2013

Mixing Biometric Data For Generating Joint Identities and Preserving Privacy

Asem A. Othman
West Virginia University

Mixing Biometric Data For Generating Joint Identities and Preserving Privacy

by

Asem A. Othman

Doctoral Dissertation submitted to the
Benjamin M. Statler College of Engineering and Mineral Resources
at West Virginia University
in partial fulfillment of the requirements
for the degree of

Doctor of Philosophy
in
Electrical Engineering

Donald A. Adjeroh, Ph.D.
Mark V. Culp, Ph.D.
Gianfranco Doretto, Ph.D.
Xin Li, Ph.D.
Arun A. Ross, Ph.D., Chair

Lane Department of Computer Science and Electrical Engineering

Morgantown, West Virginia
2013

Keywords: Multibiometrics, Face, Fingerprints, Iris, Image-level Fusion, Joint Identities, Virtual Identities, Privacy Preserving, Templates Protection, Cancelable Biometrics, Mixing Signals.

Abstract

Mixing Biometric Data For Generating Joint Identities and Preserving Privacy

by

Asem A. Othman
Doctor of Philosophy in Electrical Engineering

West Virginia University

Arun A. Ross, Ph.D., Chair

Biometrics is the science of automatically recognizing individuals by utilizing biological traits such as fingerprints, face, iris and voice. A classical biometric system digitizes the human body and uses this digitized identity for human recognition. In this work, we introduce the concept of mixing biometrics. Mixing biometrics refers to the process of generating a new biometric image by fusing images of different fingers, different faces, or different irises. The resultant mixed image can be used directly in the feature extraction and matching stages of an existing biometric system. In this regard, we design and systematically evaluate novel methods for generating mixed images for the fingerprint, iris and face modalities. Further, we extend the concept of mixing to accommodate two distinct modalities of an individual, viz., fingerprint and iris. The utility of mixing biometrics is demonstrated in two different applications. The first application deals with the issue of generating a joint digital identity. A joint identity inherits its uniqueness from two or more individuals and can be used in scenarios such as joint bank accounts or two-man rule systems. The second application deals with the issue of biometric privacy, where the concept of mixing is used for de-identifying or obscuring biometric images and for generating cancelable biometrics. Extensive experimental analysis suggests that the concept of biometric mixing has several benefits and can be easily incorporated into existing biometric systems.

To my family.

Acknowledgments

> “ Glory be to You (O Allah)! We have no knowledge except what You have taught us. It is you who are the Knowledgeable, the Wise” Quran 2:32

Foremost on the list to whom I would like to say thank you is Dr. Arun Ross; thank you for accepting me as a member of your research lab (i-probe lab). He introduced me into the topic, supported me, gave me important hints during many interesting discussions, and always encouraged me in my work. I have been privileged to work under his supervision, and I truly appreciate his guidance. It will be a lifelong effort for me to inculcate in me his good qualities.

I am very grateful to have such a capable and cooperative dissertation committee. Dr. Xin Li and Dr. Gianfranco Doretto have been a great help during my studies. I would also like to thank my committee members: Dr. Donald Adjeroh and Dr. Mark Culp. I am truly proud to have them serving as committee members for this dissertation.

It is important that my fellow students in i-probe lab know that their help and friendship was greatly appreciated. I truly enjoyed the time I spent with all of you: Cunjian, Simona, Brian, Yaohui, Gizem, Ravindra, Aglika, Raghavender, Raghunandan, Manisha.

I appreciate the administrative help and support of Karen, Maggie, Laura and Lucy.

I want to express my deep gratitude to Dr. Ayman Abaza for always being there. I thank my kids, parents, brothers, and sister for their unconditional love. Finally yet importantly, I would like to thank my wife Rasha for her support, encouragement, quiet patience, and unwavering love. It is to them that I dedicate this thesis to.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Identity Authentication In Digital Era

Over the course of human history, individuals have been asked to identify themselves in various scenarios; and legal names, address, tokens, pseudonyms, etc. have been used for this purpose [12] [13]. In our vast interconnected world, the need for reliable identity authentication techniques has become of paramount importance. The emergence of biometrics has addressed some of these needs. Biometrics refers to the science of establishing individuals' identities based on their physical and behavioral traits such as fingerprints, face, iris, voice and gait [14]. Compared to traditional authentication schemes that are knowledge-based (e.g., passwords) or token-based (e.g., smart cards), biometric-based systems are considered convenient (the user does not have to memorize passwords or possess proof of identity such as ID cards) and secure (the impostors can be deterred or detected easily) [15]. Hence, biometric systems have been deployed in numerous commercial, civilian and forensic applications to establish identities. Figure 1.1 shows examples of biometric traits used for establishing individuals' identities.

Biometric-based recognition systems rely on the comparison of a digital representation of a physical or behavioral trait with a previously recorded one of the same trait. The first step in all biometric systems is acquiring the raw biometric data. The device used to acquire biometric data varies based on the type of the trait. For example, an optical sensor is typically used to scan a fingerprint or palm and a digital camera is used to capture facial images or certain aspects of the retina or iris. This sensor or camera generates a digital image of the biometric. Next, in most biometric systems, the observed raw biometric data (i.e., image) is reduced into a set of

Figure 1.1: Examples of some of the biometrics traits used for authenticating an individual. Physical traits include face, fingerprint, iris, retina, palmprint, hand geometry, tooth, ear and ocular, while gait, signature and keystroke dynamics are some of the behavioral characteristics. Voice has been traditionally viewed as being physical or as behavioral characteristic.

salient characteristics (i.e., feature set). These feature sets are approximations of the acquired images, but contain more discriminatory and invariant information than the raw digital data. Finally, the biometric system checks whether the extracted feature set has a matching template in the database. Depending on the application, a biometric system could be either a verification system or an identification system. A verification system compares the extracted feature set with a recorded template of a claimed identity. A verification system is referred as a 1-to-1 matching system. On the other hand, an identification system identifies an individual by matching the extracted feature set against all recorded templates in order to determine a match. An identification system is referred as a 1-to-N matching system.

Abstractly, biometric systems digitize our physical body in order to recognize us, which implies a certain degree of simplification, and modifies the nature of our identities. An identity from an individual's perspective is related to their self-image (an individual's mental model of him or herself), self-esteem and perceived individuality within a given society [16]. The digital representations (created by biometric systems) of body traits typically lead to the exclusion of all details except those that are relevant for human recognition in a specific application. So biometric systems attempt t0 reduce the individual into a digital persona [17], that can be measured and

-hopefully-matched.

The thrust of biometrics involves transferring identities from an individual's body to an external electronic digital persona. Although, this transfer raises the controversial issue [12, 18] that biometric systems are digitizing (i.e., oversimplifying) our physical body and living identities into passwords (i.e, feature templates), our research relies on this ability to digitize the human body. First we provide more details about a biometric system before introducing the focus of this research.

1.2 Biometric System

A biometric recognition system (or simply a biometric system) is a pattern recognition system that recognizes individuals based on their biometric trait(s) [15]. A typical biometric system consists of four main modules: (i) sensor module that captures samples of a biometric trait, (ii) feature extraction module that extracts certain salient features from the raw biometric data captured by the sensor, (iii) database module that stores the features extracted by the feature extraction module along with some biographic or other pertinent labels, and (iv) matcher module that matches the features extracted from the biometric samples with the features stored in the system database. These modules will operate in two main stages: enrollment and recognition. The enrollment stage generates a digital representation of an individual's biometric trait and then stores this representation (in some cases, the original raw data is also stored) in the system database. The recognition stage falls into two different categories: verification and identification. Verification involves confirming or denying an individual's claimed identity - "Am I who I claim I am?". These systems are referred as 1-to-1 authentication systems, as a probe is compared against a single (or relatively small) number of gallery entries. Identification involves establishing an individual's identity - "Who am I?". These systems are referred as 1-to-N authentication systems, as the entire database is typically searched during the recognition stage. Figure 1.2 shows a block diagram of a typical biometric recognition system.

The following terminologies related to biometric systems will be adopted in this thesis:

- Biometric trait: A physical or behavioral trait of an individual that is sensed, processed and matched for person verification/identification. Examples include fingerprint, face, voice, iris and gait.

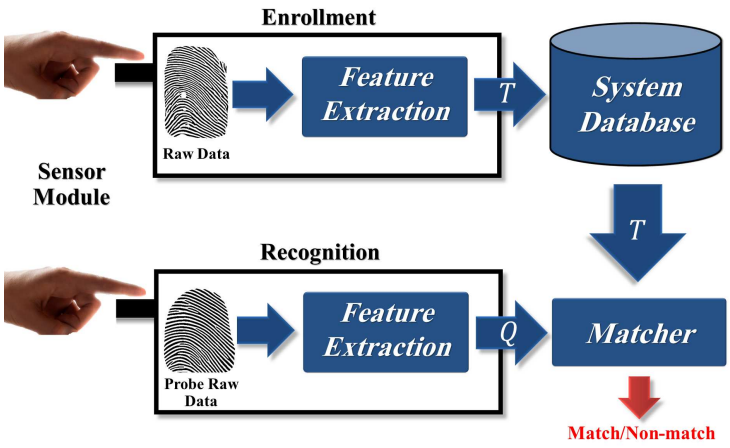


Figure 1.2: An example of a typical biometric recognition system which depicts the enrollment (top) and recognition (bottom) stages of a fingerprint recognition system. T denotes the feature vector that is extracted from the image during enrollment and stored as a template in the system database. Q denotes the probe feature set.

- Biometric instance: A specific instance of a biometric trait such as the left eye or the right index finger.
- Biometric sample: The snapshot of a specific instance of an individual's biometric trait captured by a biometric sensor such as the impression of the right index finger or the image of a face.
- Biometric template (or simply template): The features extracted from a biometric sample acquired during user enrollment and stored in the system database.
- Biometric gallery (or simply gallery): The biometric samples labeled with user identities that are stored in the biometric database.
- Biometric probe (or simply probe): The biometric sample provided by a user during recognition.

We observe that classical biometric systems generate a *single* digital identity corresponding to a single individual during the enrollment and recognition stages. This digital identity is stored in the database. Moreover, preserving the privacy of the stored digital identity is necessary to mitigate concerns related to data sharing and data misuse [19]. This has heightened the need to impart privacy to the stored digital identity. In this thesis, we explore the notion of mixing

biometrics. Mixing biometrics generates a new biometric image by fusing multiple biometric images pertaining to a single or different individuals. The generated image can be considered as a digital representation of a *joint* identity (i.e., a virtual identity) that inherits its uniqueness from *two* different individuals. The mixing biometrics concept also can be used to transform a biometric template into a revocable (i.e., changeable) template that protects the privacy of biometric data. Consequently, mixing biometrics has benefits (as will be discussed in the following section) over traditional biometric systems in terms of storage and security.

1.3 Research objective: Mixing Biometrics

Observed physical attributes of an individual are captured in pixel space (i.e., images) and then deterministically transformed to a lower dimensional feature space (i.e., templates). Mixing biometrics consolidates two different biometric images pertaining to different identities (e.g., fingerprint images of Alice and Bob) or to different instances of the same individual (e.g., left and right index fingerprints of Alice). Consolidating biometrics of different identities at image level (instead of feature level) has the benefit that different feature extraction algorithms can be used to compute the features of the mixed image. This means the mixed images can be used in different applications. The concept of biometrics mixing can be utilized in the following ways.

1.3.1 Generating joint identities

Mixing biometrics can be used to create a joint digital identity that pertains to multiple individuals instead of a single individual. A joint identity is a digital identity that inherits its uniqueness from two (or more) different individuals. In the following scenarios, generating joint identities would be preferable.

Scenario 1:

To achieve a high level of secure authentication, governments have implemented two-man rule accessing mechanism in some government buildings, military installations, laboratories such as those dealing with nuclear material [20], poisonous substances, etc. The joint identity concept can be used in these safety critical applications where the presence of two people is required be-

fore a potentially hazardous operation can be performed. In other words, the authentication process relies on verifying the presence of two authorized identities by presenting their biometrics simultaneously. For instance, in the case of missile launching, two officers must agree that the launch order is valid and both crew members must turn their keys simultaneously to launch the missile. By adopting the joint identity concept, their biometrics could be used to prevent accidental or malicious actions. Hence, their biometrics could be used to generate joint identities in such a way that a successful authentication can be guaranteed only when both persons are providing their biometrics simultaneously.

Scenario 2:

Another benefit of a joint identity is in banking applications. A joint account is a bank account shared by two or more individuals. Any individual who is a member of the joint account can withdraw from the account and deposit to it. Here, the joint identity concept could be utilized to generate a biometric template of this joint identity. Then, this template can be positively matched with either a single biometric probe from one of the owners, or a mixed biometric probe generated by mixing the probe samples of the two owners. In both cases the access to the joint account is guaranteed by performing one verification comparison.

Based on the described scenarios, joint identities can be categorized into identities that are *dissimilar* or *similar* to the original identities, which were mixed to generate it.

1.3.2 Preserving privacy

Although biometrics-based systems are reliable approaches to personal identification and verification, traditional authentication systems still have one advantage over biometrics-based systems. Tokens such as smart cards or passwords can be revoked easily when they are compromised; on the other hand, the user has a limited number of biometrics (e.g., one face, two irises, etc). Moreover, there is the possibility of sharing and misusing of the biometrics data between different agencies. Therefore, there are growing concerns about biometric *function creep*. A company that scans the iris of a user might also allow government or commercial entities to compare this biometric data against their own databases without user's knowledge. In some instances, biometrics data may have to be transmitted across networks with the user's knowledge.

Also, biometric templates tend to reveal private information about a user such as race, gender and certain health conditions [12]. Those issues have heightened the need to accord privacy to the user by adequately protecting the contents of the databases of biometrics systems.

Conventional cryptography provides numerous approaches and algorithms to secure important data/images. However, there are two main concerns when it comes to encrypting biometric templates (i.e., the stored features). First, the security of the cryptographic algorithms relies on the assumption that the cryptographic keys are known only to the legitimate user. Maintaining the secrecy of keys is one of the main challenges in practical cryptosystems. Second, during every identification/verification attempt, the stored template has to be decrypted. Thus, the original biometric template will be exposed to eavesdroppers. The stolen templates could be used to reconstruct the original biomertics images [21, 22, 23, 24, 25]. In other words, compromising a biometric template may result in the loss of a subject's identity.

Therefore, there are two major requirements with regards to protecting biometric templates [26, 27, 28]:

1. Non-invertibility (Irreversibility): It must be computationally infeasible to recover the original biometric image/data from the stored template.

2. Cancelability (Unlinkability): Different versions of protected biometric templates can be generated based on the same biometric data (renewability), while protected templates should not allow cross-matching between different applications (diversity).

In order to fulfill these requirements, a number of techniques have been proposed to limit the amount of information that can be easily extracted from a stored template. Template protection techniques can be broadly categorized into biometric cryptosystems and de-identifying techniques [27, 28].

Biometric cryptosystems [26, 27, 28] offer solutions to biometric-dependent key-release and biometric template protection. In these systems, a cryptographic key is secured by using biometric template or directly generating a cryptographic key from the biometric template. In a biometric cryptosystem, some public information about the biometric template is stored and referred to as helper data. The helper data does not reveal any significant information about the original biometric template, but needed during matching to extract a cryptographic key from the

probe biometric template. Matching is performed indirectly by verifying the validity of the extracted key. Nevertheless, biometric cryptosystems generally result in a noticeable decrease in recognition performance. This is because cryptosystems introduce a higher degree of quantization in the feature extraction module.

De-identifying a biometric image means intentionally changing the biometric content of the image. De-identifying function should allow matching of biometric templates in the transformed domain and should be noninvertible in order to protect the identity even if the transformation function and its parameters are compromised [27, 28]. The de-identified biometric image is typically referred to as a private template [29] or a cancelable biometric [30]. Ratha et al. [30] suggested that templates of the cancelable biometric should be in the same image or data space after transformation which allows the use of existing feature extraction and matching algorithms. Hence, the transformation functions are severely constrained because the space of the biometric images or data should not be changed after the process (e.g., the cancelable face image is a face image and the cancelable fingerprint image is a fingerprint image). So there is a trade-off between the recognition performance and security.

In mixing biometrics, the biometric images pertaining to different individuals are utilized to generate joint, unique, and revocable digitized identities. Therefore, this concept could be considered as an alternative approach to transform the biometric data by mixing them. For instance, mixing fingerprints can be used to de-identify an input fingerprint image by fusing it with another fingerprint (e.g., from a different finger) at image level, in order to produce different mixed images that obscure the identity of the original fingerprints. This allows cancelability in biometrics systems. A user can revoke a template that has been compromised and generate a new template that cannot be easily guessed using the compromised template.

1.4 Mixing Biometrics: An information fusion exercise

Mixing biometrics may be viewed as an exercise in information fusion in general, and image level fusion in particular. For instance, our proposed concept of mixing biometrics could be utilized in multi-instance systems. The left and right thumbs, the left and right irises, or even a

fingerprint and an iris of an individual may be fused and used to verify an individual's identity. In the following sections, we will provide an overview of multibiometric fusion and different image level fusion approaches. Finally, a brief comparison between mixing biometrics and multibiometric fusion is made.

1.4.1 Multibiometric Fusion

Consolidating multiple sources of an individual's digitized representations (e.g., multiple fingerprint images, multiple matchers operating on a single trait, or multiple traits such as fingerprint and iris) solves some of the limitations of unimodal biometric systems (e.g., population coverage, or spoof attacks) [31]. Although, the development of multibiometric systems was considered to be the logical extension of traditional unimodal approaches, there is a need for reliable multimodal fusion algorithms to consolidate different biometric representations. Therefore, there has been a substantial amount of work done on multibiometric fusion approaches. This involves combining biometric information at the image, feature extraction, match score, or decision level. The different levels of fusion can be broadly categorized as follows [31, 32]:

1. Fusion prior to matching.
    - Image level fusion: The raw data from the sensor(s) are combined.
    - Feature level fusion: The different feature sets extracted from multiple biometric sources are combined.
2. Fusion after matching.
    - Score level fusion : The matching scores output by different biometric matchers are combined in order to assist the final recognition decision.
    - Rank level fusion: The output of each biometric system is a subset of possible matches (i.e., identities) sorted in decreasing order of confidence, these subsets of identities are combined. This is relevant in an identification system where a rank may be assigned to the top matching identities.
    - Decision level fusion: The decisions output by the individual biometric matchers are combined.

1.4.2 Image Level Fusion

Image fusion is a process of combining information from different images into a composite that is suitable for post processing tasks, such as classification, recognition and tracking [33]. Image level fusion is the first fusion route for biometric data in a multibiometric system. In the context of multibiometrics, image level fusion entails the consolidation of evidence presented by multiple sources of raw data before they are subjected to feature extraction. In order to accommodate other types of raw biometric data such as voice, video, text, etc; the phrases *signal level fusion* and *sensor level fusion* are also used [31].

The fusion in this early stage of a multibiometric system has the benefit that different application-specific feature extraction algorithms could be used to compute the features from the fused data. So the fused image could be used in different applications and fusion algorithms at other different levels could be applied on it. For example, a mixed fingerprint image could be fused with a mixed iris image at the score level. Till date, a number of image level fusion algorithms have been proposed and we provide a brief overview of these algorithms in the following section.

Literature Review

Image level fusion has been actively utilized in different multibiometric systems. However, this level of fusion is the least explored compared to the other levels of fusion in the context of biometrics. The work done on the fusion of raw biometric data can be classified into three categories [34]:

1. Single sensor, single trait: This category of image level fusion can benefit biometric systems that acquire multiple samples of the same trait using a single sensor. Fusing those samples can account for variations that occur in a biometric trait. For example, partial fingerprint images or different profiles image of a face can be combined to obtain a fused representation of the fingerprint or the face image, respectively, which can address the challenges due to the limitation of small fingerprints sensors or the pose variations between face images. Note that fusing multiple samples of a biometric trait does not necessarily model the intra-user variations. It utilizes the acquired samples of the biometric trait to generate a composite probe or gallery image. Generating a composite representation of different samples of a biometric trait has the following merits [31]: (a) when multiple samples of a subject's trait are available at the time of enrollment, instead of storing these samples as

independent entities, they are fused into a single entity to reduce the probability of a false reject and the matching time, and (b) consolidating the evidence presented by multiple samples of the same biometric alleviates the problem of template selection.

In the context of fingerprints, this category of image fusion has been used to combine multiple impressions of the same finger as exemplified in the following scenarios:

Small-area sensor: Some sensors capture only a small portion of the fingertip [35]. Therefore, several fingerprint mosaicking techniques [36, 37, 38, 39, 40, 41, 42] have been developed to stitch multiple impressions of the same finger and create a larger fingerprint.

Multi-view sensor: Touchless fingerprint sensors capture multiple views of a finger using several calibrated cameras [43] or a single camera with two planar mirrors [44]. These multiple views are mosaicked together to yield a single nail-to-nail fingerprint.

Multispectral sensor: Rowe et al. [45] fused multiple images acquired from a multispectral fingerprint scanner into a single high quality fingerprint image by utilizing a wavelet-based method of image fusion.

In the context of faces, multiple 2D face images obtained from different viewpoints can be stitched together to form a 3D model of the face [46] or a panoramic face mosaic [47][48].

In the context of irises, Hollingsworth et al. [49] and Jillela et al. [50] took advantage of the temporal continuity in videos to improve matching performance using image level fusion. From multiple frames of a frontal iris video, they created a single image. They concluded that using fused iris images for matching resulted in a performance which is comparable to state of the art score level fusion techniques, with less computational burden. Moreover, fusing irises in image domain has been proposed in Zuo et al.'s work to de-identify normalized iris images [51]. They proposed a GRAY-SALT transformation [51] to de-identify irises by adding a synthetic iris image to the original iris image.

2. Multi-sensors, single trait: In this category, samples are acquired by multiple senors instead of using a single sensor. The information obtained from multiple sensors are complementary to each other, and can augment the biometric content and minimize the intra-user variability. In the literature, this category of image level fusion has been used in face identification systems to minimize the variations due to facial appearance (e.g., hairs, wrinkles, and expression) and the effects due to changes in pose and illumination. Hence, researchers have fused the visible spectrum images with near infrared images [52, 53, 54, 55] and with

the corresponding 3D scan (i.e., the range image) in order to create a 3D texture [56, 57].

3. Multibiometric: The previous categories of image level fusion were employed in unimodal biometric systems. However, there has also been some research conducted in fusing images of different biometric traits into a single composite image. The fused multibiometric image can address issues such as memory storage [58] and small sample size recognition [59]. Jing et al. [59] generated a composite image from face and palmprint biometrics by concatenating the responses of different Gabor filters. The resulted image is not in the same image or data space of the face or palmprint images. Therefore, during authentication, kernel discriminative common vectors are extracted from the fused image and radial basis function based neural network is used for classification. Noore et al. [58] developed a fusion algorithm which is based on multi-level discrete wavelet transform to fuse images of four biometric traits (i.e., face, iris, fingerprint, and signature). Here, the resulted image is a scrambled multimodal biometric image and special reconstruction procedures are used to reconstruct the original images and perform authentication. Liu et al. [60] fused the phase of a normalized iris and a palmprint image by using Baud Limited 2D-IDFT. But the fused image can only be matched with a stored template by using a special matcher, i.e., a phase-based image matcher and they did not analyze if the fused image is a cancelable template or not.

