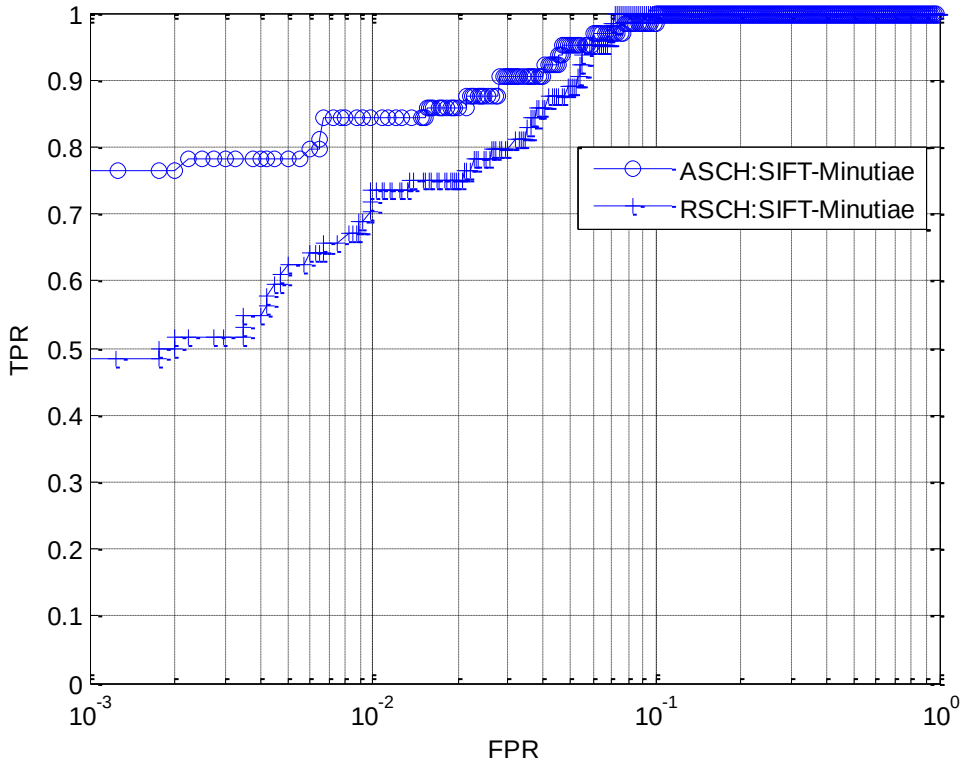



(d) ROC curves under rotation

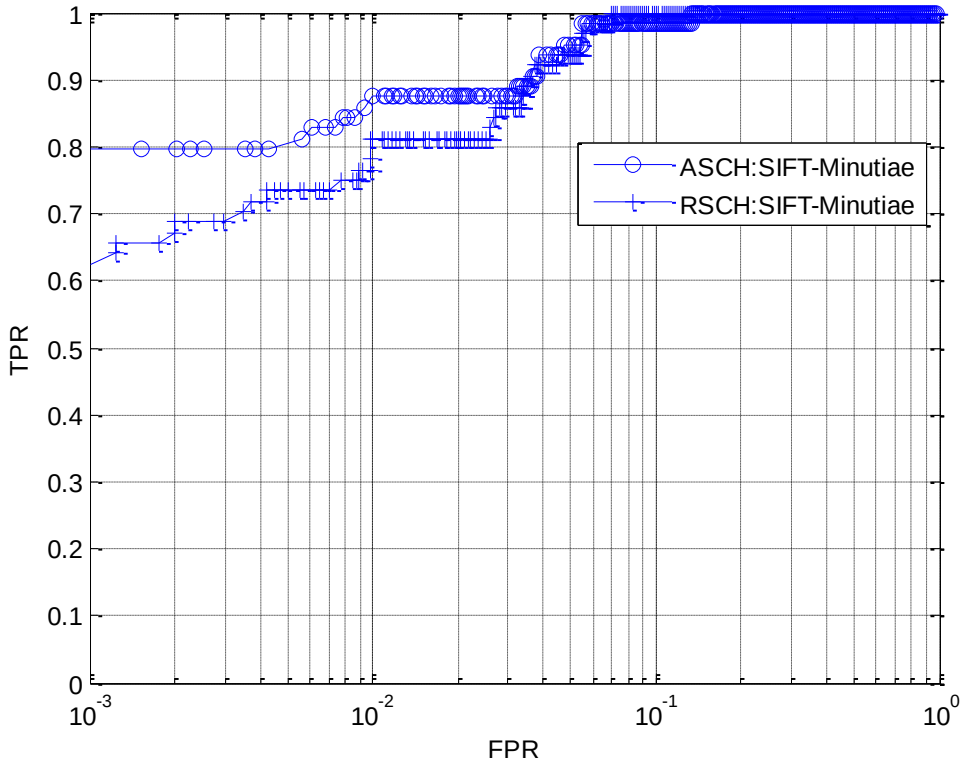



(e) ROC curves under translation

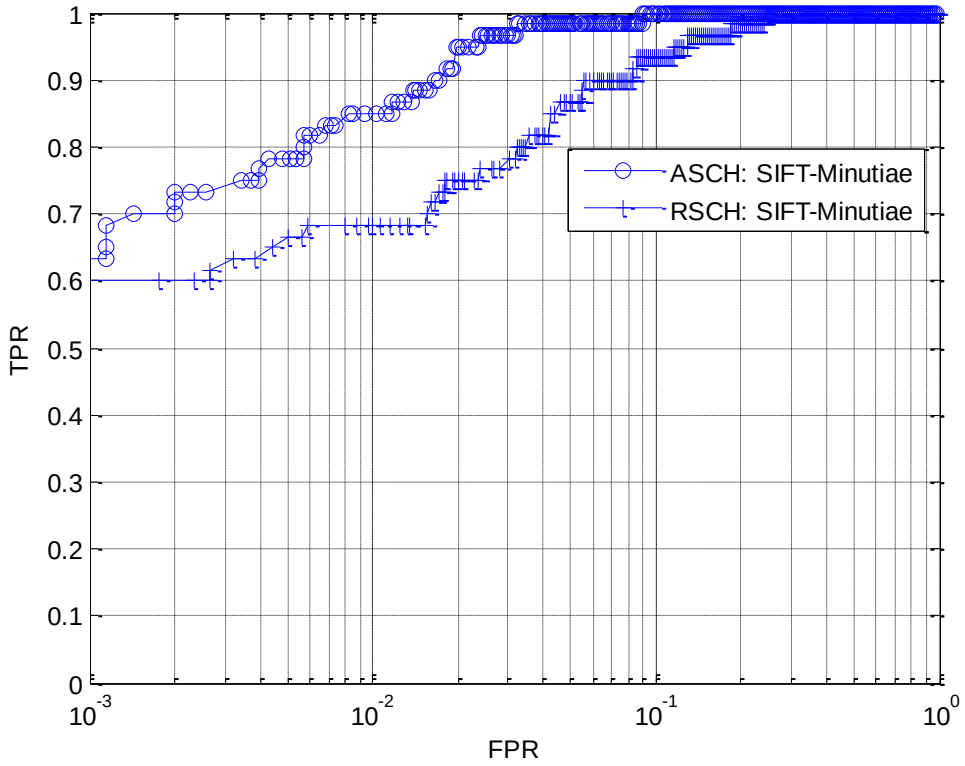
Figure 5.11: ROC curves for the proposed robust minutiae of the fingerprint image (SIFT-Wavelet-Minutiae), using the shape context based image hashing technique, (a) ROC curves under JPEG lossy compression (b) ROC curves under median filter (c) ROC curves under Gaussian blur (d) ROC curves under rotation (e) ROC curves under translation



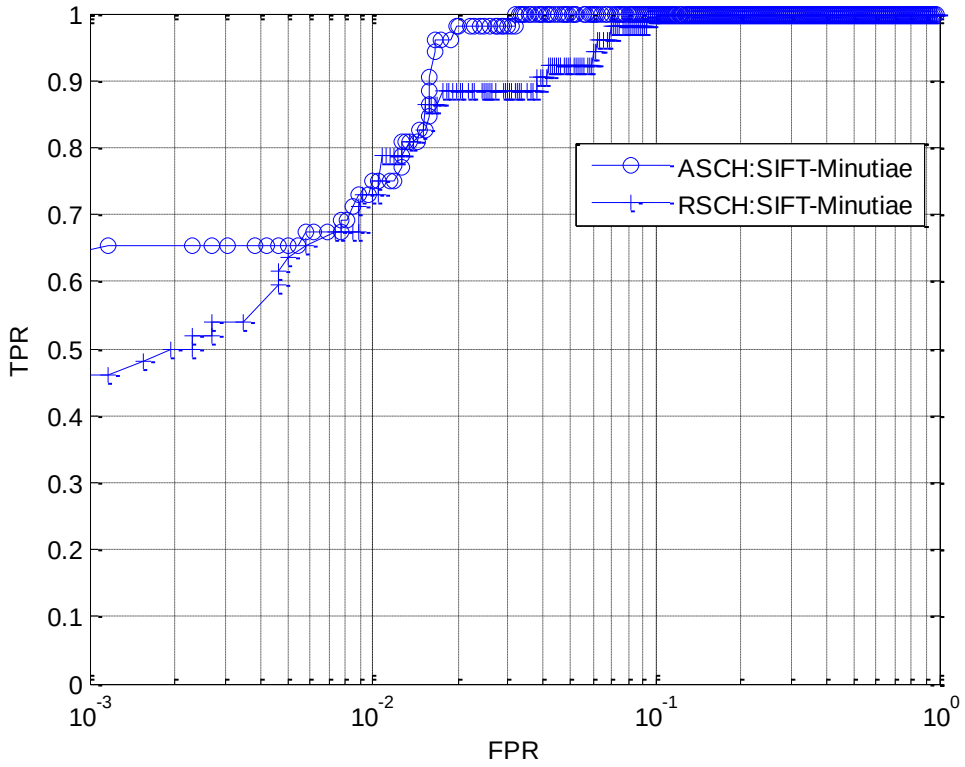

(a) ROC curves under JPEG lossy compression



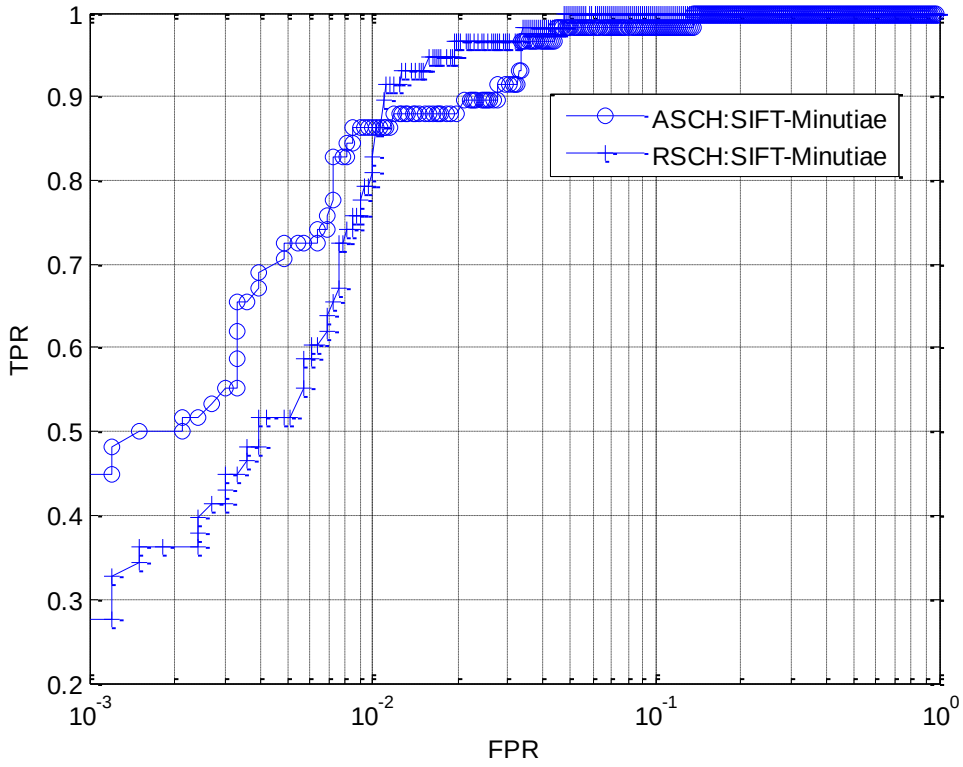

(b) ROC curves under median filter




(c) ROC curves under Gaussian blur

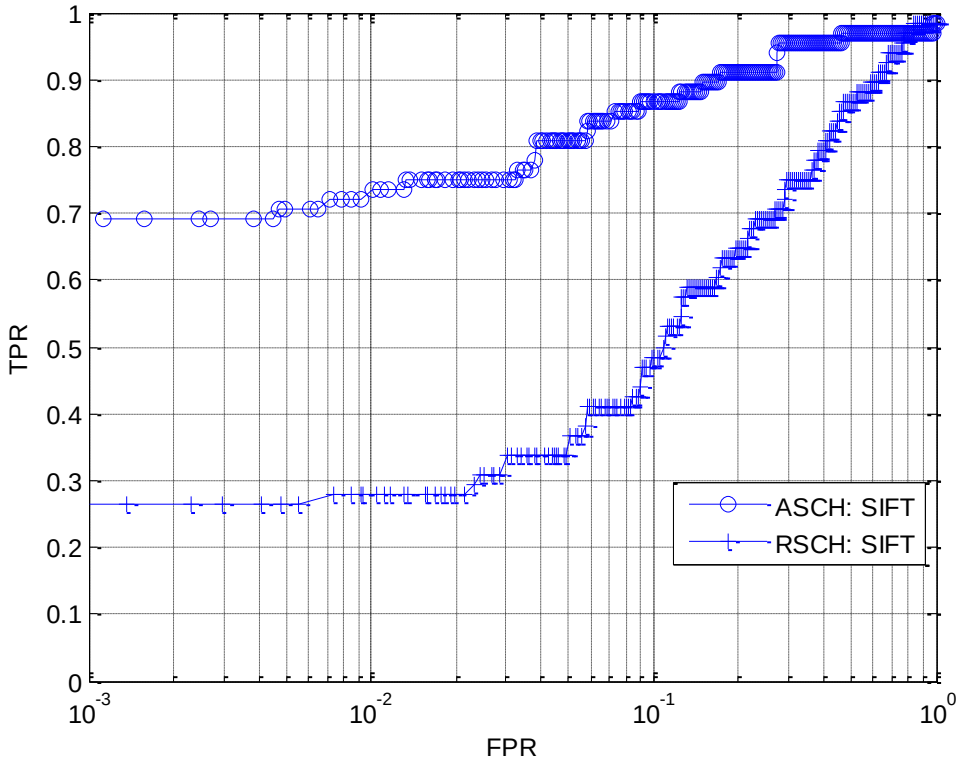



(d) ROC curves under rotation

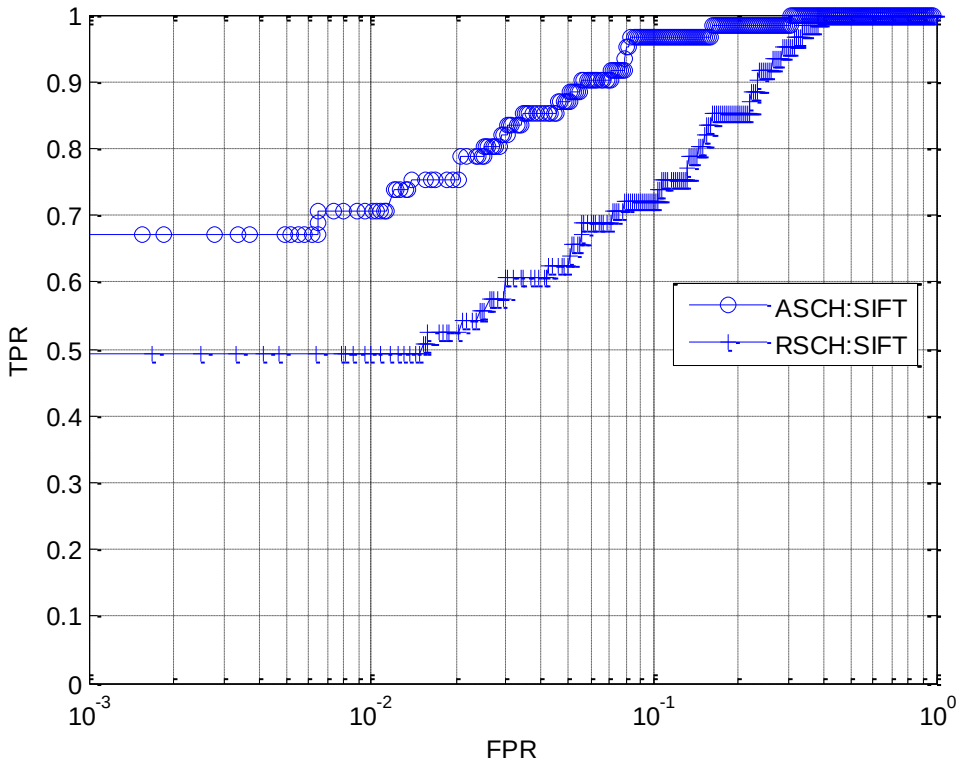



(e) ROC curves under translation

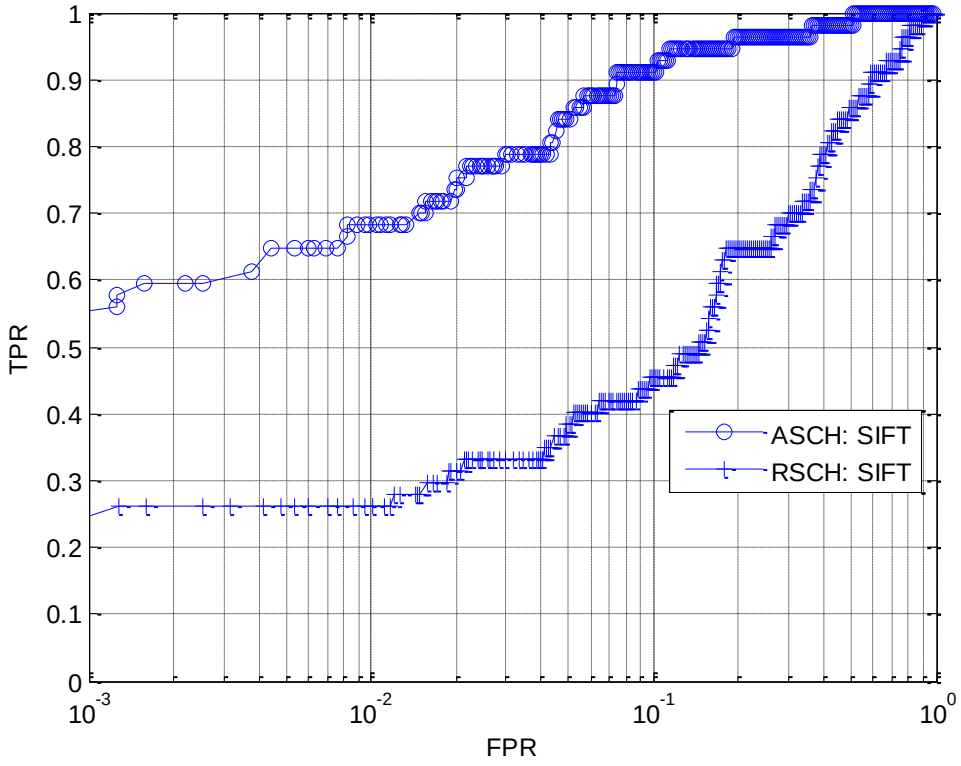
Figure 5.12: ROC curves for the proposed robust minutiae of the fingerprint image (SIFT-Minutiae) using the shape context based image hashing technique, (a) ROC curves under JPEG lossy compression (b) ROC curves under median filter (c) ROC curves under Gaussian blur (d) ROC curves under rotation (e) ROC curves under translation.