1.4.3 Mixing Biometrics *versus* Multibiometric fusion

First of all, deploying a multibiometric system improves the recognition performance by consolidating multiple biometric sources of a single individual (i.e., it increases the biometric content of the digital identity of a specific individual). On the other hand, one objective of mixing biometrics is to generate a joint identity, whose uniqueness pertains to multiple individuals. Therefore, the biometric samples, i.e., images will be fused to generate a new biometric image.

Second, although generating a biometric image is possible by traditional image level fusion approaches (see Section 1.4.2), the sources have to be samples of the same biometric instance obtained from a single sensor or multiple compatible sensors. In other words, traditional image level fusion augments the biometric content of the template pertaining to a single individual by fusing multiple samples of the same instance of a biometric trait. On the contrary, mixing biometrics generates a new biometric image by fusing images of different biometric instances

pertaining to single or different individuals.

Moreover, as described in Section 1.4.2, to fuse biometrics samples at image level, these samples must be compatible, and the correspondences between raw data must be either known in advance or reliably estimated. Therefore, the traditional image level fusion approaches cannot be directly used for mixing biometrics images of different individuals. This is because it is difficult to ensure the existence of such correspondences between two biometric samples acquired from different individuals or instances.

Finally, the multibiometric approach improves the accuracy of the system over its individual unimodal components, but this improvement comes at a cost. Multibiometric systems may be viewed as combinations of two or more unimodal biometric systems. Each unimodal system has its own feature extractor and matcher. Thus, fusing their features, scores or decisions requires additional time. On the other hand, these systems could be cost-effective if a single image is used in the matching step. Hence, the concept of mixing biometrics could provide benefits with regards to storage and security. For example, when images of a subject's index and thumb are available at the time of enrollment, a common approach is to store these images as independent galleries. Thus, when probe images of these fingers are acquired, each probe image is compared against the corresponding gallery image independently. The resulting set of scores can be consolidated to generate a single score (e.g., via the sum rule). However, in the case of mixing biometrics, images of a subject's fingers are mixed into a single image. This mixed image will be stored at the time of enrollment and during the authentication it will be matched against a single mixed probe image.

Although there are stated differences between mixing biometrics (as a concept) and multibiometrics fusion (as deployed systems), mixing biometrics is still a multibiometric fusion exercise by definition [31]. We believe that mixing biometrics extends and boosts the biometrics concept in general, and the multibiometrics fusion concept in particular. Therefore, in this thesis, we will introduce different approaches in order to mix different biometric traits.

1.5 Thesis Contributions

In this thesis, we explore the possibility of generating a biometric template that inherits its characteristics from different individuals or instances. This section provides an overview of the

thesis organization and approaches designed to accomplish our research objective.

In Chapter 2 we will discuss the use of fingerprints, faces and irises as biometrics. The purpose of this chapter is to give a brief introduction to biometric traits that have been utilized in the thesis. The reader can skip this chapter without any loss of continuity.

In Chapter 3 we describe a method to protect the privacy of fingerprint templates by mixing images to generate a cancelable fingerprint image. To mix two fingerprints, each fingerprint pattern is decomposed into two different components, viz., the continuous and spiral components by viewing the patterns as holograms. After pre-aligning the components of each fingerprint, the continuous component of one fingerprint is combined with the spiral component of the other fingerprint.

Chapters 4 and 5 present methods for mixing faces and irises, receptively, in order to generate joint identities that are similar to the original identities (as in scenario 2 in Section 1.3.1). The mixed face image is an intermediate face image in the morphing continuum between two faces and its position on this continuum is specified by the mixing parameters. In the case of iris, in order to mix two iris patterns, horizontal seams are copied from normalized iris images into a new iris image after sorting them based on their importance in the images.

In Chapter 6, the mixing concept is utilized in a different manner. Here, the mixed image corresponds to a true identity (and is not a virtual identity); however, the components of the mixed image are obtained from other identities. Therefore, we investigate the possibility of dithering a private face image into two host face images such that the private image can be revealed only when dithered host images are simultaneously available; at the same time, the individual dithered host images do not reveal the identity of the private image.

In Chapter 7, we extend the concept of mixing in order to mix instances of *different* biometric traits to obscure the original identity. Specifically, the goal here is generating a new mixed image that inherits its uniqueness from a finger impression and an iris image, i.e., a fingerprint image and an annular iris image are mixed in order to generate a fing'iris'print image. This mixed image incorporates characteristics from the original fingerprint impression and iris image, and can be used directly in the feature extraction and matching stages of an existing fingerprint system. To mix a fingerprint with an iris, the fingerprint is decomposed into two components, viz., the continuous and spiral phases, and iris minutiae is extracted in order to generate the iris spiral phase. Then, the continuous phase of the fingerprint is combined with the spiral phase of the

annular iris image.

In all cases, extensive experiments are conducted to convey the benefits and limitations of the proposed concepts.

The final chapter summarizes our contributions and provides suggestions for future work.

Chapter 2

Biometric Traits

2.1 Introduction

The purpose of this chapter is to give a brief introduction about different biometric traits, i.e., fingerprint, face, and iris, that have been discussed in the thesis.

2.2 From anthropometry to biometrics

In the nineteenth century, Alphonse Bertillon [1], a French policeman, was the first to introduce the science of identifying a person based on his/her anatomical features. To identify repeat offenders, Alphonse built a set of tools referred to in contemporary literature as the Bertillonage system. These tools were used to measure certain anatomical traits of a person including eleven different body measurements such as height, length, and breadth of the head, the width of cheeks, the length of different fingers, the length of forearms, etc. Figure 2.1 shows an illustration of the process for acquiring these measurements. These measurements were then recorded on an identity card (as shown in Figure 2.2) and/or manually compared to a record database to check if the same person was convicted before. The system was used until 1903, when it was replaced by fingerprint records. But a few elements of the Bertillon system exist even today in the criminal police identification process, such as the combination of profile and frontal shots, i.e., mug shots when photographing offenders (see Figure 2.3).

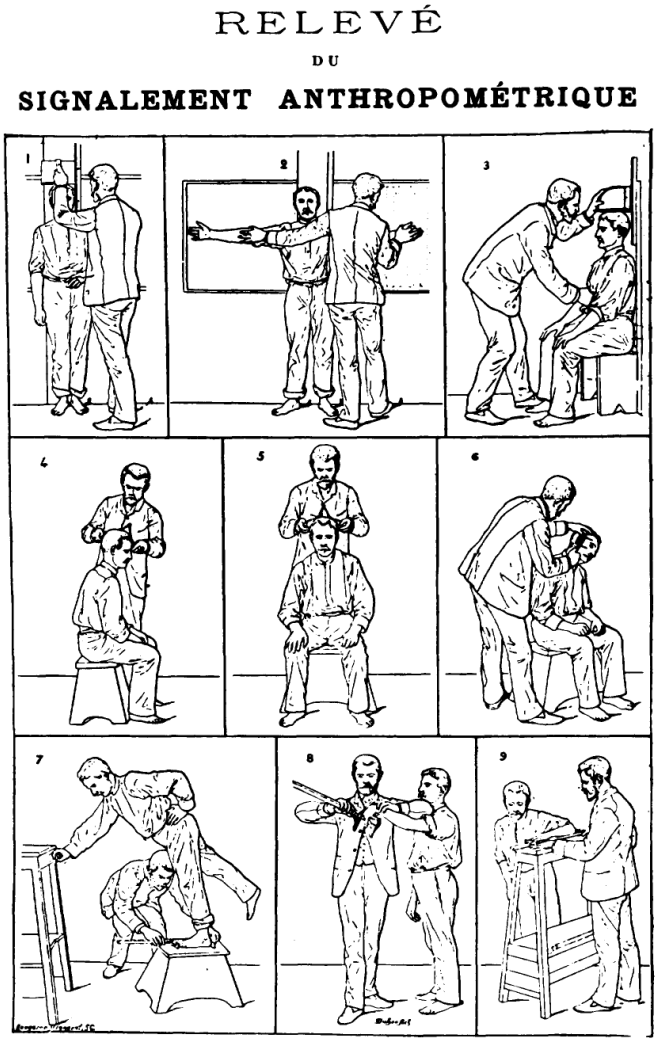


Figure 2.1: Anthropometry measurements used in Bertillonage identification system (taken from [1])

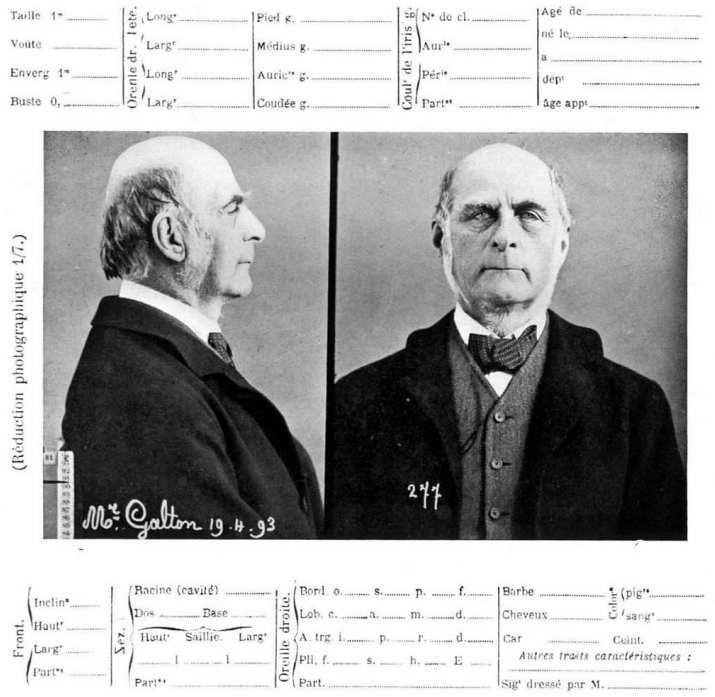


Figure 2.2: The ID card of Francis Galton as per the Bertillonage system (taken from [2]) created during Galton's visit to Bertillon's laboratory in 1893.

Figure 2.3: Mugshot of Alphonse Bertillon (taken from [3]).

2.3 Fingerprint as a biometric

The complexity of the Bertillonage system was the reason for providing criminal identification systems with accurate and reliable data, but it was also the reason for the system's downfall. Therefore, the supremacy of the Bertillon system began to fade in the face of a new (at that time) identification technique, i.e., fingerprint identification which was simpler to administer than the Bertillon anthropometry system. The use of fingerprints for establishing identity was started in the 16th century and thereafter replaced Bertillonage system as the world-wide standard for criminal identification.

A fingerprint refers to the flow of ridge patterns in the tip of the finger. The ridge flow exhibits irregularities in local regions of the fingertip termed as minutiae points (Figure 2.4). In 1892, Sir Francis Galton used the minutiae features for fingerprint matching. Since then, the distribution of these minutiae points along with the associated ridge structure has been believed to be distinctive to each fingerprint, and has been used in individual identification records in police offices.

Figure 2.4: A fingerprint image. The red circles represent some of the irregularities in the fingerprint,i.e.,the minutiae points.

Fingerprints recognition systems are considered to be a reliable method to recognize indi-

viduals and are used in different biometric applications, such as physical access control, border security, watch list, background check, and national ID systems.

2.3.1 Representation and matching

The uniqueness of a fingerprint is predominantly determined by the local ridge characteristics and their relationships, and matching fingerprints manually to claim that two impressions belong to the same person, requires complex protocols that have been used by examiners. Over the last three decades, research in fingerprint recognition has seen tremendous growth; however, most automatic fingerprint matchers follow similar protocols as human examiners and depend on the ridge characteristics of fingerprints. These characteristics (i.e., fingerprint features) can be organized in a hierarchical order [35] at three different levels. Level 1 features include the ridge flow, pattern type, external fingerprint shape, orientation image, and frequency image; level 2 features consist of minutiae location and orientation; and level 3 features consist of information available at higher resolution images, such as local shape of ridges, dots, pores and incipient ridges. On the basis of the described hierarchical order, fingerprint matching can be accomplished using three classes of matchers [35].

Level 1 features matchers

The matchers of this class compare the global pattern of ridges, e.g., correlation based matchers. During the matching procedures, the fingerprint or the global ridge orientation images are superimposed on each other and the correlation between the corresponding pixel intensities is computed for different alignments (e.g., various displacements and rotations). In general, it has been reported [35] that the level 1 features are useful for fingerprint classification and indexing, but not sufficient for fingerprint matching.

Level 2 features matchers

These are the most popular matchers whereby minutiae points are extracted from the fingerprint to be matched, and their location and ridge orientations are stored as a fingerprint template in a central database. The matching process determines the alignment between two minutiae sets that results in the maximum number of minutiae pairings. Some matchers utilize the level 1 features, such as texture information, local orientation, frequency and/or ridge pattern, along with

the extracted minutiae, to match two fingerprints.

Level 3 features matchers

This class of matchers is the least explored by researchers [35], compared to level 2 features matchers. This is due to two major reasons; (1) robust extraction of level 3 features (e.g., ridge shapes, sweat pores) requires high resolution images ($\geq$ 1,000 ppi - number of pixels per inch in the image) compared to 500 ppi, i.e., the current FBI standard [35]; and (2) even with availability of good quality images, these matchers require high computational complexity. These reasons has made the practicality of using these matchers for some commercial applications debatable. However, level 3 features play a significant role in latent fingerprint matching, where fingerprints are lifted from a surface prior to digitizing them.

2.4 Face as a biometric

Extracting intrinsic information from faces, such as identity, gender, ethnicity and age, is a task that humans perform routinely and efficiently. Therefore, the availability of powerful and low-cost computing systems has created an interest in developing automatic face recognition systems and deploying them in a number of applications, including biometric-based access systems. Automatic face recognition represents a challenging problem in the field of image analysis and computer vision. Thus, research in face recognition is striving to (a) solve fundamental challenges such as developing face matching methods that are invariant to age, pose, illumination, and facial expressions; (b) utilize the advances in technologies such as digital cameras and mobile devices to perform face recognition in new applications and scenarios; and (c) fulfill the increased demands on security in numerous practical applications where human identification is needed.

2.4.1 Representation and matching

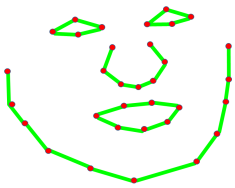
To identify a face in a digital image, the face recognition system should automatically find the faces in the image (if there is one), and then the recognition occurs by matching the detected face with the face template in a database. Just as in the case of fingerprints (see section 2.3), where ridge details were described in a hierarchical order at three different levels, Klare and Jain

[4] developed a hierarchical order for describing facial features (see Figure 2.5).

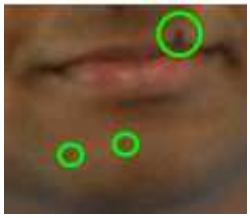
Level 1 features are the facial characteristics that can be observed from the general appearance of the face, such as skin color. Level 2 features are the localized characteristics of the face, such as the shape of the face and the relationship among the facial attributes. Finally, level 3 characteristics are the micro features that can be useful for the discrimination of monozygotic (i.e., identical) twins [61], such as facial marks.

(a) A face image

(b)Level 1 feature: skin color



(c) Level 2 feature: face shape



(d) Level 3 feature: face marks

Figure 2.5: Examples of the three levels of facial features (adopted from [4]).

Face matching is the process of measuring the similarity or dissimilarity between two face image based on the extracted features. Level 1 face features are quite analogous to level 1 fingerprint features. Hence, level 1 face features cannot accurately identify an individual over a large population of candidates. Similarly, as level 2 features of fingerprints, level 2 face features are the most discriminative features, and are predominantly used for face recognition approaches. There

are two broad categories of main approaches to match the detected face images [62]: appearance-based and feature-based methods. Appearance-based methods consider the global properties of the face image intensity pattern such as Principal Component Analysis (PCA), Linear Discriminant Analysis (LDA), and Independent Component Analysis (ICA). Feature-based methods are using local features of the face such as geometric relations between the facial features and local texture features of the face that are in variant to pose and lighting such as gradient orientations and local binary patterns (LBP). Meanwhile, Level 3 features contain unstructured, micro level features on the face that includes scars and facial marks. These features have been used along with level 2 features to identify monozygotic twins [63].

2.5 Iris as a biometric

Irises exhibit an extraordinary amount of textural details that are believed [64] to be different between individuals and between different eyes of the same individual. The texture of an iris can be simply described as a multilayered, tangled mesh-like structure, which imparts a highly complex texture to its surface. Figure 2.6 provides a close-up view of the texture of a sample iris. Compared with fingerprints, iris image data acquisition is usually non-invasive. Thus the iris has become one of the most reliable biometric traits for identity verification and recognition.

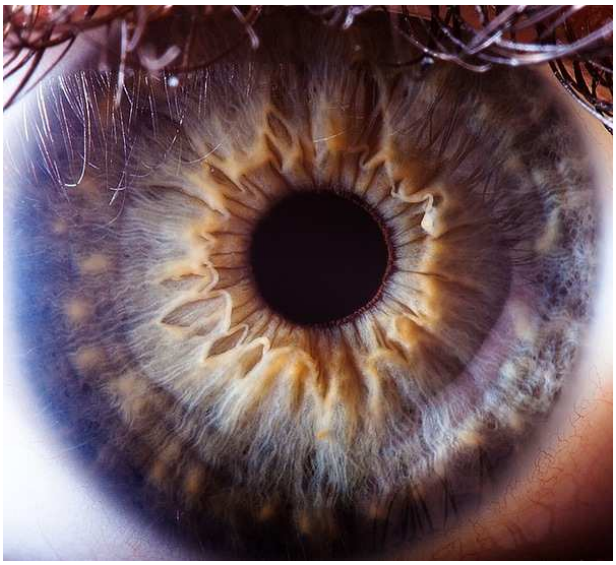


Figure 2.6: Close-up view of an iris, showing its complex texture. Image taken from [5].

2.5.1 Representation and matching

The texture of iris is formed by many interlacing minute characteristics such as pigment spots, stripes, furrows, crypts, etc. that are embedded on a stroma. [64]. Based on these features, the recognition takes place. But, prior to recognition, the iris region must first be localized and segmented from an image of the eye. Errors in the segmentation step will lead to poor performance due to the inclusion of noise (e.g. eyelashes, sclera, pupil, eyelids, and specular reflection) in the image.

Several iris representation techniques have been proposed in the literature [64, 65] and the matching is mainly based on the method of representation, i.e., the method used for encoding the iris texture. Thus, most existing techniques for iris recognition can be divided into two major classes. The first class represents the iris texture using filters or transforms [66], The second class of methods seeks to capture local and macro iris feature such as freckles, crypts, furrows, etc. in the spatial domain [67][68].

Daugman's phase encoding technique, which come under the first class, is the most common and promising among the different iris recognition approaches [64] [65] [69]. Figure 2.7 shows the processing chain of the traditional iris recognition system following Daugman's approach [70]. First, a camera acquires an image of an eye and the iris annular region is segmented, Next, the annular iris is geometrically normalized,i.e., unwrapped from raw image coordinates to polar coordinates. A texture filter is applied to the normalized iris image, and the filter responses are quantized into a binary representation (i.e., iris code). The comparison between two iris codes is done by computing the fractional HD as a dissimilarity measure.

2.6 Summary

In this chapter, we gave a brief introduction to three biometric traits, fingerprint, face and iris, which will be utilized in this thesis to generate joint identities. We discussed the different representation and matching schemes for these biometric traits. Recent research has resulted in the development of robust matchers for these modalities. Further, new cryptographic constructs have been proposed for these modalities [71]. For a more detailed description, the reader is referred to [14].

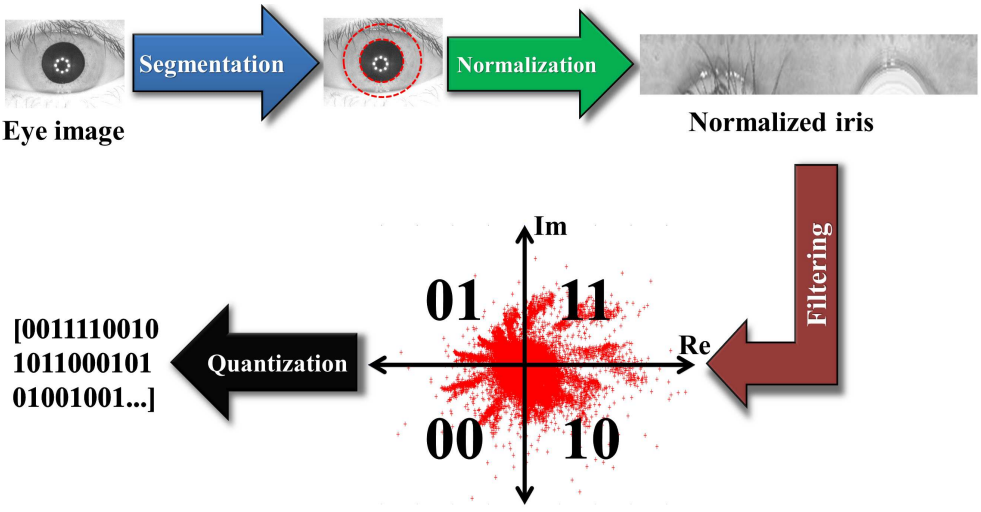


Figure 2.7: Diagram of Daugman's approach for encoding an iris image.

Chapter 3

Mixing Fingerprints

3.1 Introduction

In this dissertation, the proposed concept of generating joint identities by mixing biometrics of different individuals is introduced. Biometric images of different individuals are fused at the image level to generate a new biometric image. Image level fusion has been previously used in the context of fingerprints to combine multiple impressions of the same finger [35]. In this chapter, unlike previous work (see Section 1.4.2), two fingerprint impressions acquired from two *different* fingers are fused into a new fingerprint image resulting in a new identity*. The mixed image incorporates characteristics from both the original fingerprint images, and can be used directly in the feature extraction and matching stages of an existing biometric system. In the following, the major motivations behind the development of the proposed approach are discussed.

- The proposed approach explores the possibility of fusing images from distinct fingers at the image level and determining how this will affect authentication performance. For example, the proposed approach could be used to mix the prints of the thumb and the index fingers of a single individual, or index fingers of two different individuals, and generate a new fingerprint. Therefore, the concept of mixing fingerprints could be utilized in a multi-finger authentication system. This has benefits in terms of storage and security.