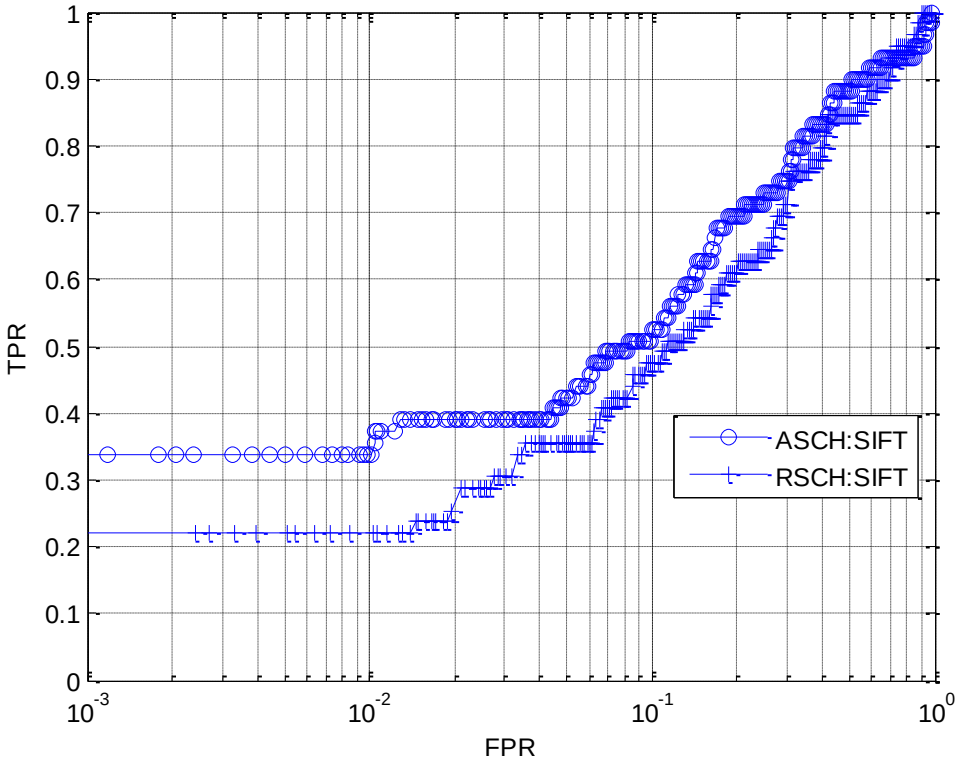

(a) ROC curves under JPEG lossy compression



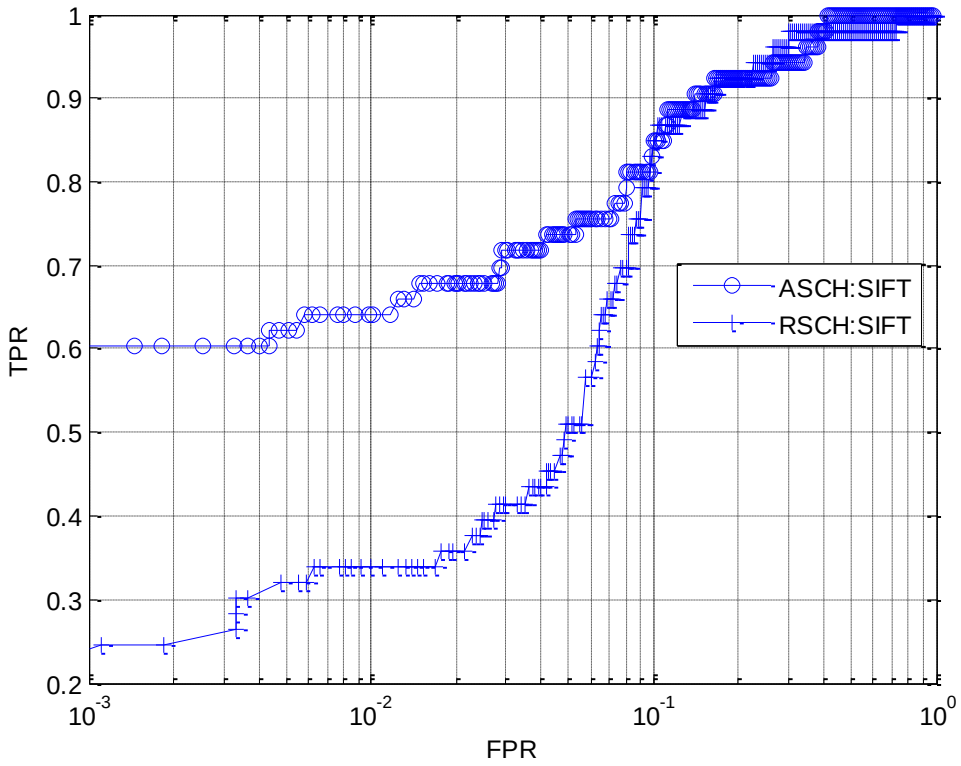

(b) ROC curves under median filter




(c) ROC curves under Gaussian blur




(d) ROC curves under rotation




(e) ROC curves under translation

Figure 5.13: ROC curves for the proposed robust minutiae of the fingerprint image(SIFT) using the shape context based image hashing technique, (a) ROC curves under JPEG lossy compression (b) ROC curves under median filter (c) ROC curves under Gaussian blur (d) ROC curves under rotation (e) ROC curves under translation.

## 5.7 Summary

In this chapter, we have developed robust minutiae based fingerprint image hashing. Based on the geometric invariance of SIFT-Harris keypoints, we combined the minutiae of the fingerprint with the SIFT-Harris feature to detect robust minutiae. Furthermore, we incorporated the orientation and descriptor in the minutiae of fingerprint image and fingerprint identification is performed using hashed robust minutiae. It can be noted that shape contexts provide an outstanding description of the geometric structure of a shape. Thus, we can embed the geometric distribution of robust minutiae feature points as well as their descriptors into a short hash vector. Therefore, SIFT-Harris-Minutiae are more suitable for generating a template and for comparison of the fingerprint content. In next chapter, the perceptual hashing technique to improve the minutiae extraction of the fingerprint image is presented.

# Chapter 6

# Perceptual Hashing For Efficient Fingerprint-Based Identification

In the fingerprint recognition system, the protection of feature points as well as their authentic usage is an important issue. Problems in image data protection have emerged due to recent developments in the field of multimedia systems and communication technologies. Therefore, the security of image data has gained much more importance and thus, the researcher has been developing approaches for protecting and authenticating image data.

A prominent solution to protect image data is perceptual hashing. Nevertheless, other methods, for instance steganography, watermarking and cryptography that can provide protection for image data exist, alongside perceptual hashing. Steganography and watermarking both come under data hiding techniques and are used to hide secret information in the original image. However, differences exists between steganography and watermarking i.e., steganography conceals the very existence of secret information.

Therefore, if the existence of secret information is revealed, the steganography fails, whereas, in watermarking the existence of secret information can be known. The goal of watermarking is to make the removal/manipulation of secret information impossible. In contrast, cryptography does not conceal the existence of secret information; rather it encrypts the information in such a way that it appears useless to an imposter unless decrypted with an appropriate key. The advantage and properties of perceptual hashing has been discussed in chapter 5.

In this research, we use perceptual hashing to improve the minutiae extraction of fingerprint images. We particularly focus on securing the hash and improving minutiae extraction, even if the fingerprint image has been distorted. The proposed method extracts the hash after the wavelet transform and singular value decomposition (SVD). Consequently, the extracted hash obtains good imperceptibility and robustness. The recent literature describes the robustness and

imperceptibility of image data. Lei et al [116] presented robust and reversible watermarking schemes that embed and /or extract watermarks blindly using Recursive Dither Modulation (RDM) with a combination of wavelet transform and Singular Value Decomposition (SVD). In addition, Differential Evolution (DE) optimization is used to control the strength of the watermark. This method demonstrates excellent robustness and imperceptibility, in terms of Structural Similarity Index Measure (SSIM) and Peak Signal-to-Noise Ratio (PSNR). Additionally, Aslantas [117] presented a new optimal method of robust image watermarking based on SVD using DE. The DE was employed to optimise the fitness function to achieve maximum robustness and transparency.

Bhatnagar and Raman [118] presented a new semi-blind reference watermarking scheme based on Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) for copyright protection and authenticity. The result demonstrates the semi-blind reference watermarking scheme withstand to various noise operation like average fingering, median filtering, additive Gaussian noise, JPEG compression, cropping, rotation and other blurring operation.

Ghouti et al [119] presented a novel image-adaptive watermarking scheme based on a subband decomposition to balance multiwavelet transform and this scheme use various statistical models for the host image to derive the watermarking (data-hiding) capacity.

Ramakrishnan et al [120] developed a hybrid image watermarking algorithm which satisfies both imperceptibility and robustness requirements. The watermarking scheme use singular values of Wavelet Transformation's HL and LH subbands to embed watermark. The efficiency of the scheme are explained through PSNR, Normalized Cross Correlation (NCC) and gain factor against to signal and image processing operation.

Moreover, Hore and Ziou [121] analysed a theoretical study to compare the PSNR and SSIM. The study reveals that an analytical link exists between them, which work for various kinds of image degradations, such as Gaussian blur, additive white noise, jpeg and jpeg 2000 compression. The authors also explained the sensitivity of PSNR and SSIM to these degradations

Tang et al [122] demonstrated a metric to evaluate the perceptual similarity between an original image and its distorted version. The result discloses that the metric is insensitive to content-preserving processing, for instance JPEG compression, rotation, low-pass filtering, watermarking embedding and other moderate noise, but that it is very sensitive to malicious modification. The metric evaluation is useful in applications, such as image hashing and content-based image retrieval.

Image quality assessment plays an important role in the field of image manipulation. Wang et al [123] summarized the traditional approach to image quality assessment and its limitations. The authors introduced structural similarity as an alternative principle for the design of image quality measures. Al-Najjar et al [124] presented the comparison of image quality assessment between PSNR, HVS, SSIM and universal image quality index (UIQI) metrics.

Additionally, Hofbauer et al [125] described fusion scenario by combining image metrics and hamming distance approaches in iris biometric systems. The incorporation of distinct image metrics in a fusion scenario significantly improves the recognition accuracy of systems. Keimel and Diepold [126] improved the predication accuracy of PSNR by simple temporal pooling and demonstrate the effectiveness of temporal pooling on a set of high –definition television sequences and broadcasting applications, whilst Run et al [127] demonstrated two methods to develop reliability and robustness: the principle components of the watermark are embedded into the host image in discrete cosine transform (DCT) and inserted into the host image in DWT. The particle swarm optimization (PSO) is used for suitable scaling factors, to improve robustness.

In addition, Braeckman et al [128] illustrated a flexible framework algorithm for reduced reference (RR) visual quality assessment, which is based on perceptual hashing and image and video watermarking. The RR quality assessment is based on perceptual hashing and watermarking techniques. Gao et al [129] proposed a reduced-reference image quality assessment framework, by incorporating merits of multiscale geometry analysis, contrast sensitivity function and Weber's law of just-noticeable difference.

Li et al [130] recommended a method of effective combination of the human vision system with regional mutual information (RMI). This method measures the similarity between an original image and its distorted version. The performance comparison shows that the MRMI method performs better than the SSIM and PSNR method.

Weng et al [131] suggested a novel image authentication system by combing perceptual hashing and robust watermarking. In these algorithms, an image is divided into blocks and each block is represented by a compact hash value, which is embedded in the block. The authenticity of the image can be verified by re-computing hash values and comparing them with the ones extracted from the image. Thus, the system tolerates a wide range of attacks and tamper location of the image.