- Fingerprint mixing can be used to generate a large set of virtual identities. These virtual identities can be used to conceal the original identities of subjects or be used for large-scale

*Here, the term "identity" is used to suggest that the mixed fingerprint is unique and possibly different from other fingerprints.

evaluation of algorithms [72][35].

- De-identifying a fingerprint image is necessary to mitigate concerns related to biometric data sharing and data misuse [19][29][30]. Fingerprint mixing can be used to de-identify an input fingerprint image by fusing it with another fingerprint (e.g., from a different finger) at image level, in order to produce a new mixed image that obscures the identity of the original fingerprint. In [73] and [24] a similar approach has been proposed to preserve the privacy of fingerprints by fusing two distinct fingers but only at the feature level. Our proposed approach creates a new image that looks like a plausible fingerprint image and, thus, (a) it can be processed by conventional fingerprint algorithms and (b) an intruder cannot easily determine if a given print is mixed or not.

  The mixing process begins by decomposing each fingerprint image into two different components, viz., the continuous and spiral components (see Figure 3.1). The continuous component defines the local ridge orientation, and the spiral component characterizes the minutiae locations. Next, the two components of each fingerprint are aligned to a common coordinate system. Finally, the continuous component of one fingerprint is combined with the spiral component of the other fingerprint. This work confirmed that (a) the new fingerprint representing a new identity can potentially be used for authentication; (b) the proposed method can be utilized to generate different-sized databases of virtual identities from a fixed fingerprint dataset; (c) it can be used to obscure the information present in an individual's fingerprint image prior to storing it in a central database; and (d) it can be used to generate a cancelable template, i.e., the template can be reset if the mixed fingerprint is compromised. Since the proposed approach can be used for de-identifying fingerprints, in this chapter, a detailed analysis of the security aspects, i.e., the changeability and non-invertability properties of the mixing fingerprint approach has been included. This security analysis is based on metrics commonly used in the cancelable biometrics literature [27][28]. The rest of the chapter is organized as follows. Section 3.2 presents the proposed approach for mixing fingerprints. Section 3.3 reports the experimental results and Section 3.4 summarizes the chapter.

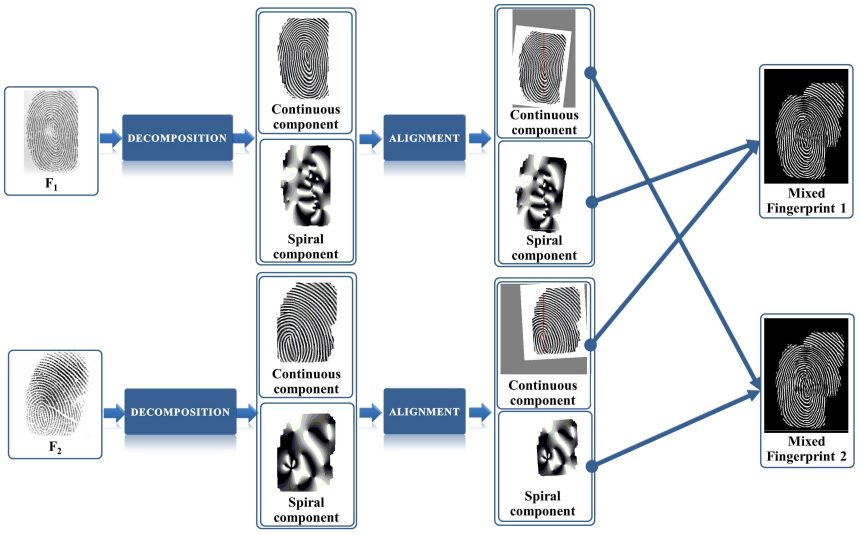


Figure 3.1: Proposed approach for mixing fingerprints

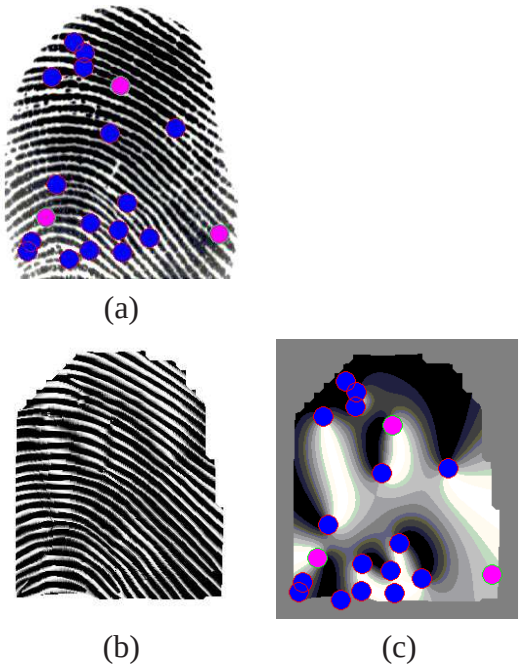
3.2 Mixing Fingerprints: The proposed approach

The ridge flow of a fingerprint can be represented as a 2D Amplitude and Frequency Modulated (AM-FM) signal [74]:

$$I(x,y) = a(x,y) + b(x,y)cos(\Psi(x,y)) + n(x,y), \tag{3.1}$$

where $I(x,y)$ is the intensity of the original image at (x,y), $a(x,y)$ is the intensity offset, $b(x,y)$ is the amplitude, $\Psi(x,y)$ is the phase and $n(x,y)$ is the noise. Based on the Helmholtz Decomposition Theorem [75], the phase can be uniquely decomposed into the continuous phase and the spiral phase, $\Psi(x,y) = \psi_c(x,y) + \psi_s(x,y)$. As shown in Figure 3.2, the cosine of the continuous phase, i.e., the continuous component $cos(\psi_c(x,y))$, defines the local ridge orientation, and the cosine of the spiral phase, i.e., the spiral component $cos(\psi_s(x,y))$, characterizes the minutiae locations. Let $\phi(x,y)$ denote the spiral phase of a local region in a fingerprint. Assume that the function $\phi(x,y)$ monotonically changes from 0 to 2π around a particular point, (x_n, y_n), and has a characteristic jump from 0 to 2π at the point (x_n, y_n). This forms a residue at (x_n, y_n) with an associated polarity, $p_n \in \{-1, 1\}$. A residue with positive (negative) polarity is referred to as a positive (negative) spiral.

$$\phi(x,y) = p_n \tan^{-1}((x - x_n)/(y - y_n)). \tag{3.2}$$



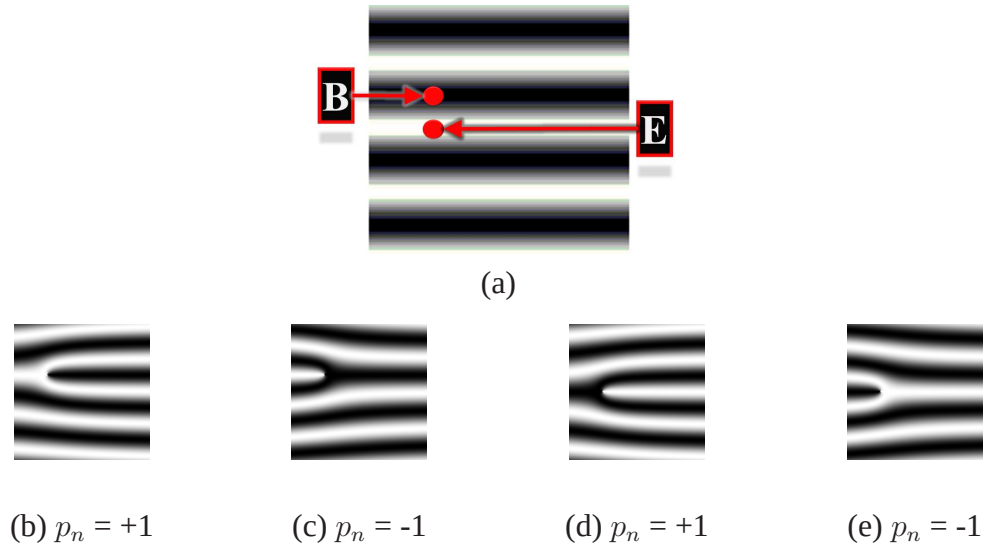
(a) (b) (c)

Figure 3.2: Decomposing a fingerprint. (a) A fingerprint image. (b) Continuous component, $\cos(\psi_c(x,y))$. (c) Spiral component, $\cos(\psi_s(x,y))$. The blue and pink dots represent ridge endings and ridge bifurcations, respectively.

Appending this function to the continuous phase will cause a phase jump at (x_n, y_n) resulting in a minutia. In Figure 3.3, a local ridge pattern is generated based on the continuous phase function $2\pi fy$, with $f = 4$. Depending upon the polarity value (+1 or -1), a minutia is generated on the ridge pattern. The relation between the polarity, p_n, and the occurrence of ridge ending or bifurcation is dependent on the gradient direction of the cosine of the continuous phase. Hence, the spiral phase allows for an abrupt change in the local fringe density by either inserting or deleting a ridge based on the polarity and the appending location within the continuous phase. If the simple function in (3.2) is replaced by a sum of such functions, the spiral phase, $\psi_s(x,y)$, will correspond to a set of minutiae:

$$\psi_s(x,y) = \sum_{n=1}^{N} p_n \tan^{-1}((x-x_n)/(y-y_n)), \tag{3.3}$$

where x_n and y_n denote the coordinates of the n^{th} minutia, and N denotes the total number of minutiae. Moreover, the type of a minutia (ending or bifurcation) is determined by its polarity $p_n \in \{-1, 1\}$. Thus, based on this 2D AM-FM representation, the fingerprint's oriented patterns can be uniquely decomposed into (a) a small number of topologically



(a)

(b) p_n = +1 (c) p_n = -1 (d) p_n = +1 (e) p_n = -1

Figure 3.3: Generating minutia in a fringe pattern. (a) Gray scale image of continuous phase given by $\cos(2\pi fy)$. (b) and(c) Appending a minutia at "B". (d) and (e) Appending a minutia at "E".

distinct discontinuities, i.e., the spiral phase, and (b) a well defined smooth flow field, i.e., the continuous phase.

3.2.1 Fingerprint Decomposition

Decomposing images into semantic parts is of great interest in many applications such as compression, enhancement, restoration, and more. Therefore, this task has drawn a lot of research attention and most of the proposed approaches are utilizing total variational calculus. These methods are inspired by the total variation (TV) regularization for image denoising and restoration [76]. The separation is done by decomposing the image into texture and non-texture (or cartoon) components, as shown in Figure 3.4. So this kind of image decomposition can be useful for image compression where compressing the cartoon and the texture components separately can provide better results, image denoising where zero mean oscillatory noise can be regarded as a fine texture, image feature selection, etc.

But these methods are suggested for textures with no prior knowledge about it, meanwhile, in order to decompose a biometric image into its component structures, understanding the non-linear nature of the image and the source of its distinctiveness and individuality will be beneficial.

(a)

(b) (c)

Figure 3.4: Cartoon-texture decomposition using a total variation method [6]. (a) A fingerprint image. (b) Cartoon image. (c) Texture image.

Therefore, we found that the Larkin et al.'s hologram model [77] (check Equation 3.1), i.e., a phase modulated fringe pattern to represent the fingerprint images can be the suitable method to decompose fingerprint images. Larkin et al.'s work [77][74] is the culmination of several years of investigating mathematical methods for demodulation of optical interferograms that have fringe pattern such as fingerprint images.

The hologram representation of fingerprint is an adaptive and data-driven approach in comparison to traditional representation such as the Fourier or wavelet methods where a predefined decomposition basis is used. Moreover, the frequency representation fails to work properly because there is an infinite singularity at each minutiae point. On the other hand, the hologram phase circumvents the infinite frequency singularities that always occur at minutiae in the phase estimation step.

Since ridges and minutiae can be completely determined by the phase [74] $\Psi(x, y)$. The other three parameters in Equation (3.1) contribute to the realistic textural appearance of the fingerprint. Before fingerprint decomposition, the phase $\Psi(x, y)$ must be reliably estimated; this is termed as demodulation.

Vortex demodulation

The objective of vortex demodulation [77] is to extract the amplitude $b(x, y)$ and phase $\Psi(x, y)$ of the fingerprint pattern. First, the DC term $a(x, y)$ has to be removed since the failure to remove this offset correctly may introduce significant errors in the demodulated amplitude and phase [77]. To facilitate this, a normalized fingerprint image, $f(x, y)$, containing the enhanced ridge pattern of the fingerprint (generated by the VeriFinger SDK[†]) is used. From Equation (3.1), $f(x, y) = I(x, y) - a(x, y) \simeq b(x, y)cos(\Psi(x, y))$. The vortex demodulation operator $\mathbf{V}$ takes the normalized image $f(x, y)$ and applies a spiral phase Fourier multiplier $\exp[i\Phi(u, v)]$:

$$\begin{aligned} \mathbf{V}\{f(x,y)\} &= F^{-1}\{\exp[i\Phi(u,v)].F\{b(x,y).\cos[\Psi(x,y)]\}\} \\ &\cong -i\exp[i\beta(x,y)].b(x,y).\sin[\Psi(x,y)] \end{aligned} \tag{3.4}$$

where, F is the Fourier transform, F^{-1} is the inverse Fourier transform and $\exp[i\Phi(u, v)]$ is a 2-D signum function [77] defined as a pure spiral phase function in the spatial frequency space (u, v):

$$\exp[i\Phi(u,v)] = \frac{u+iv}{\sqrt{u^2+v^2}}. \tag{3.5}$$

Note that in Equation (3.4) there is a new parameter, $\beta(x, y)$, representing the perpendicular direction of the ridges. In Equation (3.6), this directional map is used to isolate the desired magnitude and phase from Equation (3.4), i.e.,

$$-\exp[-i\beta(x,y)].\mathbf{V}\{f(x,y)\} = ib(x,y).\sin[\Psi(x,y)]. \tag{3.6}$$

Then, Equation (3.6) can be combined with the normalized image, $f(x, y)$, to obtain the magnitude $b(x, y)$ and the raw phase map $\Psi(x, y)$ as follows:

$$-\exp[-i\beta(x,y)].\mathbf{V}\{f(x,y)\} + f(x,y) = b(x,y).\exp(i\Psi(x,y)). \tag{3.7}$$

Therefore, determining $\beta(x, y)$ is essential for obtaining the amplitude and phase functions, $b(x, y)$ and $\Psi(x, y)$, respectively. The direction map $\beta(x, y)$ can be derived from the orientation image of the fingerprint by a process called unwrapping. A sophisticated

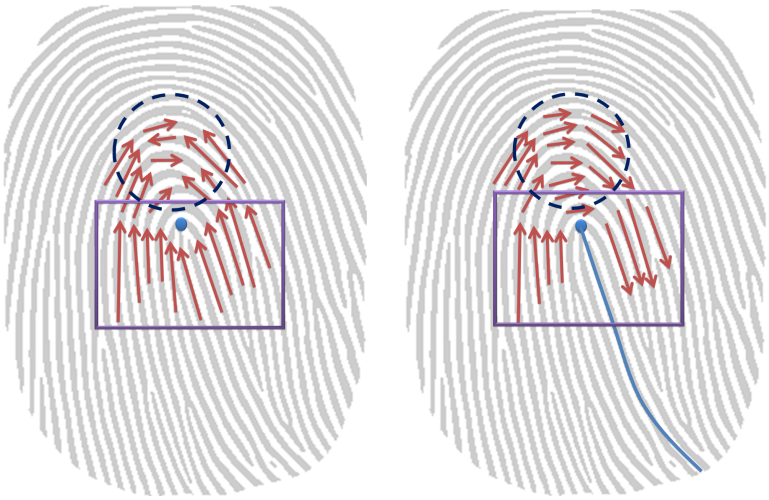
[†]http://www.neurotechnology.com

unwrapping technique using the topological properties of the ridge flow fields is necessary to account for direction singularities such as cores and deltas [74] [23].

Direction Map $\beta(x, y)$

Direction is uniquely defined in the range 0° to 360° (modulo 2π). In contrast, fingerprint ridge orientation is indistinguishable from that of a 180° rotated ridge (modulo π). Therefore, the fingerprint's *orientation* map, denoted by $\theta(x, y)$, should be unwrapped to a *direction* map, $\beta(x, y)$ [74]. Phase unwrapping is a technique used to address a 2π phase jump in the orientation map. The unwrapping process adds or subtracts an offset of 2π to successive pixels whenever a phase jump is detected [75]. This process proceeds by starting at any pixel within the orientation image and using the local orientation information to traverse the image pixel-by-pixel, and assigning a direction (i.e., the traversed direction) to each pixel with the condition that there are no discontinuities of 2π between neighboring pixels. However, the presence of flow singularities means that there will be pixels in the orientation image with a discontinuity of $\pm 2\pi$ in the traversed direction and, therefore, the above unwrapping technique will fail. In fingerprint images, such flow singularities arise from the presence of singular points such as core and delta. Figure 3.5(a) illustrates that estimating the direction of ridges in the vicinity of a core point by starting at any point within the highlighted rectangle and arbitrarily assigning one of two possible directions, can result in an inconsistency in the estimated directions inside the dashed circle. This inconsistency in the estimated direction map can be avoided by using a branch cut [75]. The branch cut is a line or a curve used to isolate the flow singularity and which cannot be crossed by the paths of the unwrapping process. Consequently, branch cut prevents the creation of 2π discontinuities and restores the path independence of the unwrapping process. As shown in Figure 3.5(b), tracing a line down from the core point and using this line as a barrier resolves the inconsistency near the core point (i.e, inside the dashed circle) by selecting two different directions in each side of the branch cut within the same region (i.e, inside the highlighted rectangle). In our work, a strategy based on the techniques described in [74] [7] [23] has been adapted to estimate the direction map $\beta(x, y)$, which is summarized in the following three steps.

1. The orientation image $\theta(x, y)$ of the normalized fingerprint $f(x, y)$ is determined via the



(a) (b)

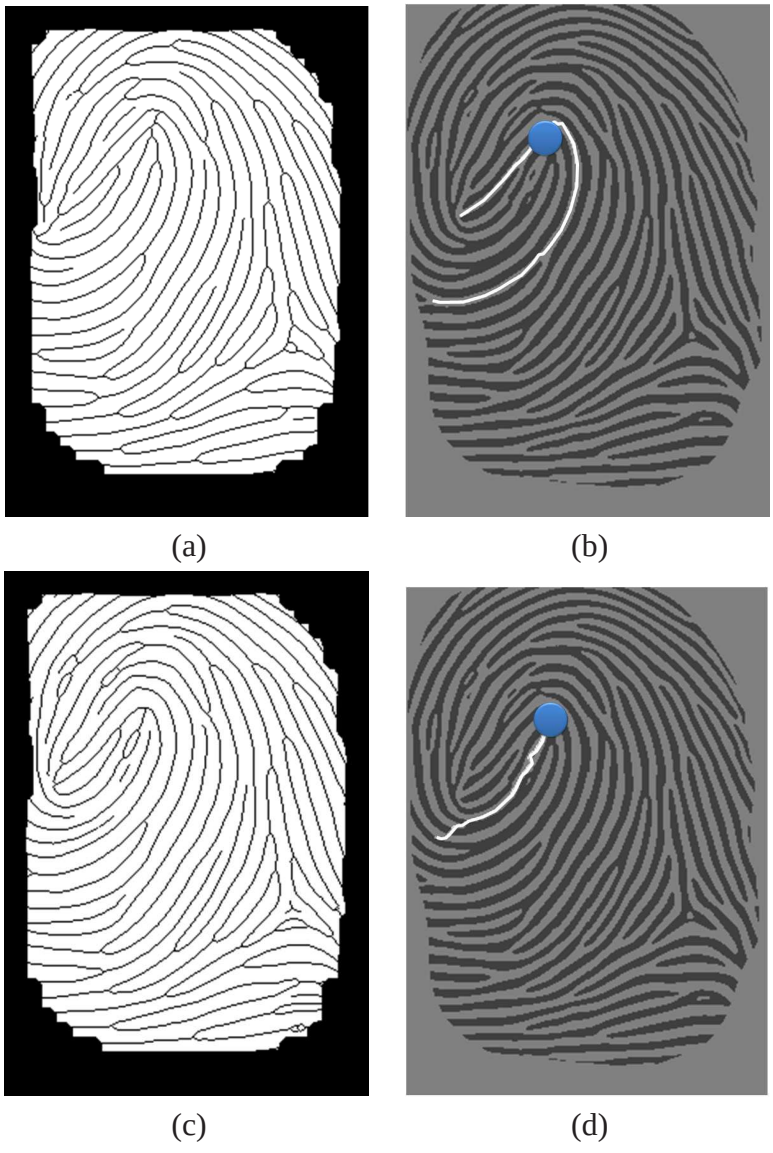
Figure 3.5: A portion of the estimated direction map (a) before assigning a branch cut and (b) after assigning a branch cut [7].

least mean-square method [78]. Then the Poincaré [35] index is used to locate the singular points, if any.

2. In case there are singular points, an algorithm is applied to extract the branch cuts along suitable paths such as ridge contours, as shown in Figure 3.5(b), to resolve the inevitable direction ambiguities near those singularities. The branch cuts are extracted by tracing the contours of ridges (rather than the orientation field) in the skeleton images. The algorithm starts from each singular point in a skeleton image until the trace reaches the border of the segmented foreground region of the fingerprint or when it encounters another singular point. To generate the skeleton images, first, a set of smoothed orientation maps are generated by applying a Gaussian smoothing operation at different smoothing scales ($\sigma \in \{1, 2, 3, 5, 10, 15, 20, 32, 50, 64\}$) on $\theta(x, y)$. Next, a set of Gabor filters, tuned to the smoothed orientation maps [78], is convolved with the normalized image $f(x, y)$. Then, a local adaptive thresholding and thinning algorithm [79] is applied to the directionally filtered images producing 10 skeleton images. Thus, there are at least 10 branch cuts and the shortest one, associated with each singular point, is selected and Figure 3.6 shows two examples of skeleton images and the corresponding branch cuts of a core point. Figure 3.7 shows examples of the branch cuts extracted from the singular points of different fingerprints.

3. The phase unwrapping algorithm [80] [75] starts from any arbitrary pixel in the orienta-

tion map $\theta(x, y)$ and visits the other pixels, which are unwrapped in the same manner as in images without singularity, with the exception here that the branch cuts cannot be crossed. Then, each branch cut is visited individually and its pixels are traced and unwrapped.



(a) (b)

(c) (d)

Figure 3.6: Examples of skeleton images and branch cuts for a singular point where (a) and (c) are skeleton images generated with σ = 3 and 32, respectively and (b) and (d) are the corresponding branch cuts. Branch cut in (d) is the selected one.

Finally, the direction map $\beta(x, y)$ is determined from the unwrapped $\theta(x, y)$ by adding $\pi/2$ which allows for the determination of the amplitude $b(x, y)$ and phase $\Psi(x, y)$ modulations of fingerprint image from Equation (3.7). A flowchart for demodulating a fingerprint image is depicted in Figure 3.8.