## 6.1 Singular value decomposition (SVD)

The basic concepts of singular value decomposition (SVD) operations are discussed as follows: SVD decomposes a $N$x$N$ real matrix A into a product of 3 matrices:

$$A = USV^T = [u_1, u_2, u_{3\ldots\ldots,} u_n] \begin{bmatrix} \sigma_1 & & \\ & \sigma_2 & \\ & & \sigma_3 \end{bmatrix} [v_1, v_2, v_{3\ldots\ldots,} v_n]^T \quad (6.1)$$

Where s is a $N$x$N$ diagonal matrix $U$ and $V^T$ are $N$x$N$ orthogonal matrices, whose column vectors are $u_i's$ and $v_i's$, respectively. The elements of $S$ are only non-Zero on the diagonal arranged in decreasing order and are called the $SVs$ of A. when the rank of A is r, $S = \text{diag}(\sigma_1, \sigma_2, \ldots\ldots, \sigma_n)$ satisfies$\sigma_1 \geq \sigma_2 \geq \cdots \geq \sigma_r \geq \sigma_{r+1} = \sigma_{r+2} \ldots\ldots \sigma_n = 0$. Let A be a matrix whose elements are pixel values of an image. The image can be written as:

$$A = \sum_{i=0}^{r} \sigma_i \, u_i v_i^T \quad (6.2)$$

### 6.1.1 Properties of SVD

SVD has several attractive properties from the viewpoint of image processing applications. SVD efficiently represents the intrinsic algebraic properties of an image, where singular values specify the brightness of the image and the corresponding pair of singular vectors reflects the geometry of the image. The main properties of SVD operations are as follows:

- *Stability*: Let$A,B \in R^{mxn}$ and their corresponding SVs are $\sigma_1, \sigma_2, \ldots\ldots, \sigma_n$ and $\tau_1, \tau_2, \ldots\ldots, \tau_n$, respectively. Then a relation can be established between them as$|\sigma_i - \tau_i| \leq \|A - B\|_2$. This indicates that the singular value of an image has very good stability.
- *Proportionality*: The singular values of $A(\sigma_1, \sigma_2, \ldots\ldots, \sigma_n)$ and the singular values of $kA(\sigma_{1,}^*\sigma_2^*, \ldots\ldots\ldots\sigma_n^*)$ are related as $|k|(\sigma_1, \sigma_2, \ldots\ldots, \sigma_n)$=$(\sigma_{1,}^*\sigma_2^*, \ldots\ldots\ldots\sigma_n^*)$ which indicates that the proportion invariance of singular value must depend on standardization of singular value.
- *Transpose*: $A$ and its transposed counterpart $A^T$ have the same non-zero singular values.
- *Flip*: $A$ and its flipped versions give the same non-zero singular values.
- *Rotation*: $A$ and its rotated version obtained by rotating $A$ through an arbitrary angle have the same non-zero singular values.
- *Scaling:* Let $A \in R^{mxn}$ has the singular values $\sigma_1, \sigma_2, \ldots\ldots, \sigma_n$ then its scaled counterpart is equal to $A^s$ and has singular values equal to $\sigma_i^*\sqrt{L_r}L_c$, where $L_r$ and $L_c$ are the scaling factors or rows and columns, receptively. If the scaling function affects only rows or columns, $A^s$ has the singular values equal to $\sigma_i^*\sqrt{L_r}$ or $\sqrt{L_c}$ , respectively.
- *Translation*: Both the matrix $A$ and its translated counterpart $A^t$ have the same non-zero singular values.

## 6.2. Proposed hash security for fingerprint images

Figure 6.1 illustrates the block diagram for the proposed hash security technique of the fingerprint image, which is presented in detail below:

Step1: The original fingerprint image ($I^*$) is partitioned into sub-blocks $B^{*k}$, where $k = 1,2, \ldots . N$.

Step 2: Two-level transform is performed to each subblock $B^{**k}$. The approximate coefficients are selected for SVD calculation. The basic operation of SVD and its properties are explained in section 6.1 and 6.1.1 respectively**.**

Step 3: Perform SVD on the low frequency of each block to generate SVs $S^{**k}$.

Step 4: The SVs ($S^{**k}$) is normalised as

$$S_N^{*K} = \| S^{**k} \| \tag{6.3}$$

Let $S_a^{**K}$=floor $S_N^{**K}/\Delta^K$ and the hash is extracted with the following rule

$$E * (i,j) = \begin{cases} 0, mod\ (S_w^{K*}, 2) = 0 \\ 1, mod\ (S_w^{K*}, 2) = 1 \end{cases} \tag{6.4}$$

Where floor (.) is rounding toward the negative infinity and $\Delta^K$ is quantization steps

Step 5: The final hash is obtained from the original fingerprint image.

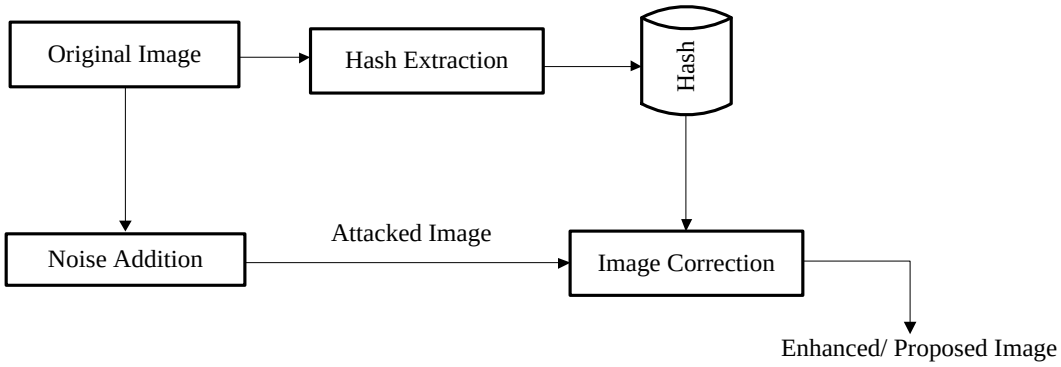



Figure 6.1: Proposed hash securing for fingerprint images

The hash is extracted after wavelet transform and singular value decomposition and stored in the database. As shown in the figure 6.1, when the given image is distorted by noise (Table6.1), the stored hash is used to correct the distorted image. Thus, the corrected image (Enhanced/Proposed Image) is close to the original image in structural similarity. Through this approach, we can retain the maximum minutiae of the fingerprint image, even if the original image is distorted as mentioned in Table 6.1. The performance evaluation of the proposed approach includes important

metrics, such as SSIM and PSNR, which are utilized to represent imperceptibility. Experimentally, the proposed technique demonstrates good quality robustness against image processing operations and geometric attacks. The results are detailed in section 6.4.

## 6.3 Performance Evaluation of Proposed Approach

The proposed approached is evaluated in relation to their robustness and imperceptibility. The SSIM and PSNR are utilized to represent imperceptibility, and BER used to measure robustness. These are explained in the following section.

### 6.3.1 Structural similarity Index Measure (SSIM)

The structural similarity index measure (SSIM) is used to measure quality by capturing the similarity of images [123] based on three comparisons: luminance, contrast and structure, which are selected for the measure of imperceptibility. Three components are combined to yield an overall similarity measure as:

$$\mathrm{SSIM}(X,Y) = l(X,Y)c(X,Y)s(X,Y) \tag{6.5}$$

$$\begin{cases} l(X,Y) = \frac{2\mu_X\mu_Y + C_1}{\mu_X^2 + \mu_Y^2 + C_1} \\ c(X,Y) = \frac{2\sigma_X\sigma_Y + C_2}{\sigma_X^2 + \sigma_Y^2 + C_2} \\ s(X,Y) = \frac{\sigma_{XY} + C_3}{\sigma_X\sigma_Y + C_3} \end{cases} \tag{6.6}$$

The first term in the equation (6.6) is the luminance comparison function, which measures the closeness of the two images mean luminance $\mu_X$ and $\mu_Y$. The second term $c(X,Y)$ is the contrast comparison function, which measures the closeness of the contrast of the two images. Consequently, the contrast is measured by the standard deviation $\sigma_X$ and $\sigma_Y$. The third terms $(X,Y)$ is the structure comparison function, which measures the correlation coefficient between the two images $X$ and $Y$. The covariance between $X$ and $Y$ is represented as $\sigma_{XY}$. The positive value of the SSIM index is in [0, 1]. A value of 0 means no correlation between the images, and 1 means that $X = Y$. The positive constant $C_1, C_2, C_3$ provides stability.

By combining the three comparison functions, the SSIM index is obtained as

$$\mathrm{SSIM}(X,Y) = [l(X,Y)]^{\alpha}.[c(X,Y)]^{\beta}.[s(X,Y)]^{\gamma} \tag{6.7}$$

Where $\alpha > 0$, $\beta > 0$ and $\gamma > 0$ are parameters used to adjust the relative importance of the three components and the parameters are set as $\alpha = \beta = \gamma$ and $C_3 = C_2/2$. From the above parameters, the SSIM index can be defined as:

$$\mathrm{SSIM}(X,Y) = \frac{(2\mu_X\mu_Y + C_1)(2\sigma_{XY} + C_2)}{(\mu_X^2 + \mu_Y^2 + C_1)(\sigma_X^2 + \sigma_Y^2 + C_2)} \tag{6.8}$$

### 6.3.2 Peak Signal-to-Noise Ratio (PSNR)

Given a reference image X and a test image Y, both sizes MxN, the PSNR between, the PSNR between X and Y is defined as:

$$\mathrm{PSNR}(X,Y) = 10\log_{10}\left(255^2/_{MSE(X,Y)}\right) \tag{6.9}$$

Where,

$$MSE(X,Y) = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\left(X_{ij} - Y_{ij}\right)^2 \tag{6.10}$$

The PSNR [114] value approaches infinity as the *MSE* approaches zero; therefore, this shows that a higher PSNR value provides an enhanced quality image. At the other end of the scale, a small value of the PSNR implies a high numerical difference between images.

### 6.3.3 Bit- Error- Rate (BER)

In digital transmission, the number of bit errors is the number of received bits of a data stream over a communication channel that have been altered due to noise, interference, distortion or bit synchronization errors. The bit error rate or bit error ratio (BER) is the number of bit errors divided by the total number of transferred bits

during a studied time interval. The BER is a unitless performance measure, often expressed as a percentage number.

$$\text{BER} = \text{Errors} / \text{Total Number of Bits} \tag{6.11}$$

## 6.4 Experimental Results

The image hashing scheme are applied in the fields of image authentication and retrieval. In general the experiments are tested on 20 standard natural images to show the robustness against usual content preserving operations [132]. The proposed hash security technique is applied on 20 randomly selected images from fingerprint database of FVC2002/DB1_A. The number of blocks has a great effect on the extraction of hash and is used to correct the image. Therefore, the number of blocks should be taken in such a way so as to achieve a superior PSNR and SSIM. In this research, the block size is 8x8. In addition, the performance evaluation of the proposed approach includes important metrics, such as robustness and imperceptibility. Hence, the SSIM and PSNR are utilized to represent imperceptibility, while the BER is used to measure robustness.

The PNSR is easy to evaluate but is not always in accordance with human judgment of quality. On other hand, the SSIM is closer to human visual system. It can be seen that the proposed hash security technique is tested on content-preserving operations (Table 6.1): rotation (1 degree), average filter (3x3 window), Gaussian noise ($\sigma = 0.005$), salt and pepper ($\sigma = 0.01$), JPEG compression of 90%, and Contrast Low (CL) and Contrast High (CH). Table 6.2 gives the average SSIM and PSNR values between the proposed image and distorted image. The wavelet transform- singular value decomposition (DWT-SVD) method is included for comparison.

A drawback of basic SSIM index [133] has sensitivity to relative operation like rotation, JPEG compression, Gaussian noise, salt and pepper noise, blurring, translation and scaling. The proposed hash security technique provides high SSIM values (closer to value of 1) for average filter (3x3 window), JPEG compression (QF=90%), Contrast Low (CL) and slightly sensitive to rotation (1 degree), salt and pepper ($\sigma = 0.01$) and Contrast High (CH), whilst Gaussian noise ($\sigma = 0.005$) has better correlation when compared to DWT-SVD method.

The PSNR improvement for the proposed image are more than 3dB for rotation (1 degree), average filter (3x3 window), Gaussian noise ($\sigma = 0.005$), JPEG compression (QF=90%) and Contrast Low (CL). The PSNR value is less sensitivity for salt and pepper ($\sigma = 0.01$) and Contrast High (CH), ranging from 2.5 dB to 3dB.