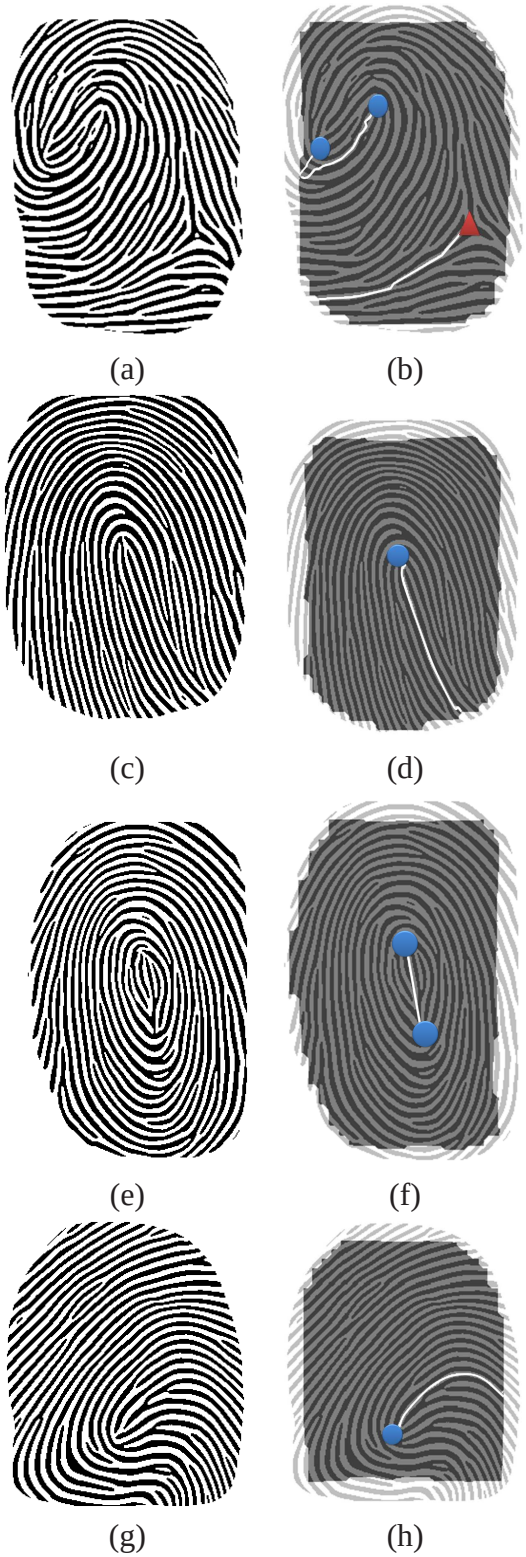


Figure 3.7: Examples of fingerprints with singular points (The blue dots and red triangle represent cores and delta, respectively). (a), (c), (e), and (g) The normalized fingerprints. (b), (d), (f), and (h) The extracted branch cuts obtained by tracing the ridges instead of the orientation field.

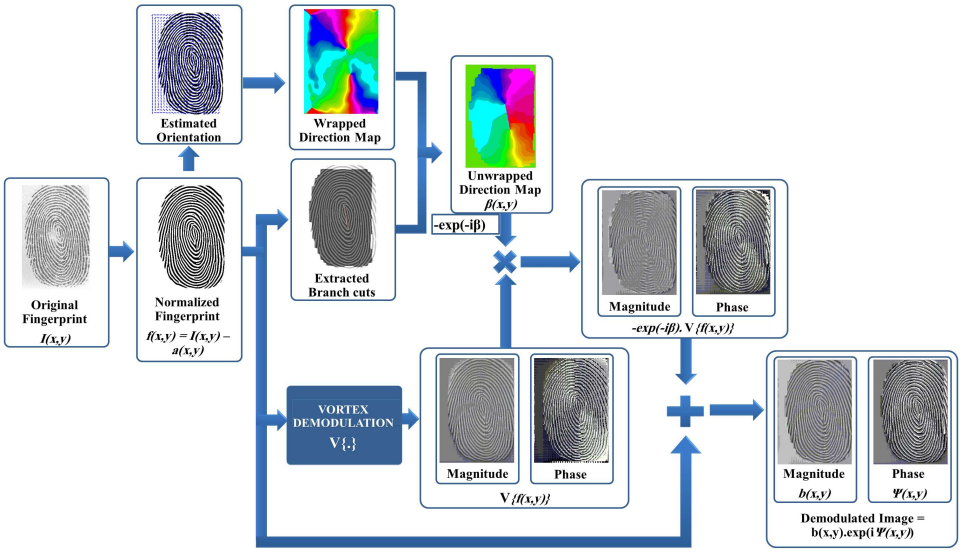


Figure 3.8: Flowchart for demodulating a fingerprint image.

Helmholtz Decomposition

The Helmholtz Decomposition Theorem [75] is used to decompose the determined phase $\Psi(x, y)$ of a fingerprint image into two phases. The first phase, ψ_c is a continuous one, which can be unwrapped, and the second is a spiral phase,ψ_s, which cannot be unwrapped but can be defined as a phase that exhibits spiral behavior at a set of discrete points in the image. The Bone's residue detector [81] [75] is first used to determine the spiral phase $\psi_s(x, y)$ from the demodulated phase $\Psi(x, y)$. Next the continuous phase, is computed as $\psi_c(x, y) = \Psi(x, y) - \psi_s(x, y)$. Finally, although subtracting the spiral phase from the phase should results in a continuous phase with no discontinuities, due to the inevitable quantization errors in the subtracting operation, it is essential to unwrap the continuous phase again by using the branch cuts from the previous step. Figure 3.9 illustrates the steps to determine the continuous component $cos(\psi_c(x, y))$ (Figure 3.9(h)) from the estimated spiral component $cos(\psi_s(x, y))$ (Figure 3.9(f)) of a fingerprint and the demodulated phase $\Psi(x, y)$ (Figure 3.9(a)).

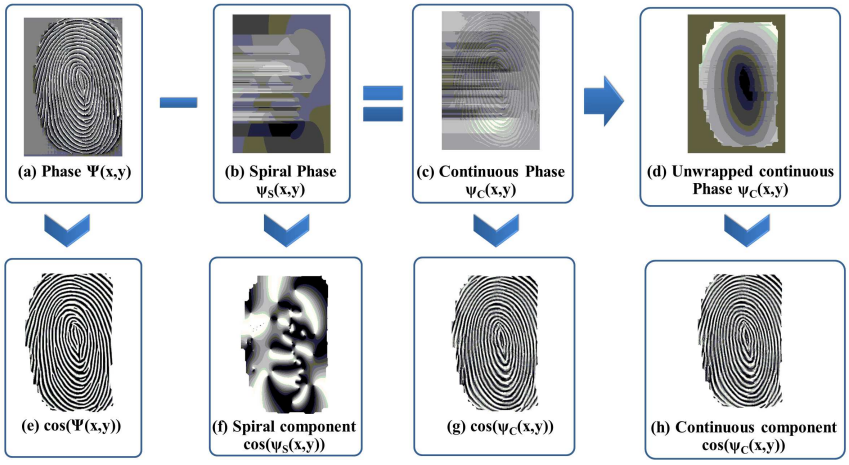


Figure 3.9: Determining fingerprint constituents from (a) the demodulated phase $\Psi(x, y)$. (b) Spiral Phase $\psi_s(x, y)$. (c) Continuous Phase $\psi_c(x, y)$. (d) Unwrapped continuous Phase. (e), (f), (g) and (h) are the cosine (according to the hologram modal representation of fringe pattern, as explained in Equation 3.1) of (a), (b), (c) and (d), respectively.

3.2.2 Fingerprint Pre-alignment

To mix two different fingerprints after decomposing each fingerprint into its continuous component $cos(\psi_c(x, y))$ and spiral component $cos(\psi_s(x, y))$, the fingerprints themselves should be appropriately aligned. Previous research has shown that two fingerprints can be best aligned using their minutiae correspondences. However, it is difficult to ensure the existence of such correspondences between two fingerprints acquired from different fingers. In this work, the components are pre-aligned to a common coordinate system prior to the mixing step by utilizing a reference point and an alignment line. The reference point is used to center the components. The alignment line is used to find a rotation angle about the reference point. This angle rotates the alignment line to make it vertical. The two phase components of each fingerprint are rotated by the same angle.

Locating a reference point

The reference point used in this work is the northern most core point of extracted singularities. For plain arch fingerprints or partial fingerprint images, Novikov et al.'s technique [82] [21], based on the Hough transform, is used to detect the reference point.

Finding the alignment line

The first step in finding the alignment line is to extract high curvature points from the skeleton of the fingerprint image's continuous component. Next, horizontal distances between the reference point and all high curvature points are calculated. Then, based on these distances, an adaptive threshold is applied to select and cluster points near the reference point. Finally, a line is fitted through the selected points to generate the alignment line. Figure 3.10 shows the steps to find the reference point and the alignment line by utilizing the continuous phase component of an arch fingerprint. Since the continuous component of a fingerprint is a global feature of the fingerprint pattern and is not affected by breaks and discontinuities which are commonly encountered in ridge extraction, the determined reference point and alignment line are consistence and do not reveal any information about the minutia attributes which are local characteristics in the fingerprint.

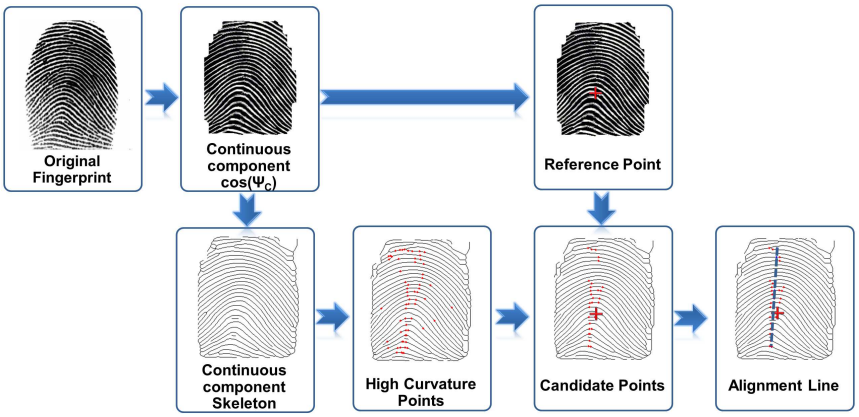


Figure 3.10: Finding the reference point and alignment line for an arch fingerprint.

3.2.3 Mixing Fingerprints

Let F_1 and F_2 be two different fingerprint images from different fingers, and let $\psi_{ci}(x, y)$ and $\psi_{si}(x, y)$ be the pre-aligned continuous and spiral phases, $i = 1, 2$. As shown in Figure 3.1, there are two different mixed fingerprint image that can be generated, MF_1 and MF_2:

$$\begin{aligned} MF_1 &= \cos(\psi_{c2} + \psi_{s1}), \\ MF_2 &= \cos(\psi_{c1} + \psi_{s2}). \end{aligned} \tag{3.8}$$

The continuous phase of F_2 (F_1) is combined with the spiral phase of F_1 (F_2) which generates a new fused fingerprint image MF_1 (MF_2).

3.2.4 Compatibility Measure

Variations in the orientations and frequencies of ridges between fingerprint images can result in visually unrealistic mixed fingerprint images, as shown in Figure 3.11. This issue can be mitigated if the two fingerprints to be mixed are carefully chosen using a compatibility measure. In this work, the compatibility between fingerprints is computed using non-minutiae features, viz., orientation fields and frequency maps of fingerprint ridges. Figure

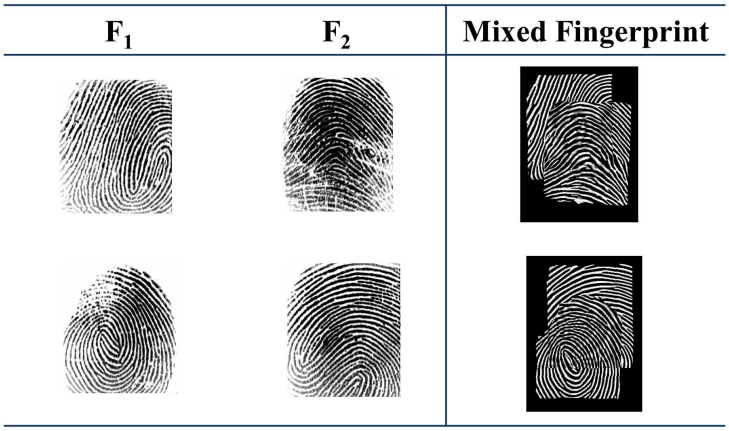
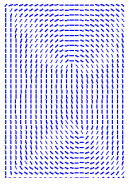


Figure 3.11: Examples of mixed fingerprints that look unrealistic.

(a) Fingerprint Image



(b) Orientation Field (c) Frequency Map

Figure 3.12: Orientations and frequencies of the ridges of a fingerprint image.

3.12 shows the orientation and frequency images were computed from the pre-aligned continuous component of a fingerprint using the technique described in [78]. Then, Yager and Amin's [83] approach is used to compute the compatibility measure. To compute the compatibility between two fingerprint images, their orientation fields and frequency maps are first estimated (see below). Then, the compatibility measure C between them is computed as the weighted sum of the normalized orientations and frequency differences, OD and FD, respectively:

$$C = 1 - (\alpha.OD + \gamma.FD), \tag{3.9}$$

where α and γ are weights that are determined empirically. Figure 3.13 shows examples of mixed fingerprints after utilizing the compatibility measure to select the fingerprints pairs, (F_1, F_2). Perfect compatibility (C = 1) is likely to occur when the two prints to be mixed are from the same or the look-alike finger - a scenario that is *not* applicable in the proposed application. On the other hand, two fingerprints having significantly different ridge structures are unlikely to be compatible (C = 0) and will generate an unrealistic looking fingerprint. Between these two extremes (see Figure 3.14), lies a range of possible compatible values that is acceptable. However, determining this range automatically may be difficult.

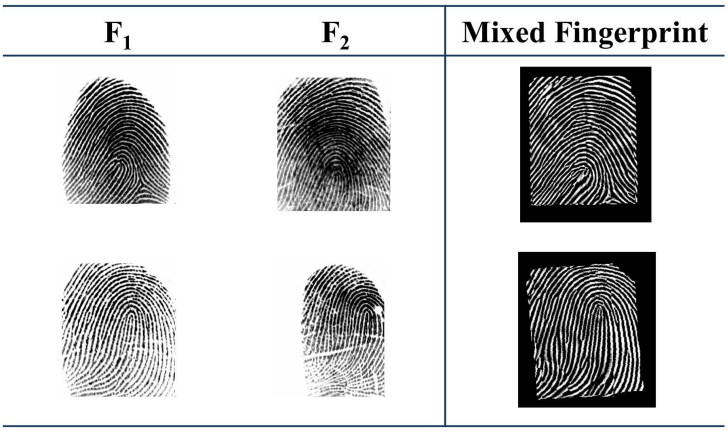


Figure 3.13: Examples of mixed fingerprints that appear to be visually realistic.

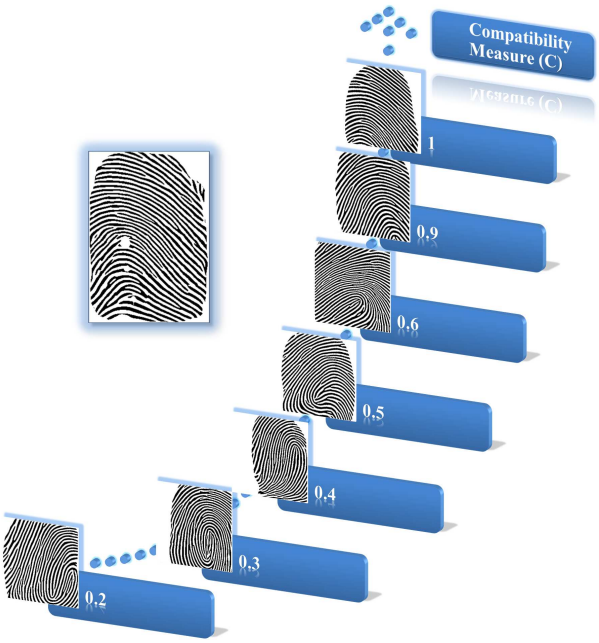


Figure 3.14: Examples of a fingerprint image and its compatibility measure with other images.

Orientation Field Difference (OD)

The difference in orientation fields between F_1 and F_2 is computed as

$$OD = \left(\frac{1}{|S|}\right) \sum_{(x,y)\in S} d(\theta_1(x,y), \theta_2(x,y)), \tag{3.10}$$

where S is a set of coordinates within the overlapped area of the aligned continuous components of two different fingerprints, and θ_1 and θ_2 represent the orientation fields of the two fingerprints. If orientations are restricted to the range $[-\pi/2, \pi/2]$, the operator $d(.)$ is written as

$$d(\alpha,\gamma) = \begin{cases} \pi - (\alpha - \gamma), & \text{if } \frac{\pi}{2} < \alpha - \gamma \\ |\alpha - \gamma|, & \text{if } -\frac{\pi}{2} < \alpha - \gamma < \frac{\pi}{2} \\ \pi + (\alpha - \gamma), & \text{if } \alpha - \gamma \leq -\frac{\pi}{2}. \end{cases} \tag{3.11}$$

Frequency Map Difference (FD)

Local ridge frequencies are the inverse of the average distance between ridges in the local area in a direction perpendicular to the local orientation. Hong et al.'s approach [78] is used to find the local ridge frequencies of the continuous component of a fingerprint image. The

difference function is computed as :

$$FD = \left(\frac{1}{|S|}\right) \sum_{(x,y)\in S} |Freq_1(x,y) - Freq_2(x,y)|, \tag{3.12}$$

where S is a set of coordinates within the overlapped area, and $Freq_1$ and $Freq_2$ represent the frequency maps of the two fingerprints F_1 and F_2, respectively.

3.3 Experiments and Discussion

The performance of the proposed fingerprints mixing approach was tested using two different datasets. The first dataset was taken from the West Virginia University (WVU) multimodal biometric database [84]. A subset of 1000 images corresponding to 500 fingers (two impressions per finger) was used. The second dataset was the FVC2002 DB2 fingerprint database containing 110 fingers with 8 impressions per finger (a total of 880 fingerprints). The VeriFinger SDK was used to generate the normalized fingerprint images and the matching scores. Also, an open source Matlab implementation [85] based on Hong et al.'s approach [78] was used to compute the orientation and frequency images of the fingerprints. In order to establish the baseline performance, for each finger in each dataset, an impression was used as a probe image and another impression was added to the gallery. This resulted in a rank-1 accuracy of $\sim$ 100% for the WVU dataset and $\sim$ 100% for the FVC2002 dataset. The EERs for these two datasets were 0.5% and 0.2%, respectively. In the following subsections, two set of experiments are discussed. These experiments investigate if the new approach for image level fusion can be utilized to (a) generate a new identity by mixing two distinct fingerprints and (b) de-identify a fingerprint by mixing it with another fingerprint. Although they have some common experiment routines, the used dataset and the objectives are different.

Computational time We evaluated the time complexity of the approach using $Matlab^{®}$-2013a on a PC with $Intel^{®}$ i7 CPU @2.8GHz and 8GB memory. As shown in Figure 3.1, there are three main steps for mixing fingerprints: Decomposition, Alignment, and Mixing. Table 3.1 shows the elapsed time of each step.

3.3.1 Generating Joint Identities

The purpose of the following set of experiments was to report the matching performance of mixing images of two different fingers pertaining to two different individuals from the WVU dataset to generate joint identities.Therefore, the following experiments were designed in order to address the following questions:

1. What impact does mixing fingerprints have on the matching performance, i.e., can two mixed impressions pertaining to the same new identity be successfully matched?

2. Are the original fingerprints and the mixed fingerprint correlated? It is essential to assure that the proposed approach generates a new fingerprint that is dissimilar from the original fingerprints

3. How many virtual identities can be generated from a fixed fingerprint dataset with an acceptable recognition rate?

For each finger in the WVU dataset, one impression was used as the probe image and the other was added to the gallery resulting in a probe set P and a gallery set G each containing 150 fingerprints.

– **Experiment A-1:** In this experiment, the performance of generating new identities by mixing random pairs of fingers is reported. Pairs of fingerprints in P were *randomly* paired and mixed resulting in a new probe set MF_1^P consisting of 250 fingerprints. The corresponding pairs of fingerprints in G were also mixed resulting in a new gallery set MF_1^G consisting of 250 impressions. Since, mixing is an asymmetric process (Equation (3.8)), another probe set MF_2^P and gallery set MF_2^G were also generated. Matching images in MF_1^P against those in MF_1^G and MF_2^P against MF_2^G resulted in a rank-1 accuracy of $\sim$ 68% and an EER of $\sim$ 15%. The low identifi-

Table 3.1: Elapsed time of mixing two fingerprint images as shown in Figure 3.1

Task	Time (seconds)
Decomposition	10
Alignment	4
Mixing	0.001
Total	14.001

cation rate is due to the random pairing of fingers which lead to visually unrealistic fingerprint images (see Figure 3.11).

– **Experiment A-2:** The purpose of this experiment is to enhance the identification rate of Experiment A-1 by mixing fingers based on the compatibility measure. Therefore, the compatibility measures between different pairs of fingerprints in P were computed using Equation (3.9) with $\alpha = 0.7$ and $\gamma = 0.3$. The finger pairs to be mixed were selected based on this measure. Pairs were selected and mixed in decreasing order of their compatibility measures resulting in probe sets MF_1^P and MF_2^P, and gallery sets MF_1^G and MF_2^G. Figure 3.15 shows examples of the mixed fingerprints from the WVU dataset. Matching images in MF_1^P against those in MF_1^G and images in MF_2^P against those in MF_2^G resulted in a rank-1 accuracy of $\sim$ 85% and an EER of $\sim$ 6%. As shown in Figures 3.11, 3.13, and **??**, the compatibility measure assists the mixing approach in generating visually appealing mixed fingerprints with less false minutia in the overlapping area.

– **Experiment A-3:** It is essential to assure that the new identities are dissimilar from the original fingers. Therefore, in this experiment, MF_1^P and MF_2^P, generated in Experiment A-2, are matched against F_1^P and F_2^P in P (as in Experiment A-2, F_1^P and F_2^P are paired and mixed based on the compatibility measures, and MF_1^P and MF_2^P are the resulting mixed fingerprints).

a. Matching MF_1^P (MF_2^P) against F_1^P (F_2^P) resulted in rank-1 accuracy of $\sim$ 52% and EER of $\sim$ 25%.

b. Matching MF_1^P (MF_2^P) against F_2^P (F_1^P) resulted in rank-1 accuracy of $\sim$ 38% and EER of $\sim$ 46%.

The poor matching performance indicates that the original fingerprints are different from newly generated mixed fingerprints. In other words, the original identity cannot be easily deduced from the mixed image and the new mixed fingerprint may be viewed as a cancelable fingerprint. However, in matching scenario "a", the reduction in the dissimilarity between original and mixed fingerprints is because MF_1^P (MF_2^P) and F_1^P (F_2^P) have the same minutia locations as shown in Figure 3.1 and Equation (3.8). This commonality of minutia locations leads to high similarity scores between original and virtual identities. Ridge features, e.g., ridge length and ridge curvature,

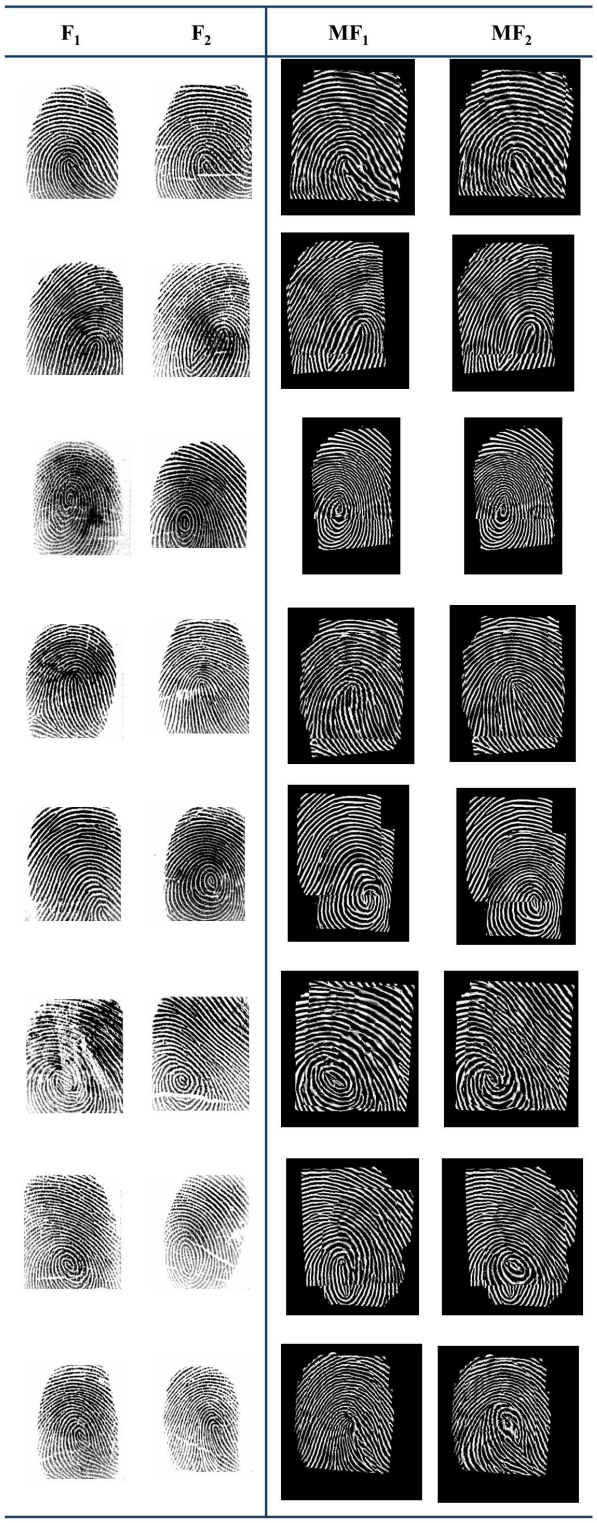


Figure 3.15: Examples of mixing fingerprint pairs from the WVU dataset.

can be used along with conventional minutia features to address the commonality of minutia locations between MF_1^P (MF_2^P) and F_1^P (F_2^P).

– **Experiment A-4:** In this experiment, the possibility of utilizing the proposed approach to mix the prints from the two fingers of a subject to create a single new fingerprint is investigated. The new identity is a result of fusing images of the thumb and the index fingers of a single individual. For this experiment, the data corresponding to both the left thumb and left index finger of 150 subjects from the WVU database were used. There were two impressions available for each finger. Each left thumb impression was mixed with the corresponding left index finger resulting in two mixed fingerprint impressions for each subject. One of these mixed impressions was used as a probe and the other was added to the gallery set. The obtained rank-1 accuracy was $\sim$ 81% and the EER was $\sim$ 9% suggesting the possibility of designing a new multi-finger authentication scheme for access control. Here, only the mixed impression needs to be stored in the database (as opposed to images of individual fingers).

– **Experiment A-5:** Mixing fingerprints generates new fused fingerprints, i.e., new identities. Therefore, in this experiment, we investigated the possibility of generating different-sized databases of virtual identities. Mixing all possible pairs from 150 subject from the probe set (P) will result in $\binom{150}{2} = 11,175$ different virtual identities pairs. In this experiment, fingerprints pairs in the probe set are sorted based on the compatibility metric values. Then, the N fingerprint pairs with highest compatibility values in P were mixed and so were their corresponding impressions in the gallery set (G). Table 3.2 reports the rank-1, rank-5 accuracies and the EERs of the virtual identity datasets created with different values of N. These results confirm the possibility of generating virtual identities by mixing fingerprints; however, there is a trade-off between database size and the identification accuracy[‡]. This trade-off is because mixing several pairs from the same probe set P can lead to the generation of several identities sharing a common fingerprint (F_1). Assume two fingerprint pairs (F_a, F_b) and (F_a, F_c) where $F_b \neq F_c$. Combining the spiral component, $\cos(\psi_s)$, of the common fingerprint (F_a), with the continuous components, $\cos(\psi_c)$, of F_b and F_c generates two mixed fingerprints MF_{ab} and MF_{ac}, respectively. MF_{ab} and MF_{ac} are

[‡]Generating and matching all the 11,175 virtual identities resulted in an EER of 17%

likely to share some common minutiae locations. This leads to high impostor matching scores between two different virtual identities, consequently resulting in high false acceptance rate and low identification accuracy.

Table 3.2: The Rank-1, -5 accuracies and EER of the virtual identity databases

Size of the database (N)	Rank-1 (%)	Rank-5 (%)	EER (%)
50	88	95	4
100	85	97	5
200	84	95	5
800	68	82	8
1000	56	81	10

3.3.2 Generating Cancelable Identities

De-identifying fingerprint image is necessary to mitigate concerns related to data sharing and data misuse [19] and this is possible by transforming fingerprint image into a new one using a set of application-specific transformation functions, such that the original identity cannot be easily deduced from the transformed. A fingerprint that is transformed in this way is referred to as a cancelable fingerprint since it can be "canceled" by merely changing the transformation function [29] [30]. The purpose of the following experiments was to investigate if the proposed approach can be used to obscure the information present in a component fingerprint image by generating a cancelable template prior to storing it in a central database. Therefore, fingerprints from FVC 2002-DB2 were de-identified by mixing them with fingerprints from the WVU dataset.

With regards to mixing fingerprints for de-identification, the following key issues are raised [86][87][88][27][89][28]:

1. Performance: What impact does mixing fingerprints have on the matching performance, i.e., can two mixed impressions pertaining to the same identity be successfully matched? (see Experiment B-1)

2. Changeability: Are the original fingerprint and the mixed fingerprint correlated? It is essential to assure that the proposed approach prevents identity linking, by preventing the possibility of successfully matching the original print with the mixed print (see Experiment

B-2).

3. Non-invertibility: Can an adversary create a physical spoof of the original fingerprint from a compromised mixed fingerprint? It must be computationally infeasible to obtain the original fingerprint features, i.e., the locations and orientations of fingerprint minutia from the mixed fingerprint (see Experiment B-3).

4. Cancelability: Does mixing result in cancelable templates? In case a stored fingerprint is compromised, a new mixed fingerprint can be generated by mixing the original with a new fingerprint. The new mixed fingerprint and the compromised mixed image must be sufficiently different, even though they are derived from the same finger. Another way of looking at this is as follows: if two different fingerprints, F_1 and F_2, are mixed with the same fingerprint F_m, are the resulting mixed fingerprints, M_1 and M_2, similar? From the perspective of security, they should *not* be similar (see Experiments B-4 and B-5).

Therefore, the following experiments were designed to evaluate the security strength and the usability of our proposed approach for generating cancelable fingerprints.

– **Experiment B-1:** The purpose of this experiment was to report the matching performance of de-identifying fingerprints from FVC 2002-DB2 by mixing them with fingerprints from the WVU dataset. For each fingerprint in FVC 2002-DB2 noted by F_1, its compatibility measure with each fingerprint in the WVU dataset (300 images of 150 subjects) was computed using Equation (3.9) with $\alpha = 0.6$ and $\gamma = 0.4$. Based on the computed compatibility measures, the spiral component of F_1 was combined with the continuous component of the most compatible fingerprint image F_2 in the WVU dataset, resulting in the mixed fingerprint MF_1. Figure 3.16 shows examples of mixed fingerprints. Because there are 2 impressions per finger in FVC2002-DB2, the mixing process resulted in 2 impressions per mixed finger. one of these mixed impressions was used as probe images and the other was added to the gallery set. The obtained rank-1 accuracy was $\sim$ 83% and the EER was $\sim$ 7%. This indicates the possibility of matching mixed fingerprints. Tables 3.3 and 3.4 show the recognition performance of mixing fingerprint along with different cancelable techniques and cryptosystems schemes, respectively. These approaches have been reported because they stated their experimental results of protecting the fingerprint templates of FVC2002-DB2.

Note that the template protection schemes such as biotokens [90] and the cryptosystems schemes [91] [92] are verification systems which combine biometric information with another assigned secret. Therefore, these schemes have better performance because the user is required to carry (e.g., a token) or remember (e.g., a password) another authenticator in addition to his biometrics.

Table 3.3: Recognition performance of mixing fingerprints and other cancelable biometrics approaches

Cacelable biometrics techniques	$EER(\%)$
Surface folding transformation [86]	12
Biotokens [90]	0.08
Biophasor [93]	5
Mixing Fingerprints	7

Table 3.4: Recognition performance of mixing fingerprints and cryptosystems schemes

Cryptosystems schemes	$FRR@FAR \simeq 0.01\%(\%)$
Fuzzy Vault [91]	5
Fuzzy Commitment [92]	12.6
Mixing Fingerprints	14

– **Experiment B-2:** In this experiment, the possibility of exposing the identity of the FVC2002-DB2 fingerprint image by using the mixed fingerprint images was investigated. The mixed fingerprints MF_1 (2 impressions per finger) were matched against the original images in FVC2002-DB2. The resultant rank-1 accuracy was less than 30% (and the EER was more than 30%) suggesting that the original identity cannot be easily deduced from the mixed image.

– **Experiment B-3:** In this experiment, the vulnerability of the proposed de-identification approach to brute-force attacks is discussed with respect to non-invertibility [87] if an attacker were to access the mixed fingerprint MF_1. In other words, if the mixed fingerprint MF_1 was compromised, the probability of successfully reconstructing the original fingerprint F_1 is estimated. Based on Equation (3.8), if an attacker accesses a mixed fingerprint MF_1 (with the knowledge that it is a mixed fingerprint) and F_2, and then decomposes MF_1 by using the technique described in sub-section 3.2.1,

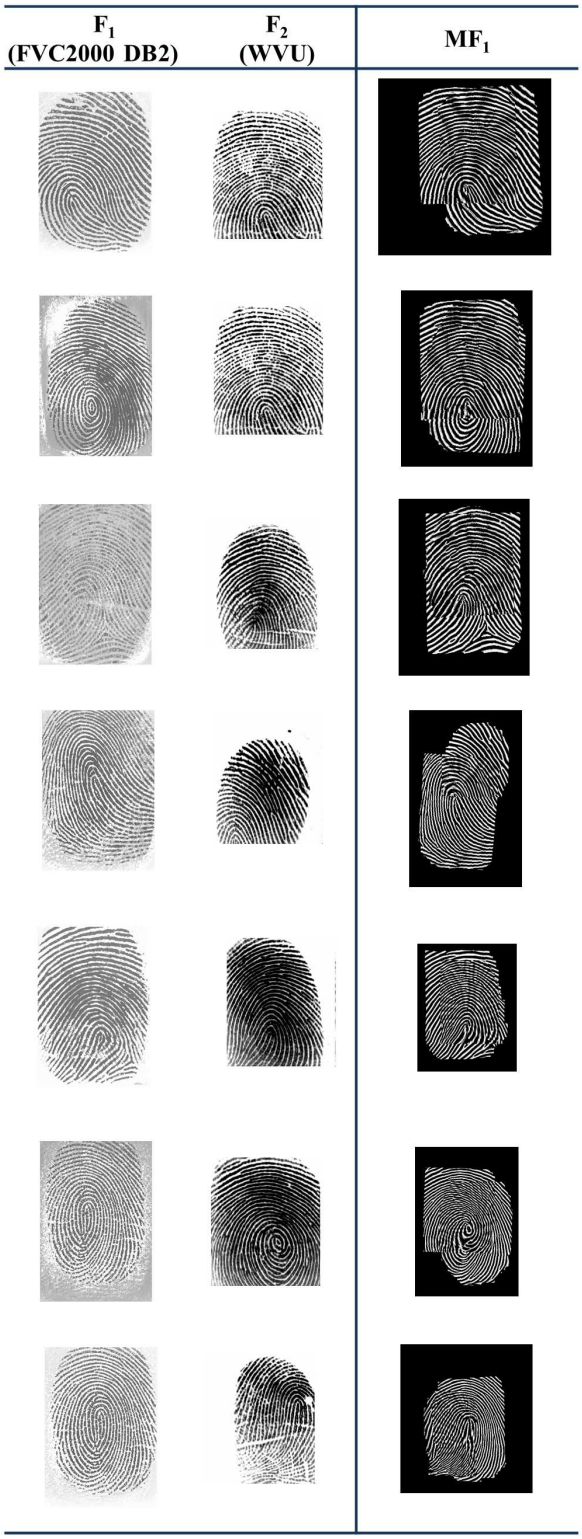


Figure 3.16: Examples of mixing fingerprints where F_1 and F_2 are fingerprints from the FVC2000 and WVU datasets, respectively.

the minutia locations of the original fingerprint F_1, characterized by the spiral component, are compromised. Although several researchers have shown that the original fingerprint image can be reconstructed from a fingerprint's minutiae consisting of their locations *and* orientations [22][21][23], there is no published work that discusses the possibility to reconstruct the original fingerprint image only from the minutiae locations. Therefore, the attacker must assume the orientation of each minutia to be able to reconstruct the original fingerprint. Hence, if x is the tolerance determining the acceptable deviation from the original orientation, the probability of assuming the correct orientation for a given minutiae is

$$p_\theta = \frac{x}{180\,^\circ}. \tag{3.13}$$

Consequently, the probability of successfully generating n or more minutiae which are the same as in the original fingerprint is

$$P = \sum_{k=n}^{N} \binom{N}{k} p_\theta^k (1 - p_\theta)^{N-k}, \tag{3.14}$$

where N is the total number of minutiae in a fingerprint, and n is the minimum number of minutiae required for authentication. Table 3.5 shows the probabilities of successfully compromising the orientations of minutiae points in the original fingerprints for different values of n. In our experiments, the average number of minutiae per fingerprint, N, is 45. The low probabilities in the table indicate that it is difficult to regenerate the original fingerprint from the mixed fingerprint.

Table 3.5: The probability P of generating n or more minutiae which are the same as in the original fingerprint ($N = 45$ and $x = 2\,^\circ$)

n	P
10	6.41×10^{-11}
12	7.2490×10^{-14}
26	3.5620×10^{-37}
45	1.1457×10^{-88}

– **Experiment B-4:** The purpose of this experiment was to investigate if the proposed

approach can be used to cancel a compromised mixed fingerprint and generate a new mixed fingerprint by mixing the original fingerprint with a new fingerprint. To evaluate this, the 2 impressions of one single fingerprint in the FVC2002-DB2 database were selected. Next, this fingerprint was mixed with each of the 500 fingers in the WVU dataset. This resulted in 500 mixed fingerprints with 2 impressions per finger. One of these impressions per mixed finger was used as a probe image and the other was added to the gallery set. Then, each image in the probe set was compared against all images in the gallery set in order to determine a match. A match is deemed to be correct (i.e., the probe is correctly identified) if the probe image and the matched gallery image are from the same mixed finger. In the resulting experiments, the rank-1 identification accuracy obtained was 85% and the EER was 7%. The reasonably high identification rate suggests that the 500 mixed fingerprints are different from each other. This means, the fingerprint from the FVC2002-DB2 database can be successfully "canceled" and converted into a new "identity" based on the choice of the fingerprint selected from the WVU database for mixing.

– **Experiment B-5:** In this experiment, two different fingerprints from FVC2002-DB2, F_1 and F_2 (i.e., a single print of two different fingers from two different identities), were mixed with each of the 500 different fingers in the WVU dataset. This resulted in two set of mixed fingerprints - one based on F_1 and the other based on F_2. Matching these two sets against each other resulted in a rank-1 accuracy of 5% and an EER of 45%. This suggests that two different fingerprints mixed with a common fingerprint cannot be easily matched against each other. This further confirms the cancelable aspect of the proposed approach.

3.4 Summary

In this chapter, the concept of fusing biometrics signals, i.e., mixing biometrics was used in the context of fingerprint images. Fingerprint images are mixed in order to generate joint identities. Mixing fingerprints refers to the process of generating a new fingerprint image by fusing fingerprints of two different fingers pertaining to a single individual or different individuals. The generated mixed image incorporates characteristics from the original im-

Table 3.6: The Rank-1 accuracies and EERs of the experiments

Experiment		Description	Rank-1 accuracy (%)	EER (%)	The Desired Output (see sec. 3.3)
Virtual Identities	A-1	Generating 250 identities (randomly paired)	68	15	Low EER High Rank-1 acc.
	A-2	Generating 250 identities (paired based on the compatibility measure)	85	6	Low EER High Rank-1 acc.
	A-3	(a) Matching new identities against original (MF_1^P (MF_2^P) vs F_1^P (F_2^P))	52	25	High EER Low Rank-1 acc.
		(b) Matching new identities against original (MF_1^P (MF_2^P) vs F_2^P (F_1^P))	38	46	High EER Low Rank-1 acc.
	A-4	Mixing two fingerprints from the same subject	81	9	Low EER High Rank-1 acc.
Cancelable Identities	B-1	De-identifying FVC 2002-DB2 fingerprints	83	7	Low EER High Rank-1 acc.
	B-2	Mixed vs original	30	30	High EER Low Rank-1 acc.
	B-4	Mixed vs mixed (same F_1 and different F_2)	85	7	Low EER High Rank-1 acc.
	B-5	Mixed vs mixed (different F_1 and same F_2)	5	45	High EER Low Rank-1 acc.

ages, and can be used directly in the feature extraction and matching stages of an existing fingerprint recognition system. Also, it was demonstrated that "mixing fingerprints" can be utilized to (a) generate a new identity by mixing two distinct fingerprints and (b) de-identify a fingerprint by mixing it with another fingerprint. To mix two fingerprints, each fingerprint is decomposed into two components, viz., the continuous and spiral components. After aligning the components of each fingerprint, the continuous component of one fingerprint is combined with the spiral component of the other fingerprint image. Experiments on two fingerprint databases, that has been summarized in Table 3.6, show that (a) the mixed fingerprint representing a new identity can potentially be used for authentication, (b) the mixed fingerprint is dissimilar from the original fingerprints used to generate it, (c) the same fingerprint can be used in various applications and cross-matching between applications can be prevented by mixing the original fingerprint with a different fingerprint, (d) mixing different fingerprints with the same fingerprint results in different identities, and (e) the proposed method can be utilized to generate a database of joint identities from a fixed fingerprint dataset.

Hence, the concept of fingerprint mixing can be utilized in the following examples to enhance the privacy of a fingerprint recognition system.

Scenario I: Consider a fingerprint system in which the left index finger, FL_s, of a subject ID_s is being enrolled. During enrollment, an impression of another finger of the subject (say the right index finger, FR_s) is mixed with FL_s resulting in a mixed print M_s. Next, M_s is stored in the central database while the images FL_s and FR_s are discarded. During authentication, the subject offers a sample of the left index finger, FL'_s, and a sample of the right index finger, FR'_s. These two images are then mixed resulting in a new print M'_s. In order to verify the subject's identity, M'_s is compared with M_s in the database. Therefore, the original fingerprint images of the left and right index fingers are never stored in the database.

Scenario II: Consider a remote fingerprint database that maintains a small set of pre-selected auxiliary fingerprints, $\mathcal{A}$, corresponding to multiple fingers (each finger in $\mathcal{A}$ is assumed to have multiple impressions). Suppose that subject ID_s offers the left index fingerprint, FL_s, during enrollment at a local machine. At that time, the local machine decomposes the fingerprint FL_s into two components, i.e., the spiral component and the

continuous component. To ensure the privacy of the fingerprint image, the remote system sends the stored fingerprints in the auxiliary set and the local machine searches through the received fingerprints to locate a "compatible" fingerprint based on the continuous component of FL_s (see Section 3.2), say $F_m \in \mathcal{A}$ (here the subscript m denotes a specific finger in the auxiliary set), which is then decomposed and its continuous component is mixed with FL_s at the local machine. The template of the new mixed print M_s is enrolled in the remote system database and FL_s is discarded from the local machine. During authentication, when the subject presents a sample of the left index finger, FL'_s, it is decomposed and its continuous component is used to search through the fingerprints in the auxiliary set from the remote fingerprint system to determine the most "compatible" fingerprint, say $F_n \in \mathcal{A}$. At the local machine, the spiral component of FL'_s is mixed with the continuous component of $F_n \in \mathcal{A}$ to generate a mixed fingerprint M'_s, which is then compared against the database entry M_s. Figure 3.17 shows the employed protocol to protect the privacy of a fingerprint image by mixing the input fingerprint image with another fingerprint from a set of pre-selected auxiliary fingerprints. The security protocol (illustrated in Figure 3.17) ensures that during the enrollment or the authentication process, the identities of the users will not be revealed by the fingerprint system. Further, since privacy of the input fingerprints is the main concern, the privacy of the stored auxiliary set, e.g. $\mathcal{A}$, could be preserved by storing just the continuous components of its pre-selected fingerprints.

3.4.1 Research Contribution

- Designing a new cancelability structure for fingerprint templates.
- Generating a fingerprint image from different fingerprint instances.
- Proposing a complete approach to decompose a fingerprint image.