The average SSIM and PNSR values for different attacks are illustrated in figures 6.2 and 6.3. The plot demonstrates the metric performance to evaluate the perceptual similarity between a proposed image and its distortion version. The result reveals that the metric achieves a higher value of SSIM and PSNR values for the fingerprint images for all the content-preserving operations.

To assess the robustness, the BER was calculated between the original and enhanced image. The result shows that the proposed method demonstrates good robustness. However, the approached method is still sensitive to a rotation (1 degree) and Gaussian noise ($\sigma = 0.005$). The robustness moderately affected the average filter (3x3 window), JPEG lossy compression (QF= 90%), and the Contrast Low (CL) and Contrast High (CH). Hence**,** for salt and pepper noise ($\sigma = 0.01$), the bit error rate is good.

In addition, we observed the performance of the minutiae extraction technique as shown in Table 6.3 and Figure 5.4. Subsequently, we calculate the Hausdorff distance (as explained in section 4.1.1) between the minutiae from the distorted image and the enhanced image. The Hausdorff distance value is comparatively low for our proposed approach, by retaining maximum minutiae compared to the DWT SVD method. Table 6.4 describes the performance evaluation of the metrics and minutiae of the fingerprint images.

Table 6.1: Content preserving operation used to assess the hash performance

| Attack | Parameters |
|---|---|
| **Image Processing Operations** | |
| JPEG lossy compression | Quality Factor =90% |
| Gaussian Noise | Variance = 0.005 |
| Average Filter | Window size 3x3 |
| Salt and Pepper | Variance = 0.01 |
| Contrast Low | / |
| Contrast High | / |
| **Geometric Distortion** | |
| Rotation | Degree $1^0$ |

Table 6.2: Average SSIM and PSNR Value

| Attack and its Parameters | Average SSIM Value | | | Average PSNR Value | | | Average BER |
|---|---|---|---|---|---|---|---|
| | Attacked Image | Proposed Image | Difference between the attacked and proposed image | Attacked Image | Proposed Image | Difference between the attacked and proposed image | |
| Rotation $1^0$ | 0.6825 | 0.8306 | 0.1481 | 16.6131 | 19.9298 | 3.3167 | 0.3209 |
| Average Filter 3x3 | 0.8615 | 0.9345 | 0.073 | 22.8825 | 25.8975 | 3.015 | 0.3089 |
| Gaussian Noise V=0.005 | 0.4968 | 0.5543 | 0.0575 | 24.5433 | 27.6197 | 3.0764 | 0.5074 |
| Salt and pepper V=0.01 | 0.7129 | 0.8026 | 0.0897 | 23.7273 | 26.2882 | 2.5609 | 0.1871 |
| Jpeg 90% | 0.9164 | 0.9531 | 0.0367 | 40.6526 | 43.6505 | 2.9979 | 0.3002 |
| Contrast Low(CL) | 0.9179 | 0.9499 | 0.032 | 19.3134 | 22.3275 | 3.0141 | 0.2924 |
| Contrast High(CH) | 0.8540 | 0.8638 | 0.0098 | 19.2542 | 22.2454 | 2.9912 | 0.2982 |

Table 6.3: Average Hausdorff Distance of the Minutiae

| Attack and its Parameters | Average Hausdorff distance | |
|---|---|---|
| | **Attacked Image** | **Proposed Image** |
| Rotation $1^0$ | 0.0103 | 0.0106 |
| Average Filter 3x3 | 0.0161 | 0.0112 |
| Gaussian Noise V=0.005 | 0.0133 | 0.0107 |
| Salt and pepper V=0.01 | 0.0201 | 0.0062 |
| Jpeg 90% | 0.0053 | 0.0024 |
| Contrast Low(CL) | 0.0548 | 0.0117 |
| Contrast High(CH) | 0.0282 | 0.0131 |

Table 6.4: Performance Evaluation of Metrics and Minutiae

| **Attacks** | **SSIM** | **PSNR** | **Hausdorff distance of the Minutiae** |
|---|---|---|---|
| Rotation $1^0$ | Better | Good | Slightly sensitivity |
| Average Filter 3x3 | Good | Good | Better |
| Gaussian Noise V=0.005 | Moderate | Good | Better |
| Salt and pepper V=0.01 | Better | Good | Good |
| Jpeg 90% | Good | Good | Good |
| Contrast Low(CL) | Good | Good | Good |
| Contrast High(CH) | Better | Good | Good |

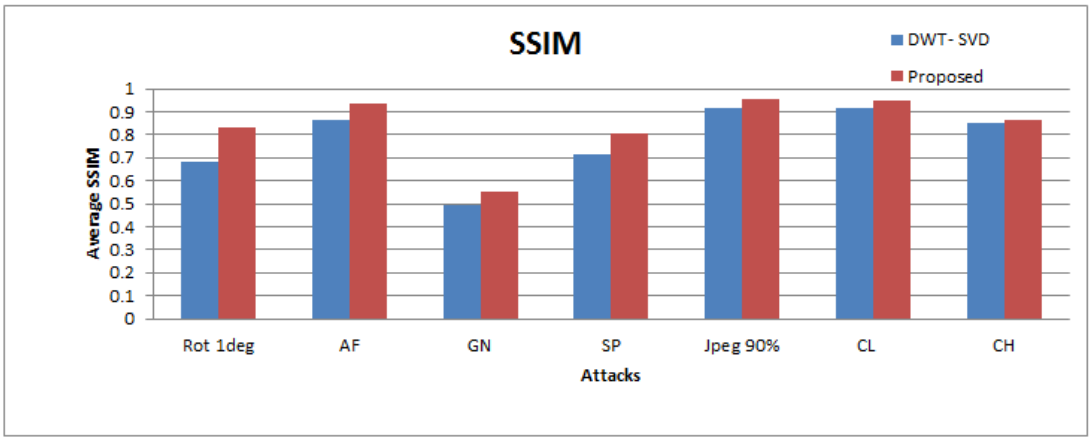



Figure 6.2: Average SSIM

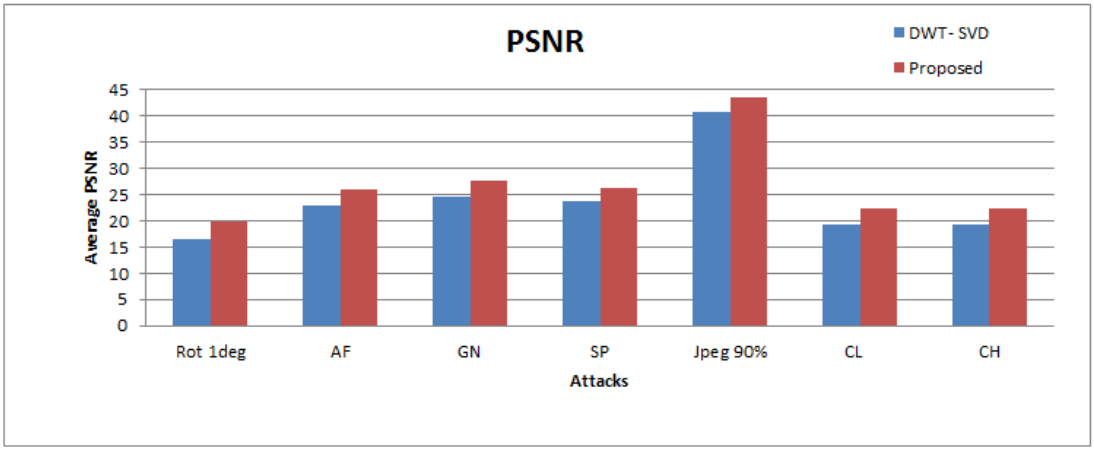



Figure 6.3: Average PSNR

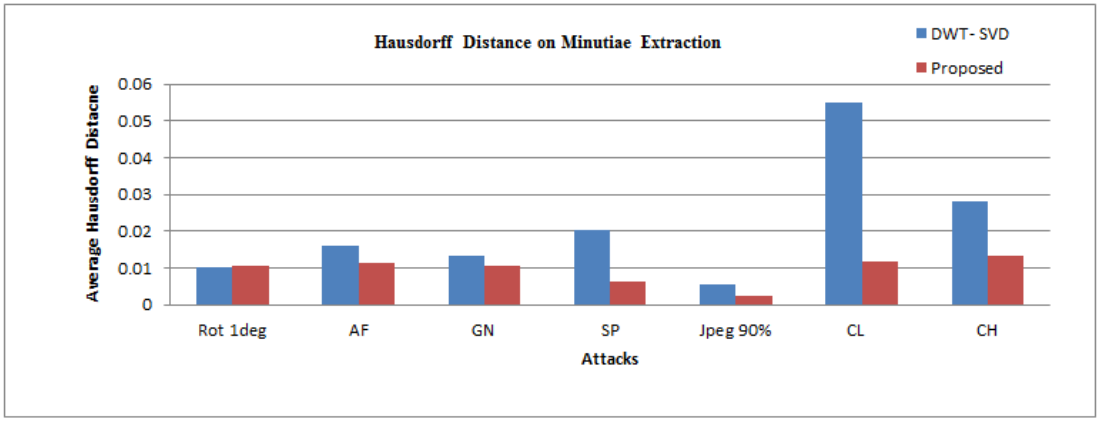



Figure 6.4: Average Hausdorff Distance of Minutiae

## 6.5 Summary

In this research, a robust perceptual hash extract technique using DWT-SVD method is proposed. The proposed method focus on extraction and securing the hash in the database after wavelet-SVD combination. The tradeoff between robustness and imperceptibility is achieved by proper selection of quantization steps. Overall, the proposed method demonstrates to enhance the fingerprint image and provide good balance of robustness and imperceptibility. Additionally, this approach retains the maximum minutiae of the fingerprint image, even if the given image is distorted.

# Chapter 7

# Conclusion and future work

## 7.1 Introduction

With the rapid increase in biometric recognition systems in the commercial sector, the security of stored biometric data is increasingly becoming crucial. Current biometric systems have a number of vulnerabilities and a motivated adversary can undoubtedly cause severe harm to a biometric system, as well as to users enrolled in the system. Furthermore, due to the permanent nature of biometrics data, its theft and misuse may be irreversible and have lasting consequences.

This thesis focuses on improving the security of fingerprint templates and accurate comparison of fingerprint content. The generation of fingerprint templates, which in turn are used to compare fingerprint content or their perceptual hashes mostly rely on feature extraction techniques, for instance SIFT or fingerprint minutiae. We used shape context based perceptual hashes using the RSCH and ASCH methods to plot the accuracy of fingerprint comparison using ROC curves. The framework of perceptual fingerprint image hashing algorithms has major components, including pre-processing on image, feature extraction and post processing. The robustness of fingerprint image hashing in conjunction with content-preserving operations such as Gaussian noise, JPEG compression, filtering and geometric attacks are investigated.

## 7.2 Contribution of the thesis

The design of fingerprint image hashing has three important modules: feature extraction, feature compression and security issues. In this thesis, I focused mainly on robust feature extraction and security issues. The contributions of this thesis are concluded as follows:

- We discuss the implementation of robust minutiae based fingerprint image hashing. In this method, the minutiae of the fingerprint is combined with the SIFT-Harris features (that tolerate geometric invariance) to detect robust minutiae.