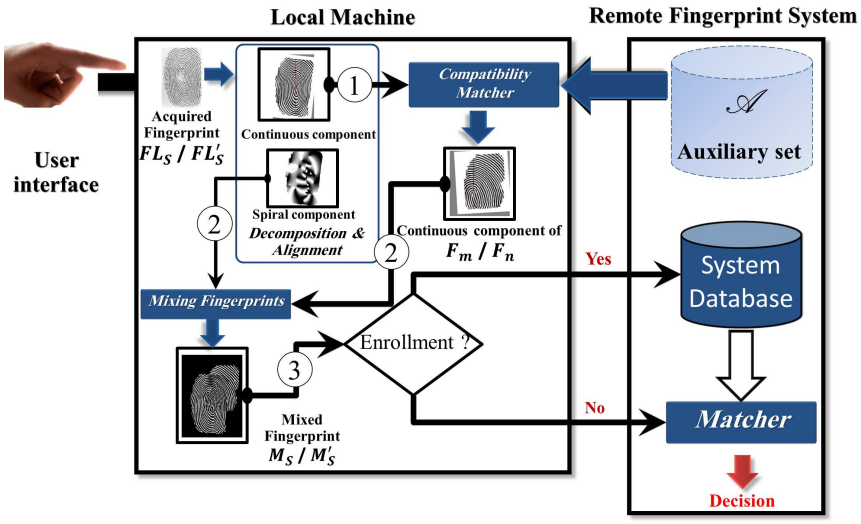


Figure 3.17: Schematic protocol to protect the privacy of a fingerprint image by utilizing the proposed approach

Chapter 4

Mixing Faces For Generating Joint Identities

4.1 Introduction

In this chapter, our goal is generating a joint identity by mixing two face images. Therefore, we explore the possibility of mixing face images of different subjects and determine how this new mixed face image will perform during the authentication process. Moreover, we investigate the possibility of generating a realistic face image that maintains a close similarity with the original face images. The generated joint identity and the original identities should reside in adjacent identity subspaces* (i.e., similar facial features and may be appearance) even if these original face images are associated with individuals who are different in race, gender and/or age.

Generating interpersonal face images by mashing celebrities' or family members' faces has received a lot of attention from digital artists to reveal the resemblance or difference between two face images (see Figure 4.1). In other cases, digital artists engage in such exercise as a challenge to mix two different face images and create a face image that looks familiar. Moreover, as shown in Figure 4.2, hybrid faces [95] is another example of a face image that visually can be interpreted as two faces. These different interpretations are based on the way humans process visual input, i.e., the viewing distance or image resolution. For example, to generate a hybrid face, two face images are summed at two different spatial scales: low-spatial scale (filtered by a low-pass filter) and the high-spatial scale (filtered by a high-pass filter) [95].

In this chapter, we discuss another scheme for generating a mixed face image that matches

*Here, the face-space is assumed to be partitioned into identity regions [94].

(a) (b) (c)

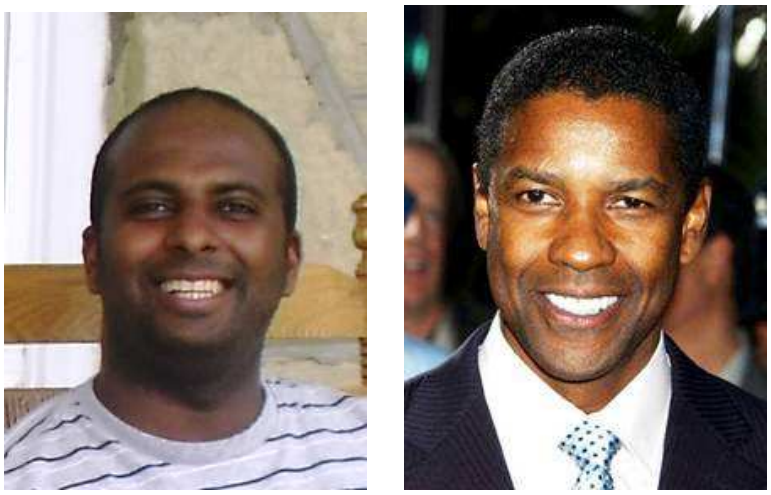
Figure 4.1: Examples of interpersonal faces generated by digital artists; (a) melding the smiles of Barack Obama and Malcolm X (source [8]), (b) splicing family members' faces (i.e., mother and daughter) together "genetic portraits" (source [9]), and (c) Morphing face images of two singers on an album cover (source [10]).

with both the component face images used to generate it. Mixing is possible even if the component face images differ in race, gender and/or age. The rest of the chapter is organized as follows. Section 4.2 discusses in more detail how the face morphing technique was adopted for mixing faces. Section 4.3 reports the experimental results and Section 4.4 summarizes the chapter.

4.2 Mixing Faces: The proposed approach

To generate an interpersonal face image, the principle of face morphing is used. Consider two face images F_1 and F_2. The morphing algorithm generates an intermediate image that is referred to as an interpersonal face image. The generated face image could be anywhere along the continuum from F_1 to F_2 and its position on this continuum is specified by the morphing parameters. The parameters, described later, are used to determine the rate of warping and color blending. So, as the morphing proceeds along the continuum from F_1 to F_2, the first image (F_1) is gradually distorted and is faded out, while the second image (F_2) is faded in (see Figure 4.5).

Ever since Galton [96] developed the first facial compositing technique in 1878 (which can be considered to be the first attempt in generating an interpersonal face image), many studies have been conducted to analyze various aspects of different face morphing techniques [97, 98, 99, 100, 101, 102, 103]. While most of them state that the generated interpersonal face image is similar to the original images, this assertion was only based on human perception. To the best of our knowledge, there has been no systematic study showing how close the morphed face image is to the original face images and the possibility of using the interpersonal face image as a biometric



(a) Face image 1 (b) Face image 2

(c) Hybrid face

Figure 4.2: A hybrid face (see (c)) constructed from low-frequency components of face image 1 in (a) and high-frequency components of face image 2 in (b).

indicator from the perspective of automated face recognition systems. As shown in Figure 4.3, there are three distinct phases in the generation of an interpersonal face image (MF) : facial feature extraction, image warping and cross-dissolving.

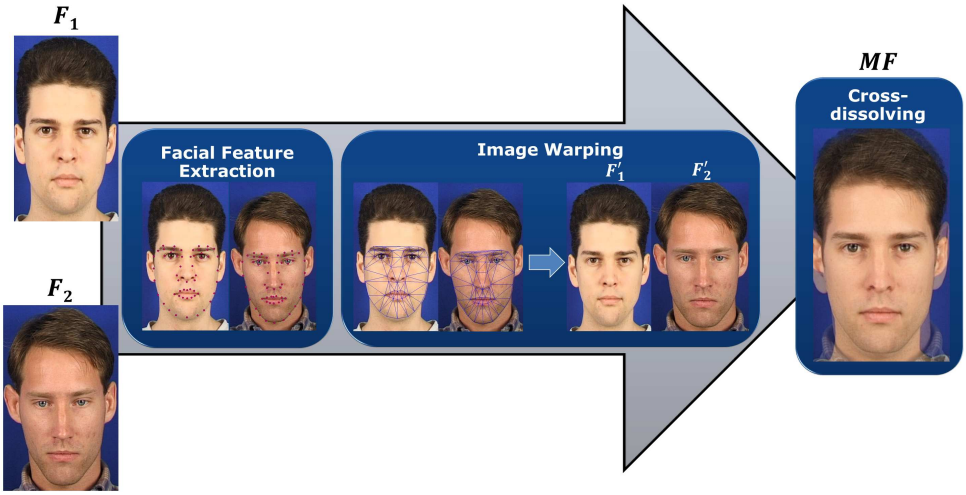


Figure 4.3: Proposed approach for generating an interpersonal face.

4.2.1 Facial feature extraction

Morphing two face images to generate an interpersonal face image involves the nontrivial task of locating facial features. For both face images, F_1 and F_2, the prominent facial features are characterized by a pre-defined set of control points. Both sets of control points, X_1 and X_2, associated with the two face images (see Figure 4.3), are stored in a vector format. This representation does not include any information about the connection between them:

$$X_j = [x_{1j}, x_{2j}, x_{3j}, \ldots, x_{nj}, y_{1j}, y_{2j}, y_{3j}, \ldots y_{nj}]^T, \tag{4.1}$$

where $j \in \{1, 2\}$ and $n = 56$ is the number of control points. Since extracting control points automatically [62] is not the focus of this work, a pre-annotated face image database was used (see Section 4.3).

4.2.2 Image warping

Once the corresponding control points between the two face images are known, the next step is to perform image warping by mapping each facial feature (e.g., mouth, nose and eyes) in the

individual face images to its corresponding feature in the interpersonal image. A triangulation-based warping scheme is used to deform the face images [104]. First, the intermediate control points set (which defines the shape of the facial features of the interpersonal face image) is determined. From the control point sets X_1 and X_2 of the face images F_1 and F_2, respectively, the intermediate control point set (X_m) is linearly interpolated as follows:

$$X_m = (1 - \alpha) \cdot X_1 + \alpha \cdot X_2, \tag{4.2}$$

where $\alpha \in [0, 1]$ is the **warping factor** that determines how the individual shapes of the two face images are integrated into the shape of the interpersonal face.

Next, the face region of each face image is dissected into a suitable set of triangles by utilizing corresponding control points as the vertices of the triangles. Generating an optimal triangulation has to be guaranteed in order to avoid skinny triangles and, therefore, Delaunay triangulation was utilized to construct a triangular mesh for each face image. An example of face images tessellated into triangular regions according to the annotated control points is shown in Figure 4.3.

Finally, the affine transformation that relates each triangular region in the original face image (F_1 or F_2) to the corresponding triangle region in the intermediate image is computed. Suppose that $T_1 = [P_1, P_2, P_3]^T$ ($T_2 = [R_1, R_2, R_3]^T$) is a triangular region in X_1 (X_2) and $T_m = [Q_1, Q_2, Q_3]^T$ is the corresponding triangular region in X_m (see Figure 4.4). A_1 (A_2) is the affine transformation that maps all points in T_1 (T_2) onto T_m.

$$T_m = A_j T_j, \tag{4.3}$$

where $j \in \{1, 2\}$ and the affine transformation $A_j = \begin{bmatrix} a_1 & a_2 & t_1 \\ a_3 & a_4 & t_2 \end{bmatrix}$.

Together, T_1's (T_2's) vertices and T_m's vertices are used in equation (4.3) to compute the parameters of the affine transformation A_1 (A_2) (i.e., $a_1, a_2, a_3, a_4, t_1, t_2$).

As shown in Figure 4.3, this results in two warped face images F_1' and F_2' such that F_1' and F_2' have similar shapes.

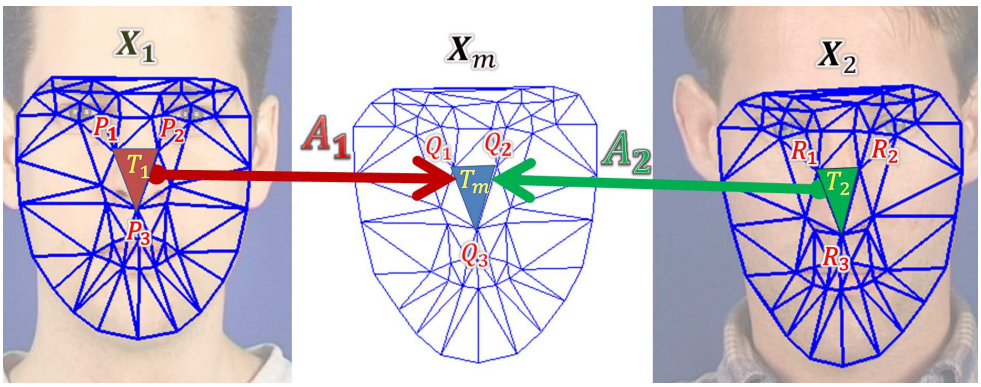


Figure 4.4: An illustration for the corresponding triangles between the faces' shapes and interpersonal face's shape.

4.2.3 Image cross-dissolving

The final step to obtain the interpersonal face image of the two face images F_1 and F_2, is simply a cross-dissolving process of the two warped images. If F_1' and F_2' are the warped images, the mixed face image is obtained by linearly interpolating their pixel intensities, such that

$$MF = (1 - \beta) \cdot F_1' + \beta \cdot F_2', \tag{4.4}$$

where $\beta \in [0, 1]$ is the **color-dissolving factor** that determines the relative influence of the appearance of the two face images on the interpersonal face image MF.

Figure 4.5 shows different examples of interpersonal face images along the continuum from F_1 to F_2 by varying the warping factor (α) and the cross-dissolving factor (β).

4.3 Experiments and Discussion

The performance of the proposed approach to generate mixed faces was tested using the XM2VTS database. This database was used since the facial landmarks (control points) of individual images were manually annotated and available online. The XM2VTS frontal image database [105] consists of 8 frontal face images each of 295 subjects. For each subject, four samples were used as the probe image and the remaining four samples were added to the gallery resulting in a probe set P and gallery set G each containing 1180 face images. In the following experiments, the match scores were generated using the Verilook SDK. In order to establish the

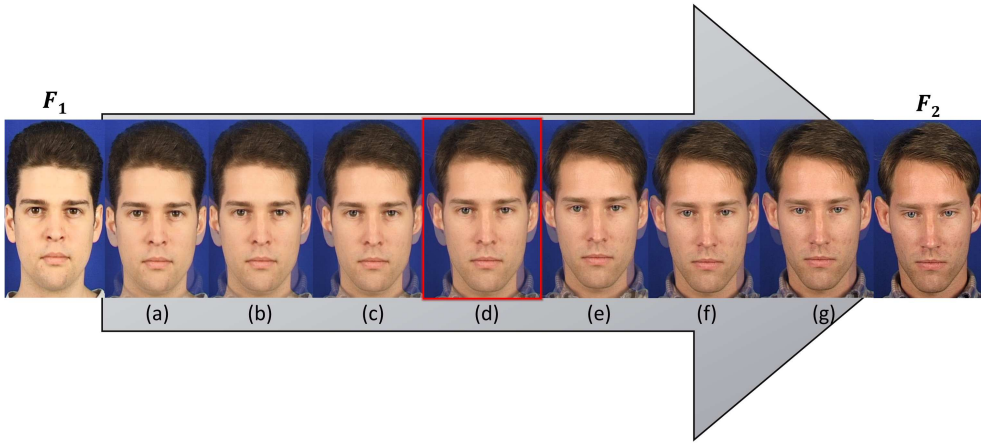


Figure 4.5: Interpersonal face images along the continuum from F_1 to F_2 at different position where $\alpha = \beta =$ (a) 0.2, (b) 0.3, (c) 0.4, (d) 0.5, (e) 0.6, (f) 0.7 and (g) 0.8.

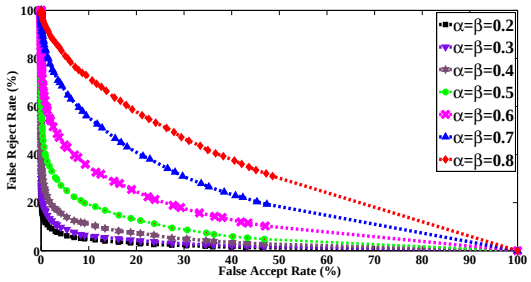
baseline performance, the images in P were matched against those in G. This resulted in a rank-1 accuracy of 98% and an Equal Error Rate (EER) of 5%. To generate the interpersonal face image from two face images F_1 and F_2, the morphing technique described earlier was utilized and the generated face image can be anywhere along the continuum from F_1 to F_2. But where on this continuous continuum should the interpersonal face image be?

The position of the interpersonal face on this continuum is specified by the morphing parameters, i.e., α and β. Although the two parameters can be different, the best quality of interpersonal face images along this continuum is observed to be obtained when assigning the same value to the two factors.

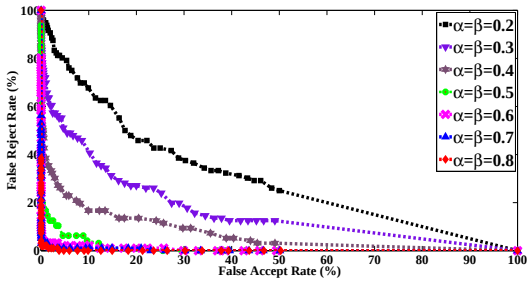
In this chapter, our objective is to generate an interpersonal face image that is unique and also has an identity subspace close to the identity subspaces of component face images (F_1 and F_2). Therefore, the similarity between the interpersonal face images (MF) that are generated for different values of morphing parameters (α and β) and the component face images was examined.

Face images of two different identities in P were *randomly* paired. Different interpersonal face images were generated by morphing the two face images of each pair with 7 different values of α and β ($\alpha = \beta = \{0.2, 0.3, 0.4, 0.5, 0.6, 0.7, 0.8\}$). This resulted in 7 probe sets and each probe set consisted of 588 face images (i.e., 147 joint identities with 4 samples for each identity). The corresponding pairs of face images in G were also mixed with the corresponding values of α and β resulting in 7 gallery sets and each gallery set consisted of 147 joint identities (each identity has 4 face image samples).

Figure 4.6 shows the ROC curves of matching the interpersonal face images against the corresponding component images F_1 and F_2, respectively. Based on these curves, and in order to ensure that the interpersonal face image is influenced to the same degree by the two component, α and β were selected to be 0.5 in the following experiments.



(a)



(b)

Figure 4.6: ROC curves of matching interpersonal face images (generated with different values of α and β) against the corresponding original images (a) F_1 and (b) F_2.

Computational time We evaluated the time complexity of the approach using $Matlab^{®}$-2013a on a PC with $Intel^{®}$ i7 CPU @2.8GHz and 8GB memory. The elapsed time of mixing two face images is 2 seconds.

4.3.1 Experimental design

In the following subsections, different experiments are discussed. These experiments were designed in order to address the following questions:

1. Can two interpersonal faces pertaining to the same joint identity be successfully matched?

2. Are the original faces and the interpersonal face image similar? In this work, note that our objective is to generate a joint identity that matches with both component identities.

3. If a set of face images are mixed with a common face image, then are the resulting joint iden-

tities different from one another? The interpersonal face images must be sufficiently different, even if they share one common face. Another way of looking at this is as follows: if two different face images, F_1 and F_2, are fused with the same face image F_m, are the resulting interpersonal face images, MF_1 and MF_2, similar? From the perspective of the distinctiveness property of biometrics, they should *not* be similar.

4. Does the degree of similarity of dissimilarity between the two original face images affect the recognition performance of the mixed face?

5. Can mixing faces be an alternative approach to obscure a demographic attribute of a database such as the gender of users enrolled in a face recognition system?

4.3.2 Performance metrics

The notion of similarity/dissimilarity is assessed using the match scores generated by a face matcher. A high degree of similarity is stated to exist between a probe image and a gallery image, if the similarity match score between the two images is generally higher than (a) the scores between the probe image and *other* gallery images, and (b) the scores between the gallery image and *other* probes. Thus, in the context of identification, a higher rank-1 accuracy would imply a higher similarity; in the context of verification, a lower Equal Error Rate (EER) would imply higher similarity. So we use rank-1 accuracy and EER to characterize notions of similarity and dissimilarity.

4.3.3 Experiment 1: Matching two interpersonal face images

In this experiment, the matching performance of interpersonal face images generated by mixing random pairs of faces is reported. The process of mixing random pairs of face images in P to generate MF^P and then mixing the corresponding pairs in G to generate MF^G is repeated 20 times. This resulted in twenty different MF^P sets and their corresponding MF^G sets. When matching each MF^P set against the corresponding MF^G set, the average of the resultant rank-1 accuracies was $\sim$ 95% and the average of the EERs was $\sim$ 8%. The reasonably good recognition rates suggest that the interpersonal face images can be used as biometric indicators for the joint identities. Figure 4.7 shows examples of mixing pairs of face images.

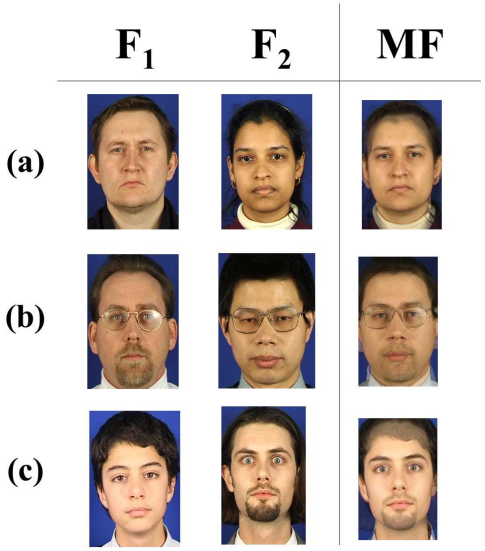


Figure 4.7: Examples of interpersonal face images. These face images are generated by mixing face images that are different in terms of gender (as in (a)), race (as in (a) and (b)), and/or age (as in (c)).

4.3.4 Experiment 2: Similarity to the original face images

In this experiment, the similarity between the interpersonal face image and the component face images was evaluated. Recall that the objective of this work is to generate a mixed face image that is sufficiently similar to both component faces. Therefore, the interpersonal face images generated in Experiment 1 were matched against the original component images in gallery set G. Here, a genuine score is generated when the interpersonal face image is matched with either of the component face images (the rest are impostor scores). The average of resultant rank-1 accuracies was 95% (and the average of EERs was 9%). These results show some evidence that the original face images are similar to the interpersonal image. The similarity between the mixed and original faces can be further enhanced by exploring alternate algorithms for mixing the different face images.

4.3.5 Experiment 3: Mixing with a common face image

The purpose of this experiment was to investigate if mixing two different face images, F_1 and F_2, with a common face image F_m, results in interpersonal face images MF_1 and MF_2 that are sufficiently dissimilar from each other.

For example, the 8 samples of F_m is mixed with the 8 samples of F_1 (i.e., the first face image

of remaining face images after selecting F_m), and the resulted mixed samples (8 samples) are pertaining to the first joint identity J_1. Then, 4 Samples of J_1 are added to MF^P and the other 4 are added to MF^G. Similarly, if samples of the face image F_m is mixed with the 8 samples of F_2 (i.e., the second face image of remaining face images) and the resulted mixed samples (8 samples) are pertaining to the first joint identity J_2. Then, 4 Samples of J_2 are added to MF^P and the other 4 are added to MF^G. Hence, 16 genuine scores will be generated by matching the 4 samples of J_1 in MF^P against the other 4 samples of J_1 in MF^G. Meanwhile, 16 impostor scores will be generated by matching the 4 samples of J_1 in MF^P against the 4 samples of J_2 in MF^G.

To achieve the goal of this work, the interpersonal face images must be sufficiently different, even if they share one common face.

To evaluate this, a face image (F_m) in the probe set P was arbitrarily selected and mixed with the remaining face images in that set to generate the set MF^P. The same pairs of images were mixed in the gallery set G resulting in MF^G. Each set now has 1176 interpersonal face images for 294 joint identities (i.e., 4 samples for each joint identity). This selection and mixing process is done 20 times, each time selecting a different face image as F_m. This resulted in twenty different MF^P sets and their corresponding MF^G sets. When matching each MF^P set against the corresponding MF^G set, the average of the resultant rank-1 accuracies was $\sim$ 85% and the average of the EERs was $\sim$ 10%. These numbers suggest that the the interpersonal face images are sufficiently different, even though they share a common component face image. However, it must be noted that the distinctiveness has decreased compared to Experiment 2.