In addition, the orientation and descriptor in the minutiae of the fingerprint image is incorporated whilst fingerprint identification is performed using hashed robust minutiae.

It shows that the shape contexts provide an outstanding description of the geometric structure of a shape. Moreover, this approach allows embedding the geometric distribution of robust minutiae feature points as well as their descriptors into a short hash vector. The experimental results demonstrate that angular shape context hashing relatively outperforms the radial shape context hashing. This leads to conclusion that the distribution of feature points in the angular direction is better discriminated than in the radial direction, however with slightly sensitivity to the geometric attacks.

- The important contribution is fingerprint image hashing based on an effective combination of wavelet based feature and SIFT feature. In this approach, SIFT-Wavelet is combined with the Fingerprint Minutiae extraction method to determine the most prominent fingerprint features. These features are post-processed using RSCH and ASCH techniques to plot the accuracy of fingerprint comparison using ROC curves.

  It shows that SIFT-Wavelet minutiae based fingerprint image hashing is robust to attacks, such as median filter and Gaussian blur and rotation, but high sensitivity to the JPEG compression and translation. For further investigation, SIFT is combined with the Fingerprint Minutiae extraction procedure and post-processed using RSCH and ASCH techniques to plot the accuracy. The experimental results demonstrate that the fingerprint template and accuracy of fingerprint comparison improved when a combination of two different feature extraction techniques are used, in contrast to using only a single feature extraction procedure.

  ROC plots of SIFT-Harris-Minutiae, SIFT-Wavelet-Minutiae, SIFT-Minutiae and SIFT are shown in Chapter 4. These ROCs further demonstrate that the SIFT-Harris-Minutiae outperform other combinations. Therefore, the new SIFT-Harris-Minutiae technique is more suitable for generating a template and comparison of the fingerprint content.

- The third contribution of thesis is to enhance the performance of a fingerprint system, perceptual hashing is used to improve the minutiae extraction of fingerprint images. The proposed work focused on securing the hash and improving minutiae extraction, under various content preservation operations. The hash extraction is performed after wavelet transform and singular value decomposition (SVD). The performance evaluation of this approach includes important metrics such as SSIM and PSNR. Experimentally, it has shown robustness against image processing operations and geometric attacks.

## 7.3 Future work

This section highlights the direction of future research to improve security of biometric recognition systems based on hash techniques.

- In this research, we developed robust minutiae based fingerprint image hashing and investigated their perceptual robustness against content persevering manipulations. Based on the geometric invariance of SIFT-Harris keypoints, we combined the minutiae of fingerprint with SIFT-Harris feature to detect robust minutiae. Shape contexts provide an outstanding description of the geometric structure of a shape. We can embed the geometric distribution of robust minutiae feature points as well as their descriptors into a short hash vector and proposed minutiae based fingerprint image hashing, i.e., The RSCH in the radial direction and ASCH in the angular direction. To achieve better perceptual robustness, a joint RSCH-ASCH can be promising future direction for fingerprint image hashing.

- The shape contexts based hashes has an advantage of embedding the geometric structure of the image, the proposed minutiae based fingerprint image hashing technique could be applied in image tampering detection.

- In this research, the robust points in the SIFT have been determined through approximation coefficients using the Haar wavelet. Horizontal, vertical and diagonal coefficients are utilized to localize the salient points. A detailed

study of various wavelet transform could be conducted to optimise the performance of fingerprint image hashing.

- We presented a technique to improve the minutiae extraction of fingerprint images using perceptual hashing. The hash is extracted using a combination of the wavelet algorithm and SVD technique. It demonstrated that the proposed scheme has superior robustness against image processing operations and geometric attacks. Machine learning technique will be used to model these attacks in order to improve the hashing system.

- Further the proposed work can be extended to other biometric traits (e.g. face, palmprint, iris, etc.,) and other image media to enhance recognition performance. Although biometrics may be susceptible to false matches, possibly due to scanning and sensor errors, there are ways to minimize this, currently, by utilizing multi-factor options like a password or smartcard combined with biometrics to add an extra layer of security towards authentication. If used together, and not alternatively, the systems are significantly stronger than when used individually.

  Recent trends, multi-biometrics (the use of different sets of biometric data simultaneously) as a good alternative to increase matching accuracy for identification and verification. Multimodal biometrics systems, which use multiple sensors for data acquisition, offer multiple recognition algorithms and take advantage of each biometric technology while overcoming the limitations of a single technology.

  In terms of use, the future of biometrics could be in mobile devices and applications for eGovernment, eHealth and eBanking. Through biometric mobile scanning devices, authentication and identification can be brought to the field. It is easy to imagine the possible uses for such systems for other professions, like law enforcement, borders control, medical and emergency services, or even to secure access to government or financial services.

Biometric technology could soon become mainstream to the growth of the mobile devices market. Biometrics Research Group, Inc.estimates that the sale of smartphones, in the U.S. only, will grow to 121 million in 2018. Due to this proliferation and to the increased functionalities they offer their users, their analysts believe there will be a strong push toward the integration of biometric technology to replace traditional authentication via pin and password. Biometrics Research Group, Inc. predicted that already in 2014 over 90 million smartphones would be shipped with biometric technology, while Goode Intelligence has forecasted that by 2019 the number of mobile and wearable biometric technology users in the world will reach 5.5 billion.

# Bibliography


[1] Bouridane, A. (2009). *Imaging for Forensics and Security: From Theory to Practice* (Vol. 106). Springer.

[2] Jain, A. K., Ross, A., & Prabhakar, S. (2004). An introduction to biometric recognition. *Circuits and Systems for Video Technology, IEEE Transactions on*, *14*(1), 4-20.

[3] Jain, A. K., & Kumar, A. (2010). Biometrics of next generation: An overview. *Second Generation Biometrics*.

[4] Ross, A. A. (2003). *Information fusion in fingerprint authentication* (Doctoral dissertation, Michigan State University).

[5] Maltoni, D., Maio, D., Jain, A. K., & Prabhakar, S. (2009). *Handbook of fingerprint recognition*. Springer.

[6] Jain, A. K., Flynn, P., & Ross, A. A. (2007). *Handbook of biometrics*. Springer Science & Business Media.

[7] Jain, A. K., Nandakumar, K., & Nagar, A. (2008). Biometric template security. *EURASIP Journal on Advances in Signal Processing*, *2008*, 113.

[8] Jain, A. K., Ross, A., & Uludag, U. (2005, September). Biometric template security: Challenges and solutions. In *Proceedings of European Signal Processing Conference (EUSIPCO)* (pp. 469-472).

[9] Ratha, N. K., Connell, J. H., & Bolle, R. M. (2001, January). An analysis of minutiae matching strength. In *Audio-and Video-Based Biometric Person Authentication* (pp. 223-228). Springer Berlin Heidelberg.

[10] Jain, A. K., Feng, J., & Nandakumar, K. (2010). Fingerprint Matching. *Computer*, *43*(2), 36-44.

[11] Nagar, A., Nandakumar, K., & Jain, A. K. (2010). A hybrid biometric cryptosystem for securing fingerprint minutiae templates. *Pattern Recognition Letters*, *31*(8), 733-741.

[12] Han, S. H., & Chu, C. H. (2010). Content-based image authentication: current status, issues, and challenges. *International Journal of Information Security*, *9*(1), 19-32.

[13] Ahmed, F., Siyal, M. Y., & Uddin Abbas, V. (2010). A secure and robust hash-based scheme for image authentication. *Signal Processing*, *90*(5), 1456-1470.

[14] Monga, V., & Evans, B. L. (2006). Perceptual image hashing via feature points: performance evaluation and tradeoffs. *Image Processing, IEEE Transactions on*, *15*(11), 3452-3465.

[15] Bay, H., Tuytelaars, T., & Van Gool, L. (2006). Surf: Speeded up robust features. In *Computer Vision–ECCV 2006* (pp. 404-417). Springer Berlin Heidelberg.

[16] Lv, X., & Wang, Z. J. (2012). Perceptual image hashing based on shape contexts and local feature points. *Information Forensics and Security, IEEE Transactions on*, *7*(3), 1081-1093.

[17] Lefebvre, F., Macq, B., & Legat, J. D. (2002, September). RASH: Radon soft hash algorithm. In *Signal Processing Conference, 2002 11th European* (pp. 1-4). IEEE.

[18] Tuyls, P., Škoriç, B., & Kevenaar, T. (2007). *Security with noisy data: on private biometrics, secure key storage and anti-counterfeiting*. Springer.

[19] Moujahdi, C., Bebis, G., Ghouzali, S., & Rziza, M. (2014). Fingerprint shell: Secure representation of fingerprint template. *Pattern Recognition Letters*, *45*, 189-196.

[20] Liang, X., Bishnu, A., & Asano, T. (2007). A robust fingerprint indexing scheme using minutia neighborhood structure and low-order delaunay triangles. *Information Forensics and Security, IEEE Transactions on*, *2*(4), 721-733.

[21] Jin, Z., Jin Teoh, A. B., Ong, T. S., & Tee, C. (2012). Fingerprint template protection with minutiae-based bit-string for security and privacy preserving. *Expert Systems with Applications*, *39*(6), 6157-6167.

[22] Liu, E., Zhao, H., Liang, J., Pang, L., Chen, H., & Tian, J. (2012). Random local region descriptor (RLRD): A new method for fixed-length feature representation of fingerprint image and its application to template protection. *Future Generation Computer Systems*, *28*(1), 236-243.

[23] Feng, J. (2008). Combining minutiae descriptors for fingerprint matching. *Pattern Recognition*, *41*(1), 342-352.

[24] Cappelli, R., Ferrara, M., & Maltoni, D. (2010). Minutia cylinder-code: A new representation and matching technique for fingerprint recognition. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, *32*(12), 2128-2141.

[25] Tulyakov, S., Farooq, F., & Govindaraju, V. (2005). Symmetric hash functions for fingerprint minutiae. In *Pattern Recognition and Image Analysis* (pp. 30-38). Springer Berlin Heidelberg.

[26] Tulyakov, S., Farooq, F., Mansukhani, P., & Govindaraju, V. (2007). Symmetric hash functions for secure fingerprint biometric systems. *Pattern Recognition Letters*, *28*(16), 2427-2436.

[27] Sutcu, Y., Sencar, H. T., & Memon, N. (2007, April). A geometric transformation to protect minutiae-based fingerprint templates. In *Defense and Security Symposium* (pp. 65390E-65390E). International Society for Optics and Photonics.

[28] Shuai, X., Zhang, C., & Hao, P. (2008, December). Fingerprint indexing based on composite set of reduced SIFT features. In *Pattern Recognition, 2008. ICPR 2008. 19th International Conference on* (pp. 1-4). IEEE.

[29] Xu, H., Veldhuis, R., Bazen, A. M., Kevenaar, T. A., Akkermans, T. A., & Gokberk, B. (2009). Fingerprint verification using spectral minutiae representations. *Information Forensics and Security, IEEE Transactions on*, *4*(3), 397-409.

[30] Xu, H., Veldhuis, R., Kevenaar, T. A., & Akkermans, T. A. (2009). A fast minutiae-based fingerprint recognition system. *Systems Journal, IEEE*, *3*(4), 418-427.