4.3.6 Experiment 4: Mixing look-alike face images

The purpose of this experiment is to investigate the effect of mixing look-alike face images [106]. The purpose here is to determine if the similarity (or dissimilarity) between the face images to be mixed has any impact on the distinctiveness of the resulting interpersonal face image. The matching scores are used as a metric to select pairs of face images that look alike.

Experiment 4a: $F1$ and $F2$ look alike

To mix look-alike faces, pairs whose matching score is more than an empirical threshold (1/10 * highest impostor score) were selected and mixed resulting in a probe set MF_1^P and a gallery set MF_1^G. Each set consists of 588 face images (i.e., 147 joint identities with 4 samples for

each identity) - this number can be changed by altering the empirical threshold. Figure 4.8 shows examples of the generated face images. Matching MF_1^P against MF_1^G resulted in a rank-1 accuracy of $\sim$ 95% and an EER of $\sim$ 8%.

Meanwhile, matching MF_1^G against the component face images (as in Experiment 2 but here the components are look-alike faces) resulted in an average of rank-1 accuracies of $\sim$ 8% and an average of EERs of $\sim$ 94%.

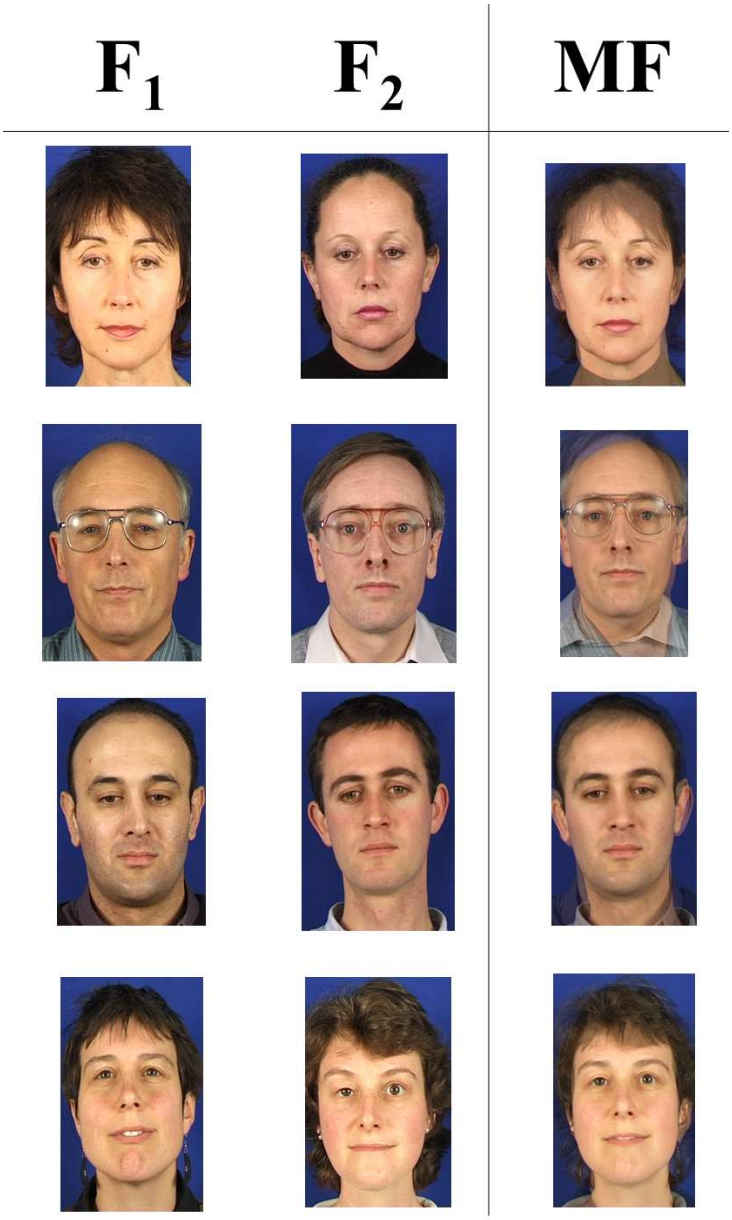


Figure 4.8: Examples of interpersonal face images generated by mixing pairs of look-alike face images based on the matching scores.

Experiment 4b: $F1$ and $F2$ do not look alike

To generate mixed face images from pairs of face images which are dissimilar (i.e., do not look-alike), pairs whose matching scores equal zero were selected and mixed resulting in a probe set MF_2^P and a gallery set MF_2^G. Each set consists of 588 interpersonal face images. Matching MF_2^P against MF_2^G resulted in a rank-1 accuracy of $\sim$ 95% and an EER of $\sim$ 9%.

Matching MF_2^G against the component face images (as in Experiment 2 but here the components are not look-alike faces) resulted in an average of rank-1 accuracies of $\sim$ 80% and an average of EERs of $\sim$ 15%.

Upon comparing the results of Experiments 4a and 4b with the results of Experiment 1, we observe that there is no big difference in the identification accuracy and the verification accuracy. These results demonstrate that the degree of similarity or dissimilarity between the face images to be mixed has almost no influence on the recognition performance of the generated joint identities.

Nonetheless, the influence is noticeable when the similarity between component face images and the mixed faces was tested. The mixed faces are more similar to their components if they are look-alike faces than if they are dissimilar. Note that, in this experiment, the components have been assigned based on the matching score. This may not be the cause of real scenarios which have been examined in Experiment 2 by mixing random pairs from a face database.

Results of the 4 experiments are summarized in Table 4.1.

4.4 Summary

In this chapter, it was demonstrated that the concept of "mixing faces" can be utilized to generate a joint identity. To mix two face images, a face morphing technique was adopted in this work. The mixed face image lies in the continuum between the two component faces and its position on this continuum is specified by the mixing parameters. We also investigated the possibility of generating a mixed face image when the two component images are different in terms of race, gender and/or age (see Figure 4.7). Further, we determined if the similarity (or dissimilarity) between the face images to be mixed has any impact on the distinctiveness of the resulting interpersonal face image. Experiments on the XM2VTS dataset, which have been summarized in Table 4.1, indicate that (a) the mixed face image representing a new joint identity can potentially be used as a biometric indicator, (b) the mixed face exhibits similarity with both

Table 4.1: Results of the experiments

Experiment	**Description**	**Rank-1 accuracy** (%)	**EER** (%)	**Implication**
1	Matching two interpersonal face images	95	8	Mixed faces can be used as biometric identifiers
2	Similarity to the original face images	95	9	The mixed face exhibits similarity to both the component faces
3	Mixing with a common face image	85	10	The mixed faces are reasonably different, even if they share a common face image
4	(a) F_1 and F_2 look alike	95	8	The degree of similarity between the original face images to be mixed has almost no influence on the recognition performance
	(b) F_1 and F_2 do not look alike	95	9	

the component faces, and (c) the mixing process is not unduly impacted by differences in gender, race, age and similarity between component images.

4.4.1 Research Contribution

- Defining the concept of digital joint identity through face images.
- Generating a face image from different face instances.

Chapter 5

Mixing Irises For Generating Joint Identities

5.1 Introduction

In this chapter, our goal is to generate a joint identity by mixing two iris images acquired from two *different* eyes. We investigate the possibility of mixing irises in order to generate a realistic iris image that maintains a close similarity with the original components. In the following, some of the applications of the proposed approach are discussed.

- **Generating Joint Identities:** Mixing irises can be utilized to generate a new iris image by fusing two different iris images acquired from two different eyes. In the context of iris, image level fusion approaches have been developed to combine different video frames of the same iris instance to improve the iris recognition performance [49] [50]. Also, fusing irises has been proposed in Zuo et al.'s work to de-identify normalized iris images [51]. They proposed a de-identifying function which adds a synthetic iris image to the original iris image. In this chapter, a new approach to fuse iris images is introduced by mixing iris images. The objective of this work is to generate a mixed iris image that is sufficiently similar to both component iris. Therefore, the mixed iris image can be used for authentication of individuals who share a joint bank account.

- **Multi-eye Authentication System:** Patterns of the left iris of an individual are assumed to be different from those of right iris in the context of iris recognition systems [107][108]. Therefore, during the enrollment phase of an iris-based authentication system, the oper-

ator/user *must* indicate the iris from which eye is enrolled. Then, during recognition, the system must capture the iris from the same eye image so that it can be successfully matched with the corresponding one in the database. In many deployment scenarios, it is easy for the operator/user to mislabel the eyes. Mislabeling in this case can lead to a drop in the matching performance as the captured iris image during the recognition will not be matched with the stored one in the database. In response to this problem, classifiers to determine whether an eye image is a left or right eye have been developed to detect errors in the labeled data. One initial approach for differentiating between left and right eyes uses the locations of the pupil center and the iris center [109]. The pupil is often located on the nasal side of iris rather than being directly concentric with it. Abiantun and Savvides [110] evaluated five different methods for detecting the tear duct in an iris image in order to classify eye images as being left or right: (1) Adaboost algorithm with Haar-like features, (2) Adaboost with a mix of Haar-like and Gabor features, (3) support vector machines, (4) linear discriminant analysis, and (5) principal component analysis. Another study [111] used active shape models (ASMs) to determine the shape of the eye and predict whether an eye is a right or left eye.

Mixing irises can be considered as an alternative method to alleviate this problem by mixing the left and right irises during the enrollment phase and storing the mixed iris image. During the recognition phase, the stored mixed iris will match correctly with the captured probe iris irrespective of it being the left or right iris image or even the mixed iris image from both eyes. Therefore, the concept of mixing irises can be utilized in a multi-eye authentication system where the irises from the left and the right eyes of a single individual, or left irises of two different individuals are mixed to generate a new iris image. This has benefits in terms of performance by avoiding the enrollment error.

The mixing process (see Figure 5.1) begins by segmenting iris regions for two acquired eyes and normalizing these segmented regions. Next, the optimal pixels from the two iris images are copied on to a mixed iris image where the optimality is defined in terms of importance of each pixel in the iris image. The selected pixels should be connected in such a way that will capture the dominant features of the irises' texture. These pixels could be in a single row in the form of a horizontal bar. However, simply copying horizontal bars seems restrictive and places a hard constraint on the location of optimal pixels. Hence, copying horizontal seams is proposed. A

seam is a horizontal 8-connected path that contains only one pixel per column of the optimal pixels. Extracting seams based on the concept of importance map has been proposed in [112] for content-aware resizing of images and is also known as seam carving.

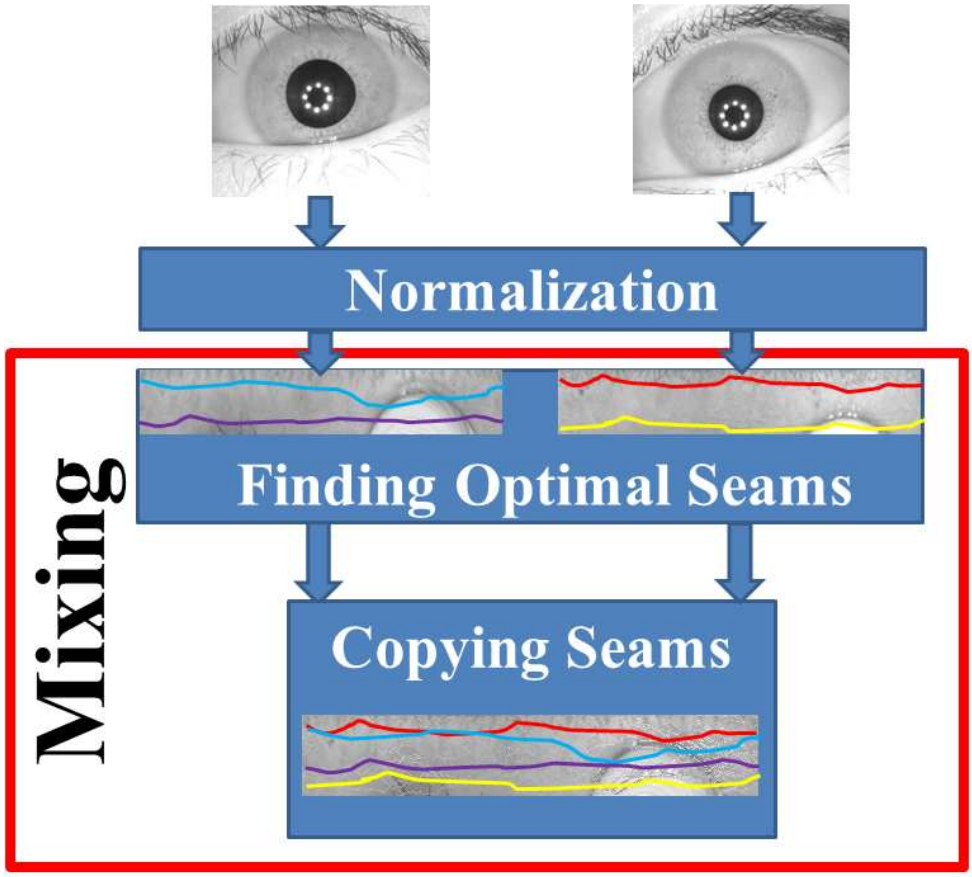


Figure 5.1: Proposed approach for mixing irises.

The rest of the chapter is organized as follows. Section 5.2 presents the proposed approach for mixing irises. Section 5.3 reports the experimental results and Section 5.4 summarizes the chapter.

5.2 Mixing Irises: The proposed approach

Our approach to mix irises from two different eyes involves copying the most important connected pixels, i.e., seams, from the normalized iris images into a new mixed iris image. The importance of a pixel is defined by an importance map that evaluates the importance of each pixel based on its contrast with its neighbors. Seams can be either vertical or horizontal. A horizontal

seam is a path of pixels connected from left to right in an image with one pixel in each column. A vertical seam is similar with the exception of the connection being from top to bottom with one pixel in each row. Here is an outline of the proposed approach to mix two iris images:

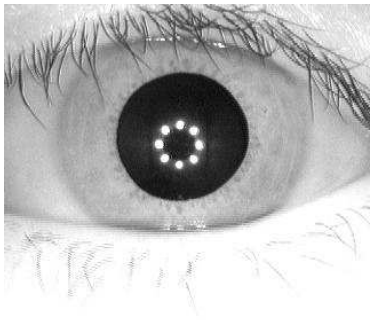
1. Generating normalized iris images
2. Constructing importance maps
3. Finding the optimal seams
4. Copying seams

5.2.1 Generating normalized iris images

Given two iris image, the irises have to be localized and isolated from the sclera, pupil, eyelids and eyelashes and this can be done by using a segmentation algorithm. In this chapter, we used an approach that utilizes geodesic active contours [113] to segment the annular region of an iris image. During the segmentation, a noise mask is generated to record the locations of eyelids and eyelashes that may be occluding the true iris region. Grabbing pixels from iris regions to copy them into a mixed iris image is computationally expensive and requires repeated Cartesian-to-Polar coordinates conversions. Therefore, both the segmented irises and corresponding noise masks are unwrapped into rectangular regions using Daugmans rubber sheet model [70]. This allows the mixing irises approach to address pixels in simple rows and columns format. For a detailed description and review of various eye localization, iris segmentation, and iris unwrapping techniques, see [66], [114], [64] and [65]. Figure 5.2 shows an example of an eye and its normalized iris and noise mask images.

5.2.2 Constructing importance maps

The next step in mixing irises is locating the important pixels in the original normalized iris images in order to copy them into the mixed image. This is done by assigning a value to every pixel in the normalized iris image, where higher values mean higher importance. In this work, every pixel in a normalized iris image I will have an corresponding value in the importance map IM, which will be the absolute sum of both gradient components at that pixel.



(a)

(b)

(c)

Figure 5.2: Iris segmentation and normalization (a) An eye image. (b) The normalized iris image. (c) The estimated noise mask.

$$IM = |\frac{\partial I}{\partial x}| + |\frac{\partial I}{\partial y}|. \tag{5.1}$$

Figure 5.3 visualizes the importance map for the normalized iris image in Figure 5.2. This also shows that using the L_1 norm (see Equation 5.1) for computing the importance map IM highlighted the edges in the normalized iris texture, i.e., the pixels along the edges have higher importance.

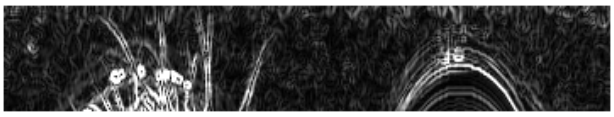


Figure 5.3: Estimated importance map (IM) of the normalized iris image in Figure 5.2.

-

5.2.3 Finding the optimal seams

Mixing irises is done by repeatedly determining seams with the maximal importance from two normalized iris images and copying them into the new mixed iris image. Therefore, once

the importance map is calculated, the next step is to find the optimal horizontal or vertical seam in normalized iris image, I. A horizontal (or a vertical) seam s_h (s_v) is an 8-connected path of pixels that runs from the left (top) of the image to the right (bottom) with one pixel in each column (row). The 8-connected property means that for each pixel, during the backtracing process, only its 8 adjacent neighbors are considered. Based on this definition of a seam and given that I is a normalized iris image of size $n \times m$, where n is the number of rows and m is the number of columns, a horizontal seam is defined as [112]:

$$s_h = \{(S_h(j), j)\}_{j=1}^{m}, s.t. \forall j, |S_h(j) - S_h(j-1)| \leq 1, \tag{5.2}$$

where S_h is a mapping function of s_h and $S_h(j) = 1, \ldots, n$. Similarly, a vertical seam is defined by its mapping function S_v as:

$$s_v = \{(i, S_v(i))\}_{i=1}^{n}, s.t. \forall i, |S_v(i) - S_v(i-1)| \leq 1, \tag{5.3}$$

where $S_v(i) = 1, \ldots, m$.

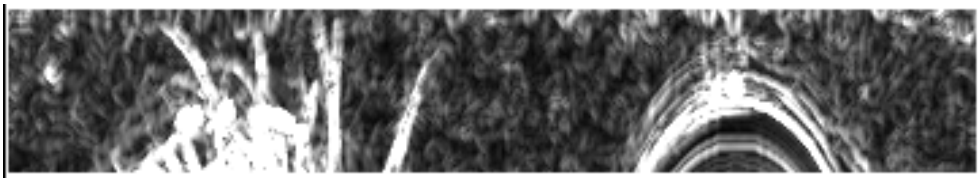
The importance of a seam s is defined as the sum of the associated importance values of pixels lying on that seam in the importance map. Hence, given the importance map IM, an optimal horizontal seam s_h^* is the seam with a mapping function S_h that maximizes its importance.

$$s_h^* = \max_{s_h} \sum_{j=1}^{m} IM(S_h(j), j). \tag{5.4}$$

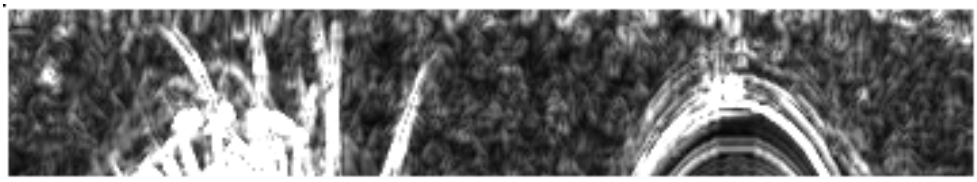
To find horizontal or vertical optimal seams in order to copy them into the mixed iris images, the dynamic programming concept is utilized and maximum cumulative importance maps are created [112]. The maximum cumulative importance maps have to be created separately for the horizontal (Figure 5.4 - a) and vertical (Figure 5.4 - b) seams and backtracking is done on these.

For example, to locate the optimal horizontal seam, the horizontal cumulative importance map CM_h is computed. The first column in the importance map IM is copied to the first column in CM_h and then,

$$\begin{aligned} CM_h(i,j) = IM(i,j) + \\ max\{IM(i-1,j-1), IM(i,j-1), IM(i+1,j-1)\}. \end{aligned} \tag{5.5}$$



(a)



(b)

Figure 5.4: Cumulative importance maps (a) The horizontal map (CM_h). (b) The vertical map (CM_v).

The optimal horizontal seam is determined by simply backtracing on CM_h the maximum entry. Figure 5.5 shows an example of a traced optimal seam on a normalized iris.

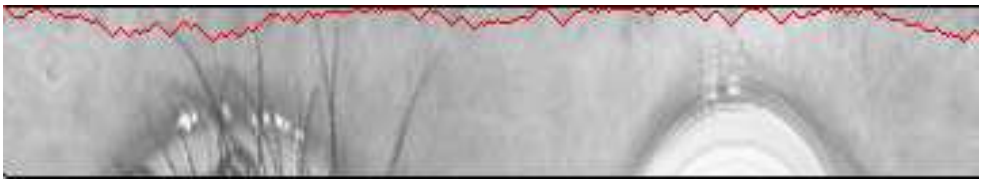


Figure 5.5: The traced optimal horizontal seam on the normalized iris image in Figure 5.2.

5.2.4 Copying seams

Let I_1 and I_2 be the two normalized iris images of size $n \times m$ from two different eye images. IM_1 and IM_2 are their importance maps, respectively. The following steps are invoked to generate a mixed iris image MI by copying horizontal seams from I_1 and I_2:

1. $MI = MI_initial$ ($MI_initial$ is an initial image).

2. Find the optimal horizontal seam s^*_{1h} in I_1.

3. Copy the pixels that make up s^*_{1h} into MI in the same location as they are in I_1.

$$MI(s^*_{1h}) = I_1(s^*_{1h}).$$

4. Replace the pixels at s^*_{1h} in I_1 and IM_1 with black pixels.

$$I_1(s^*_{1h}) = 0 \, , IM_1(s^*_{1h}) = 0.$$

5. Replace the pixels in I_2 and IM_2 that are in the same location as the pixels at s^*_{1h} with black pixels.

$$I_2(s^*_{1h}) = 0 \, , IM_2(s^*_{1h}) = 0.$$

6. Find the optimal horizontal seam s^*_{2h} in I_2.

7. Copy the pixels that make up s^*_{2h} into MI in the same location as they are in I_2.

$$MI(s^*_{2h}) = I_2(s^*_{2h}).$$

8. Replace the pixels at s^*_{2h} in I_2 and IM_2 with black pixels.

$$I_2(s^*_{2h}) = 0 \, , IM_2(s^*_{2h}) = 0.$$

9. Replace the pixels in I_1 and IM_1 that are in the same location as the pixels at s^*_{2h} with black pixels.

$$I_1(s^*_{2h}) = 0 \, , IM_1(s^*_{2h}) = 0.$$

10. Repeat steps from 2 to 9 n times.

There are some remarks the mixing steps.

- Same steps can be used to copy vertical seams from the iris images instead of horizontal seams. But this requires more iterations because the width of normalized images is much larger than their height.