[31] Feng, J., Ouyang, Z., & Cai, A. (2006). Fingerprint matching using ridges. *Pattern Recognition*, *39*(11), 2131-2140.

[32] Jain, A. K., Chen, Y., & Demirkus, M. (2007). Pores and ridges: high-resolution fingerprint matching using level 3 features. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, *29*(1), 15-27.

[33] Ahn, D., Kong, S. G., Chung, Y. S., & Moon, K. Y. (2008, May). Matching with secure fingerprint templates using non-invertible transform. In *Image and Signal Processing, 2008. CISP'08. Congress on* (Vol. 2, pp. 29-33). IEEE.

[34] Lee, C., Choi, J. Y., Toh, K. A., & Lee, S. (2007). Alignment-free cancellable fingerprint templates based on local minutiae information. *Systems, Man, and Cybernetics, Part B: Cybernetics, IEEE Transactions on*, *37*(4), 980-992.

[35] Chang, S. H., Cheng, F. H., Hsu, W. H., & Wu, G. Z. (1997). Fast algorithm for point pattern matching: invariant to translations, rotations and scale changes. *Pattern recognition*, *30*(2), 311-320.

[36] Jiang, X., & Yau, W. Y. (2000). Fingerprint minutiae matching based on the local and global structures. In *Pattern Recognition, 2000. Proceedings. 15th International Conference on* (Vol. 2, pp. 1038-1041). IEEE.

[37] Luo, X., Tian, J., & Wu, Y. (2000). A minutiae matching algorithm in fingerprint verification. In *Pattern Recognition, 2000. Proceedings. 15th International Conference on* (Vol. 4, pp. 833-836). IEEE.

[38] Bhowmick, P., Bishnu, A., Bhattacharya, B. B., Kundu, M. K., Murthy, C. A., & Acharya, T. (2005). Determination of minutiae scores for fingerprint image applications. *International journal of image and graphics, 5*(03), 537-571.

[39] Jain, A., Hong, L., & Bolle, R. (1997). On-line fingerprint verification. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, *19*(4), 302-314.

[40] Monga, V., & Mıhçak, M. K. (2007). Robust and secure image hashing via non-negative matrix factorizations. *Information Forensics and Security, IEEE Transactions on*, *2*(3), 376-390.

[41] Wu, M., Mao, Y., & Swaminathan, A. (2007, August). A signal processing and randomization perspective of robust and secure image hashing. In *Statistical Signal Processing, 2007. SSP'07. IEEE/SP 14th Workshop on* (pp. 166-170). IEEE.

[42] Kim, C. (2003). Content-based image copy detection. *Signal Processing: Image Communication*, *18*(3), 169-184.

[43] Venkatesan, R., Koon, S. M., Jakubowski, M. H., & Moulin, P. (2000). Robust image hashing. In *Image Processing, 2000. Proceedings. 2000 International Conference on* (Vol. 3, pp. 664-666). IEEE.

[44] Lefèbvre, F., Czyz, J., & Macq, B. (2003, September). A robust soft hash algorithm for digital image signature. In *Image Processing, 2003. ICIP 2003. Proceedings. 2003 International Conference on* (Vol. 2, pp. II-495). IEEE.

[45] Swaminathan, A., Mao, Y., & Wu, M. (2006). Robust and secure image hashing. *Information Forensics and Security, IEEE Transactions on*, *1*(2), 215-230.

[46] Khelifi, F., & Jiang, J. (2010). Perceptual image hashing based on virtual watermark detection. *Image Processing, IEEE Transactions on*, *19*(4), 981-994.

[47] Khelifi, F., & Jiang, J. (2010). Analysis of the security of perceptual image hashing based on non-negative matrix factorization. *Signal Processing Letters, IEEE*, *17*(1), 43-46.

[48] Kozat, S. S., Venkatesan, R., & Mihçak, M. K. (2004, October). Robust perceptual image hashing via matrix invariants. In *Image Processing, 2004. ICIP'04. 2004 International Conference on* (Vol. 5, pp. 3443-3446). IEEE.

[49] Badrinath, G. S., Gupta, P., & Mehrotra, H. (2013). Score level fusion of voting strategy of geometric hashing and SURF for an efficient palmprint-based identification. *Journal of real-time image processing*, *8*(3), 265-284

[50] Tuytelaars, T., & Mikolajczyk, K. (2008). Local invariant feature detectors: a survey. *Foundations and Trends® in Computer Graphics and Vision*, *3*(3), 177-280.

[51] Lowe, D. G. (2004). Distinctive image features from scale-invariant keypoints. *International journal of computer vision*, *60*(2), 91-110.

[52] Koval, O., Voloshynovskiy, S., Bas, P., & Cayre, F. (2009, February). On security threats for robust perceptual hashing. In *IS&T/SPIE Electronic Imaging* (pp. 72540H-72540H). International Society for Optics and Photonics.

[53] Tuyls, P., Akkermans, A. H., Kevenaar, T. A., Schrijen, G. J., Bazen, A. M., & Veldhuis, R. N. (2005, January). Practical biometric authentication with template protection. In *Audio-and Video-Based Biometric Person Authentication* (pp. 436-446). Springer Berlin Heidelberg.

[54] Breebaart, J., Yang, B., Buhan-Dulman, I., & Busch, C. (2009). Biometric template protection. *Datenschutz und Datensicherheit-DuD*, *33*(5), 299-304.

[55] Rane, S. (2014). Standardization of Biometric Template Protection. *MultiMedia, IEEE*, *21*(4), 94-99.

[56] Sun, S. W., Lu, C. S., & Chang, P. C. (2007, January). Biometric template protection: A key-mixed template approach. In *Proceeding IEEE International Conference Consumer Electronics* (pp. 10-14).

[57] Roberge, C. S. D., Stoianov, A., Gilroy, R., & Kumar, B. V. (1999). Biometric encryption. *ICSA Guide to Cryptography*, 8.

[58] Sutcu, Y., Li, Q., & Memon, N. (2007, February). How to protect biometric templates. In *Electronic Imaging 2007* (pp. 650514-650514). International Society for Optics and Photonics.

[59] Brindha, V. E. (2012). Biometric Template Security using Dorsal Hand Vein Fuzzy Vault. *J Biomet Biostat*, *3*(145), 2.

[60] Sutcu, Y., Sencar, H. T., & Memon, N. (2007, April). A geometric transformation to protect minutiae-based fingerprint templates. In *Defense and Security Symposium* (pp. 65390E-65390E). International Society for Optics and Photonics.

[61] Mirmohamadsadeghi, L., & Drygajlo, A. (2013, September). A template privacy protection scheme for fingerprint minutiae descriptors. In *Biometrics Special Interest Group (BIOSIG), 2013 International Conference of the* (pp. 1-8). IEEE.

[62] Prasad, M. V., & Santhosh Kumar, C. (2014). Fingerprint template protection using multiline neighboring relation. *Expert Systems with Applications*, *41*(14), 6114-6122.

[63] Jain, A. K., Nandakumar, K., & Nagar, A. (2013). Fingerprint Template Protection: From Theory to Practice. In *Security and Privacy in Biometrics* (pp. 187-214). Springer London.

[64] Teoh, A. B. J., Toh, K. A., & Yip, W. K. (2007). 2^ N discretisation of biophasor in cancellable biometrics. In *Advances in Biometrics* (pp. 435-444). Springer Berlin Heidelberg.

[65] Scheirer, W. J., & Boult, T. E. (2007, September). Cracking fuzzy vaults and biometric encryption. In *Biometrics Symposium, 2007* (pp. 1-6). IEEE.

[66] Draper, S. C., Khisti, A., Martinian, E., Vetro, A., & Yedidia, J. S. (2007, April). Using distributed source coding to secure fingerprint biometrics. In *Acoustics, Speech and Signal Processing, 2007. ICASSP 2007. IEEE International Conference on* (Vol. 2, pp. II-129). IEEE.

[67] Ratha, N. K., Chikkerur, S., Connell, J. H., & Bolle, R. M. (2007). Generating cancelable fingerprint templates. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, *29*(4), 561-572.

[68] Jeffers, J., & Arakala, A. (2007). Fingerprint alignment for a minutiae-based fuzzy vault. In *Proc Biometric Symposium, BCC, Baltimore, MD*.

[69] Farooq, F., Bolle, R. M., Jea, T. Y., & Ratha, N. (2007, June). Anonymous and revocable fingerprint recognition. In *Computer Vision and Pattern Recognition, 2007. CVPR'07. IEEE Conference on* (pp. 1-7). IEEE.

[70] Sutcu, Y., Rane, S., Yedidia, J. S., Draper, S. C., & Vetro, A. (2008, July). Feature extraction for a Slepian-Wolf biometric system using LDPC codes. In *Information Theory, 2008. ISIT 2008. IEEE International Symposium on* (pp. 2297-2301). IEEE.

[71] Rathor, K. Iris Collarette Boundary Localization Using 2-D DFT For Iris Based Biometric System.

[72] Imtiaz, H., & Fattah, S. A. (2011). A spectral domain dominant feature extraction algorithm for palm-print recognition. *International Journal of Image Processing*, *5*, 130-144.

[73] Amornraksa, T., & Tachaphetpiboon, S. (2006). Fingerprint recognition using DCT features. *Electronics Letters*, *42*(9), 522-523.

[74] Imtiaz, H., & Fattah, S. A. (2010, October). A DCT-based feature extraction algorithm for palm-print recognition. In *Communication Control and Computing Technologies (ICCCCT), 2010 IEEE International Conference on* (pp. 657-660). IEEE.

[75] Badrinath, G. S., Tiwari, K., & Gupta, P. (2012). An efficient palmprint based recognition system using 1D-DCT features. In *Intelligent Computing Technology* (pp. 594-601). Springer Berlin Heidelberg.

[76] Singh, S., Ramalho, M., Correia, P. L., & Soares, L. D. (2012, August). PP-RIDER: A Rotation-Invariant degraded partial palmprint recognition technique. In *Signal Processing Conference (EUSIPCO), 2012 Proceedings of the 20th European* (pp. 1499-1503). IEEE.

[77] Prungsinchai, S., Khelifi, F., & Bouridane, A. (2013, September). Fourier-Mellin transform for Robust Image Hashing. In *Emerging Security Technologies (EST), 2013 Fourth International Conference on* (pp. 58-61). IEEE.

[78] Ekinci, M., & Aykut, M. (2007). Palmprint recognition by applying wavelet subband representation and kernel PCA. In *Machine learning and data mining in pattern recognition* (pp. 628-642). Springer Berlin Heidelberg.

[79] Yang, F., Ma, B., Xia Wang, Q., & Yao, D. (2007, June). Information fusion of biometrics based-on fingerprint, hand-geometry and palm-print. In *Automatic Identification Advanced Technologies, 2007 IEEE Workshop on* (pp. 247-252). IEEE.

[80] Prungsinchai, S. (2014). *Robust and secure perceptual hashing in the transform domain* (Doctoral dissertation, Northumbria University).

[81] Derrode, S., & Ghorbel, F. (2001). Robust and efficient Fourier–Mellin transform approximations for gray-level image reconstruction and complete invariant description. *Computer Vision and Image Understanding*, *83*(1), 57-78.

[82] Khayam, S. A. (2003). The discrete cosine transform (DCT): theory and Application. *Michigan State University*.

[83] Mallat, S. G. (1989). A theory for multiresolution signal decomposition: the wavelet representation. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, *11*(7), 674-693.

[84] Smith, M. J., & Barnwell III, T. P. (1987). A new filter bank theory for time-frequency representation. *Acoustics, Speech and Signal Processing, IEEE Transactions on*, *35*(3), 314-327.

[85] Bhattacharjee, S. K., & Vandergheynst, P. (1999, October). End-stopped wavelets for detecting low-level features. In *SPIE's International Symposium on Optical Science, Engineering, and Instrumentation* (pp. 732-741). International Society for Optics and Photonics.

[86] Antoine, J. P., & Murenzi, R. (1996). Two-dimensional directional wavelets and the scale-angle representation. *Signal processing*, *52*(3), 259-281.

[87] Geisler, W. S., Gilbert, J. E., & Ghosh, J. (2005). Perceptually based methods for robust image hashing.

[88] http://bias.csr.unibo.it/fvc2004/download.asp

[89] Beaudet, P. R. (1978, November). Rotationally invariant image operators. In *International Joint Conference on Pattern Recognition* (Vol. 579, p. 583).

[90] Simard, P. Y., Bottou, L., Haffner, P., & LeCun, Y. (1999). Boxlets: a fast convolution algorithm for signal processing and neural networks. *Advances in Neural Information Processing Systems*, 571-577.

[91] Harris, C., & Stephens, M. (1988, August). A combined corner and edge detector. In *Alvey vision conference* (Vol. 15, p. 50).

[92] Schneider, M., & Chang, S. F. (1996, September). A robust content based digital signature for image authentication. In *Image Processing, 1996. Proceedings., International Conference on* (Vol. 3, pp. 227-230). IEEE.

[93] Lin, C. Y., & Chang, S. F. (2001). A robust image authentication method distinguishing JPEG compression from malicious manipulation. *Circuits and Systems for Video Technology, IEEE Transactions on*, *11*(2), 153-168.

[94] Lu, C. S., & Liao, H. Y. (2003). Structural digital signature for image authentication: an incidental distortion resistant scheme. *Multimedia, IEEE Transactions on*, *5*(2), 161-173.

[95] Fridrich, J., & Goljan, M. (2000). Robust hash functions for digital watermarking. In *Information Technology: Coding and Computing, 2000. Proceedings. International Conference on* (pp. 178-183). IEEE.

[96] Bhattacharjee, S., & Kutter, M. (1998, October). Compression tolerant image authentication. In *Image Processing, 1998. ICIP 98. Proceedings. 1998 International Conference on* (Vol. 1, pp. 435-439). IEEE.

[97] Lin, D. W., & Yang, S. H. (2007). Wavelet-based salient region extraction. In *Advances in Multimedia Information Processing–PCM 2007* (pp. 389-392). Springer Berlin Heidelberg

[98] Lim, J., Kim, Y., & Paik, J. (2009). Comparative analysis of wavelet-based scale-invariant feature extraction using different wavelet bases. In *Signal Processing, Image Processing and Pattern Recognition* (pp. 297-303). Springer Berlin Heidelberg.

[99] Sebe, N. & Lew, M. S. (2003). Comparing salient point detectors. *Pattern recognition letters*, *24*(1), 89-96.

[100] Loupias, E., Sebe, N., Bres, S., & Jolion, J. M. (2000, September). Wavelet-based salient points for image retrieval. In *Image Processing, 2000. Proceedings. 2000 International Conference on* (Vol. 2, pp. 518-521). IEEE.

[101] Omidyeganeh, M., Shirmohammadi, S., Laganiere, R., Youmaran, R., & Javadtalab, A. (2013, July). Face identification using wavelet transform of SIFT features. In *Multimedia and Expo Workshops (ICMEW), 2013 IEEE International Conference on* (pp. 1-6). IEEE.

[102] Kumar, N.A.M., Sathidevi, P.S.,(2012).Image match using wavelet — Colour SIFT features. *Industrial and Information Systems* (pp.1-6).IEEE.

[103] Wang, K., Ren, Z., & Xiong, X. (2008, August). Combination of Wavelet and SIFT Features for Image Classification Using Trained Gaussion Mixture Model. In *Intelligent Information Hiding and Multimedia Signal Processing, 2008. IIHMSP'08 International Conference on* (pp. 79-82). IEEE.

[104] Halawani, A., & Burkhardt, H. (2004, August). Image retrieval by local evaluation of nonlinear kernel functions around salient points. In *Pattern Recognition, 2004. ICPR 2004. Proceedings of the 17th International Conference on* (Vol. 2, pp. 955-960). IEEE.

[105] Tu, Z., & Zhu, S. C. (2002). Image segmentation by data-driven Markov chain Monte Carlo. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, *24*(5), 657-673. Tu, Z., & Zhu, S. C. (2002). Image segmentation by data-driven Markov chain Monte Carlo. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, *24*(5), 657-673.

[106] Jian, M., Dong, J., & Jiang, R. (2007, July). Wavelet-based salient regions and their spatial distribution for image retrieval. In *Multimedia and Expo, 2007 IEEE International Conference on* (pp. 2194-2197). IEEE.

[107] Imamoglu, N., Lin, W., & Fang, Y. (2013). A saliency detection model using low-level features based on wavelet transform. *Multimedia, IEEE Transactions on*, *15*(1), 96-105.

[108] Tsai, Y. H. (2012). Hierarchical salient point selection for image retrieval. *Pattern Recognition Letters*, *33*(12), 1587-1593.

[109] Gonzalez, R. C., Woods, R. E., & Eddins, S. L. (2004). Digital image processing using MATLAB. *Upper Saddle River, N. J: Pearson Prentice Hall*.

[110] Porwik, P., & Lisowska, A. (2004). The Haar-wavelet transform in digital image processing: its status and achievements. *Machine graphics and vision*, *13*(1/2), 79-98.

[111] Roy, S., & Sun, Q. (2007, September). Robust hash for detecting and localizing image tampering. In *Image Processing, 2007. ICIP 2007. IEEE International Conference on* (Vol. 6, pp. VI-117). IEEE.

[112] Chum, O., Philbin, J., & Zisserman, A. (2008, September). Near Duplicate Image Detection: min-Hash and tf-idf Weighting. In *BMVC* (Vol. 810, pp. 812-815).

[113] Ke, Y., Sukthankar, R., & Huston, L. (2004, October). Efficient near-duplicate detection and sub-image retrieval. In *ACM Multimedia* (Vol. 4, No. 1, p. 5).

[114] Belongie, S., Malik, J., & Puzicha, J. (2002). Shape matching and object recognition using shape contexts. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, *24*(4), 509-522.

[115] http://bias.csr.unibo.it/fvc2002/databases.asp

[116] Lei, B., Tan, E. L., Chen, S., Ni, D., Wang, T., & Lei, H. (2014). Reversible watermarking scheme for medical image based on differential evolution. *Expert Systems with Applications*, *41*(7), 3178-3188.

[117] Aslantas, V. (2009). An optimal robust digital image watermarking based on SVD using differential evolution algorithm. *Optics Communications*, *282*(5), 769-777.

[118] Bhatnagar, G., & Raman, B. (2009). A new robust reference watermarking scheme based on DWT-SVD. *Computer Standards & Interfaces*, *31*(5), 1002-1013.

[119] Ghouti, L., Bouridane, A., Ibrahim, M. K., & Boussakta, S. (2006). Digital image watermarking using balanced multiwavelets. *Signal Processing, IEEE Transactions on*, *54*(4), 1519-1536.

[120] Ramakrishnan, S., Gopalakrishnan, T., & Balasamy, K. (2011). SVD Based Robust Digital Watermarking For Still Images Using Wavelet Transform. *CCSEA*, 155-167.

[121] Hore, A., & Ziou, D. (2010, August). Image quality metrics: PSNR vs. SSIM. In *Pattern Recognition (ICPR), 2010 20th International Conference on* (pp. 2366-2369). IEEE.

[122] Tang, Z., Wang, S., Zhang, X., & Wei, W. (2009, June). Perceptual similarity metric resilient to rotation for application in robust image hashing. In *Multimedia and Ubiquitous Engineering, 2009. MUE'09. Third International Conference on* (pp. 183-188). IEEE.

[123] Wang, Z., Bovik, A. C., Sheikh, H. R., & Simoncelli, E. P. (2004). Image quality assessment: from error visibility to structural similarity. *Image Processing, IEEE Transactions on*, *13*(4), 600-612.

[124] Al-Najjar, Y. A. (2012). Der Chen Soong," Comparison of Image Quality Assessment: PSNR, HVS, SSIM, UIQI. *International Journal of Scientific & Engineering Research*, *3*(8), 2229-5518.

[125] Hofbauer, H., Rathgeb, C., Uhl, A., & Wild, P. (2012, September). Image metric-based biometric comparators: A supplement to feature vector-based Hamming distance?. In *Biometrics Special Interest Group (BIOSIG), 2012 BIOSIG-Proceedings of the International Conference of the* (pp. 1-5). IEEE.

[126] Keimel, C., & Diepold, K. (2010). Improving the prediction accuracy of PSNR by simple temporal pooling. In *Fifth International Workshop on Video Processing and Quality Metrics for Consumer Electronics-VPQM* (Vol. 2009).

[127] Run, R. S., Horng, S. J., Lai, J. L., Kao, T. W., & Chen, R. J. (2012). An improved SVD-based watermarking technique for copyright protection. *Expert Systems with Applications*, *39*(1), 673-689.

[128] Braeckman, G., Barri, A., Fodor, G., Dooms, A., Barbarien, J., Schelkens, P., & Weng, L. (2012, January). Reduced reference quality assessment based on watermarking and perceptual hashing. In *Sixth International Workshop on Video Processing and Quality Metrics for Consumer Electronics, Scottsdale, Arizona (USA)*.

[129] Gao, X., Lu, W., Tao, D., & Li, X. (2009). Image quality assessment based on multiscale geometric analysis. *Image Processing, IEEE Transactions on*, *18*(7), 1409-1423.

[130] Li, J., Wu, K., Zhang, X., & Ding, M. (2012). Image quality assessment based on multi-channel regional mutual information. *AEU-International Journal of Electronics and Communications*, *66*(9), 784-787.

[131] Weng, L., Braeckman, G., Dooms, A., Preneel, B., & Schelkens, P. (2012, July). Robust Image Content Authentication with Tamper Location. In *Multimedia and Expo (ICME), 2012 IEEE International Conference on* (pp. 380-385). IEEE.

[132] Qin, C., Chang, C. C., & Tsou, P. L. (2012). Perceptual Image Hashing Based on the Error Diffusion Halftone Mechanism. *International Journal of Innovative Computing, Information and Control*, *8*(9), 6161-6172.

[133] Wang, Z., & Bovik, A. C. (2009). Mean squared error: love it or leave it? A new look at signal fidelity measures. *Signal Processing Magazine, IEEE*, *26*(1), 98-117.