- If the mixed iris image was initially set to a black $n \times m$ image, i.e., if $MI_initial$ is a black image, the mixed iris image will exhibit black background as shown in Figure 5.6. Therefore, in this work, the mixed iris image is initialized to I_1, i.e., $MI_initial = I_1$. Figure 5.7 shows examples of mixed iris images when $MI_initial = I_1$.

- The noise mask of the mixed iris image is the union of the two noise masks of the two original iris images.

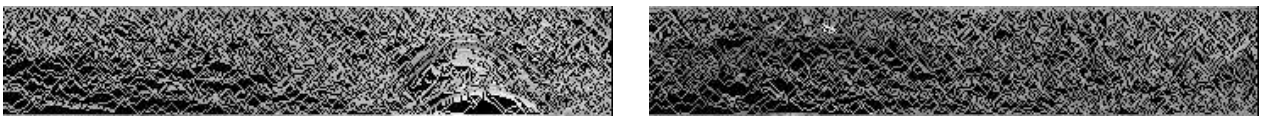


Figure 5.6: Examples of mixed iris images that were initialized to a black image.

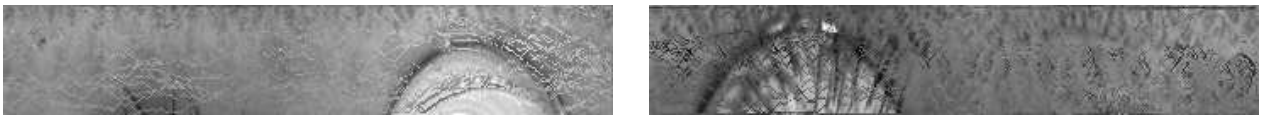


Figure 5.7: Mixed iris images from Figure 5.6 when they are initialized as I_1.

Computational time We evaluated the time complexity of the proposed approach using $Matlab$®-2013a on a PC with $Intel$® i7 CPU @2.8GHz and 8GB memory. The elapsed time for mixing two iris images is 3 seconds.

5.3 Experiments and Discussion

The experiments were conducted on a subset of the CASIA-v3 database [115]. The CASIA-v3 database consists of gray scale iris images captured using near infrared illumination. The subset used in our experiments consists of the left eye images of 182 users with 2 samples per user. The images in this dataset were segmented and normalized using the algorithms proposed by Shah and Ross [113]. An open source Matlab implementation [116] based on the Daugman's approach [117] was used to encode and match the normalized irises. The performance of matching irises is summarized using the Equal Error Rate (EER) and the rank-1 identification rate. For each iris, one sample was added to a probe set P and the other sample was added to a gallery set G each containing 182 irises. In order to establish the baseline performance, the images in P were matched against those in G. This resulted in a rank-1 accuracy of 100% and an Equal Error Rate (EER) of 1.4%.

5.3.1 Matching performance

In this experiment, the matching performance of generating mixed irises from random pairs of irises is reported. Random pairs of iris images in P were mixed in order to generate MI^P and then the corresponding pairs in G were mixed to generate MI^G. As the mixed iris can be

generated by copying horizontal or vertical seams, the results are reported for both cases below by matching MI^P set against the corresponding MI^G set.

Results of mixing by copying horizontal seams

The resultant rank-1 accuracy was $\sim$ 96% and the EER was $\sim$ 1.5%. The reasonably high recognition rate indicates the possibility of mixing irises and suggests that the mixed iris can be used as a biometric indicator. Figure 5.8 shows examples of mixed irises based on the copying of horizontal seams.

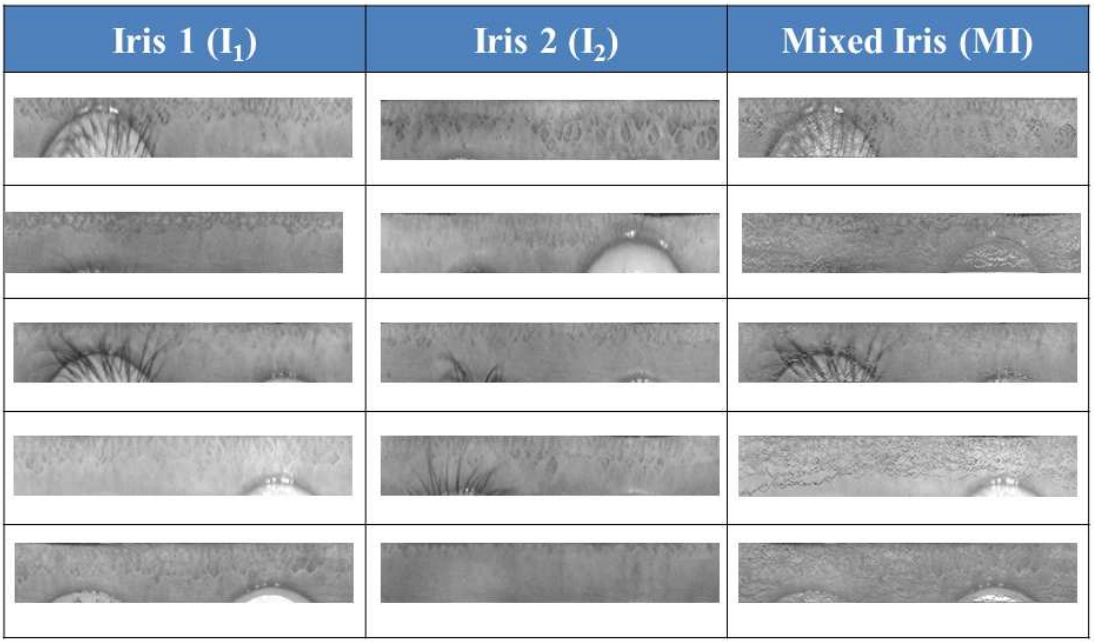


Figure 5.8: Examples of mixed irises by copying horizontal seams from the original components. Mixed iris images are initialized with I_1.

Results of mixing by copying vertical seams

The resultant rank-1 accuracy was $\sim$ 0% and the EER was $\sim$ 40%. The degradation in the performance, in comparison with the previous experiment, indicates that mixing irises by copying vertical seams may be not viable. This is because, during feature extractions the 1D log Gabor filter is convolved with each row of the normalized iris image. In other words, the encoding and matching process is row-based which causes a drop in the performance in case of mixing irises based on vertical seams.

5.3.2 Similarity to the original iris images

In this experiment, the objective of generating a mixed iris that is similar to both the original iris images is investigated. The mixed images (MI) in the probe set (MI^P), which are generated in the previous experiment by copying horizontal seams from the original irises, were matched against the corresponding original images (I_1 and I_2) in the gallery set of G.

a. Matching MI against I_1 resulted in rank-1 accuracy of $\sim$ 100% and EER of $\sim$ 1.5%.

b. Matching MI against I_2 resulted in rank-1 accuracy of $\sim$ 97% and EER of $\sim$ 1.9%.

The high matching performance suggests that the original identity is sufficiently similar to the mixed image. Note that there is a performance difference between the two cases since the mixed image, in both cases, is initialized to I_1 prior to copying the seams and this biases the mixed image with respect to I_1. The same difference in the performance is encountered if the mixed image is initialized to I_2, but this biases the mixed image with respect to I_2.

5.4 Summary

In this chapter, the possibility of generating a mixed iris by mixing two distinct irises is explored. It was demonstrated that the concept of "mixing irises" can be utilized to (a) generate a virtual identity and (b) generate mixed images that are similar to the original iris images. To mix two irises, horizontal seams are copied from normalized iris images into a new iris image after sorting them based on their importance in the images. Experiments on a CASIA-v3 dataset show that (a) the mixed iris representing a joint identity can potentially be used for authentication,and (b) the mixed iris is similar to the original irises.

5.4.1 Research Contribution

- Defining the concept of digital joint identity through iris images.
- Generating a mixed iris image from different instances.

Chapter 6

Decomposing Faces For Privacy Protection

6.1 Introduction

A face recognition system operates by acquiring face image from a subject, extracting a feature set from the data (e.g., eigen-coefficients) and comparing the feature set against the templates stored in a database in order to identify the subject or to verify a claimed identity. The template of a person in the database is generated during enrollment and is often stored along with the original face image. This has heightened the need to accord privacy* to the subject by adequately protecting the contents of the database.

For protecting the privacy of an individual enrolled in a biometric database, Davida et al. [29] and Ratha et al. [30] proposed storing a transformed face image instead of the original image in the database. This was referred to as a private template [29] or a cancelable biometric [30]. Feng et al. [118] proposed a three-step hybrid approach that combined the advantages of cryptosystems and cancelable biometrics. Apart from these methods, various image hiding approaches [119][120][121] have been suggested by researchers to provide anonymity to the stored biometric data.

For according privacy to face images present in surveillance videos, Newton et al. [122] and Gross et al. [123] introduced a face de-identification algorithm that minimized the chances of performing automatic face recognition while preserving details of the face such as expression, gender and age. Bitouk et al. [124] proposed a face swapping technique which protected the identity of a face image by automatically substituting it with replacements taken from a large library of public face images. However, in the case of face swapping and aggressive de-identification

*The term ”privacy” as used in this chapter refers to the de-identification of biometric data.

the original face image can be lost. Recently, Moskovich and Osadchy [125] proposed a method to perform secure face identification by representing a private face image with indexed facial components extracted from a public face database.

In this chapter, Visual Cryptography techniques will be used to preserve privacy. Hence, the privacy of a face image will be accorded by decomposing the original image into two face images in such a way that the original image can be revealed only when both images are mixed; further, the individual component images do not reveal any information about the original image. Figure 6.1 shows a block diagram of the proposed approach. In this approach, a private face image is decomposed into two independent public host images; thus, the private image can be viewed as being encrypted into two host face images.

During the enrollment process, the private face image is sent to a trusted third-party entity. Once the trusted entity receives it, the biometric data is decomposed into two images and the original data is discarded. The decomposed components are then transmitted and stored in two different database servers such that the identity of the private face image is not revealed to either server. During the authentication process, the trusted entity sends a request to each server and the corresponding sheets are transmitted to it. Sheets are mixed (i.e., superimposed) in order to reconstruct the private image thereby avoiding any complicated decryption and decoding computations that are used in watermarking [119][120], steganography [121] or cryptosystem [27] approaches. Once the matching score is computed, the mixed face image is discarded. Further, co-operation between the two servers is essential in order to reconstruct the original face image.

Decomposing the private face image into face images as hosts (as opposed to using random noise or other natural images) has several benefits in the context of biometric applications. First, the demographic attributes of the private face images such as age, gender, ethnicity, etc. can be retained in the host images thereby preserving the demographic aspects of the face while perturbing its identity. Alternately, these demographic attributes, as manifested in an individual's face, can also be deliberately distorted by selecting host images with opposite attributes as that of the private image. Second, a set of public face images (e.g., those of celebrities) may be used to host the private face database. In essence, a small set of public images can be used to encrypt the entire set of private face images. Third, using non-face images as hosts may result in visually revealing the existence of a secret face as can be seen in Figure 6.3. Finally, while decomposing the face image into random noise structures may be preferable, it can pique the interest of an

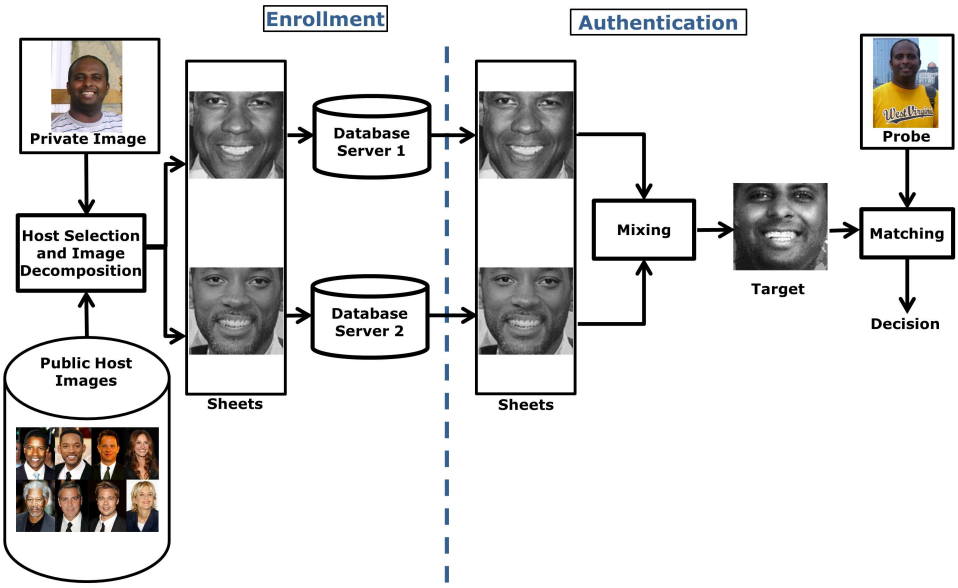


Figure 6.1: Proposed approach for de-identifying and storing a face image

eavesdropper by suggesting the existence of secret data.

Additionally, the proposed approach addresses the following template protection requirements [27][126].

(1) Diversity: Since different applications can adopt different sets of host images for encrypting the same private face image, cross-matching across applications to reveal the identity of a private face image will be difficult.

(2) Revocability: If the private data is deemed to be compromised, then it can be decomposed again into two new sheets based on new host images. However, in reality, break-ins to a server are very hard to detect when the attacker simply steals certain information without modifying the stored data. To strengthen security, the decomposing operation can be periodically invoked at regular time intervals.

(3) Security: It is computationally hard to obtain the private biometric image from the individual stored sheets due to the use of visual cryptography. Furthermore, the private image is revealed only when both sheets are simultaneously available. By using distributed servers to store the sheets, the possibility of obtaining the original private image is minimized. There have been numerous efforts in the literature to guarantee that the data stored in distributed databases are protected from unauthorized modification and inaccurate updates (e.g., [127]).

(4) Performance: As will be shown in the experiments section, the recognition performance due

to the reconstructed image is not significantly degraded after decryption.

The rest of the chapter is organized as follows. In Section 6.2 a basic introduction to visual cryptography and its extensions are presented. Section 6.3 discuss the proposed approach for face images. Section 6.4 reports the experimental results and Section 6.5 summarizes the chapter.

6.2 Visual Cryptography

One of the best known techniques to protect data such as biometric templates [128] is Cryptography. It is the art of sending and receiving encrypted messages that can be decrypted only by the sender or the receiver. Encryption and decryption are accomplished by using mathematical algorithms in such a way that no one but the intended recipient can decrypt and read the message. Naor and Shamir [129] introduced the Visual Cryptography Scheme (VCS) as a simple and secure way to allow the secret sharing of images without any cryptographic computations. VCS is a cryptographic technique that allows for the encryption of visual information such that decryption can be performed using the human visual system. The basic scheme is referred to as the k-out-of-n visual cryptography scheme which is denoted as (k, n) VCS [129]. Given an original binary image T, it is encrypted in n images, such that:

$$T = S_{h_1} \oplus S_{h_2} \oplus S_{h_3} \oplus \ldots \oplus S_{h_k} \tag{6.1}$$

where $\oplus$ is a boolean operation, S_{h_i}, $h_i \in 1, 2, ..., k$ is an image which appears as white noise, $k \leq n$, and n is the number of noisy images. It is difficult to decipher the secret image T using individual S_{h_i}'s [129]. The encryption is undertaken in such a way that k or more out of the n generated images are necessary for reconstructing the original image T.

In the case of $(2, 2)$ VCS, each pixel P in the original image is encrypted into two sub-pixels called shares. Figure 6.2 denotes the shares of a white pixel and a black pixel. Note that the choice of shares for a white and black pixel is randomly determined (there are two choices available for each pixel). Neither shares provide any clue about the original pixel since different pixels in the secret image will be encrypted using independent random choices. When the two shares are superimposed, the value of the original pixel P can be determined. If P is a black pixel, we get two black sub-pixels; if it is a white pixel, we get one black sub-pixel and one white sub-pixel.

Therefore, the reconstructed image will be twice the width of the original secret image and there will be a 50% loss in contrast [129]. However, the original image will become visible.

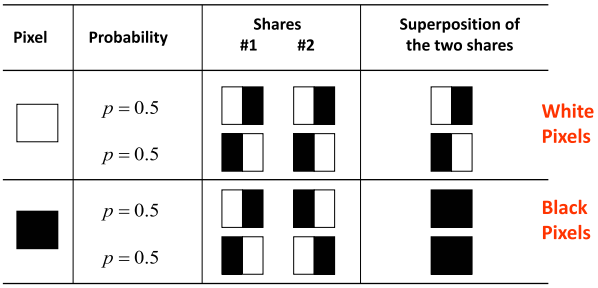


Figure 6.2: Illustration of a 2-out-of-2 VCS scheme with 2 sub-pixels construction

In 2002, Nakajima and Yamaguchi [11] presented a 2-out-of-2 Extended Visual Cryptography Scheme for natural images. They suggested a theoretical framework for encoding a natural image in innocuous images as illustrated in Figures 6.3 and 6.4. This is known as the Gray-level Extended Visual Cryptography Scheme (GEVCS). In this work, the extended visual cryptography scheme for grayscale images is used to secure face images by decomposing a private face image into two host images. Then, mixing, i.e., overlying the host images reveals the secret image. The basic Visual Cryptography scheme and its extension (GEVCS) are discussed in detail below.

Figure 6.3: Encryption of a private face image in two standard host images. (a) Camera-man image. (b) Lena image. (c) A private face image. (e) and (f) The two host images after visual encryption (two sheets). (g) Result of superimposing (e) and (f)

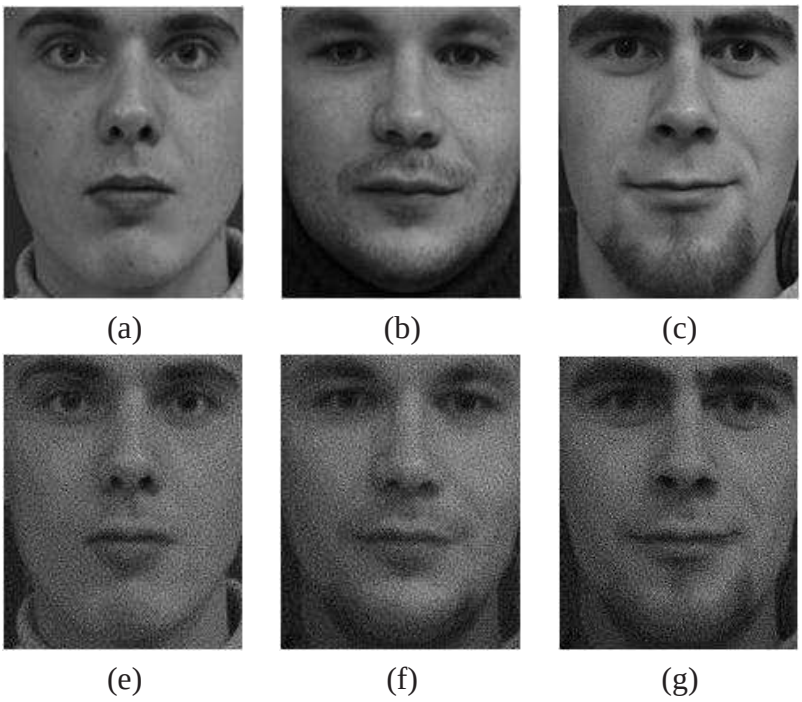


Figure 6.4: Encryption of a private face image in two pre-aligned and cropped face images. (a) and (b) are two host images. (c) is a private face image. (e) and (f) are the host images after visual encryption (two sheets). (g) is the result of mixing (e) and (f)

6.2.1 Visual Cryptography Scheme

There are a few basic definitions which need to be provided before formally defining the VCS model and its extensions.

(1) Secret image (O): The original image that has to be hidden. In our application, this is the private face image.

(2) Hosts ($H's$): These are the face images used to encrypt the secret image using the Gray-level Extended Visual Cryptography Scheme (GEVCS). In our application, these correspond to the face images in the public dataset.

(3) Sheets ($S's$): The secret image is encrypted into n sheet images which appear as random noise images (in the case of (k, n) VCS) or as a natural host image (in the case of GEVCS).

(4) Target (T): The image reconstructed by mixing (i.e., superimposing) the sheets.

(5) Sub-pixel: Each pixel P is divided into a certain number of sub-pixels during the encryption process.

(6) Pixel Expansion (m): The number of sub-pixels used by the sheet images to encode each pixel of the original image.

(7) Shares: Each pixel is encrypted by n collections of m black-and-white sub-pixels. These collections of sub-pixels are known as shares.

(8) Relative Contrast (α): The difference in intensity measure between a black pixel and a white pixel in the target image.

(9) OR-ed m-vector (V): An $n \times m$ matrix is transformed to an m-dimensional vector by applying the boolean OR operation across each of the m columns.

(10) Hamming weight ($H(V)$): The number of '1' bits in a binary vector V.

The k-out-of-n VCS deals with binary images. Each pixel is reproduced as n shares with each share consisting of m sub-pixels. This can be represented and described by an $n \times m$ boolean matrix B= [b_{ij}] where b_{ij} = 1 if and only if the j^{th} sub-pixel in the i^{th} share is black. The B matrix is selected randomly from one of two collections of $n \times m$ boolean matrices C_0 and C_1; the size of each collection is r. If the pixel P in the secret image is a white pixel, one of the matrices in C_0 is randomly chosen; if it is a black pixel, a matrix from C_1 is randomly chosen. Upon overlaying these shares, a gray level for the pixel P of the target image becomes visible and it is proportional to the Hamming weight, $H(V)$, of the OR-ed m-vector V for a given matrix B. It is interpreted visually as black if $H(V) \geq d$ and as white if $H(V) < d - \alpha m$ for some fixed threshold $1 \leq d \leq m$ and relative difference $\alpha > 0$. The contrast of the target is the difference between the minimum $H(V)$ value of a black pixel and the maximum allowed $H(V)$ value for a white pixel, which is proportional to the relative contrast (α) and the pixel expansion (m). The scheme is considered valid if the following three conditions are satisfied.

Condition (1) For any matrix B in C_0, the OR operation on any k of the n rows satisfies $H(V) < d - \alpha m$.

Condition (2): For any matrix B in C_1, the OR operation on any k of the n rows satisfies $H(V) \geq d$.

Condition (3): Consider extracting q rows, $q < k$, from two matrices, $B_0 \in C_0$ and $B_1 \in C_1$ resulting in new matrices B'_0 and B'_1. Then, B'_0 and B'_1 are indistinguishable in that there exists a permutation of columns of B'_0 which would result in B'_1. In other words, any $q \times m$ matrix $B_0 \in C_0$ and $B_1 \in C_1$ are identical up to a column permutation.

Conditions (1) and (2) define the image contrast due to VCS. Condition (3) imparts the security property of a (k, n) VCS which states that the careful examination of fewer than k shares will not provide information about the original pixel P. Therefore, the important parameters of the

scheme are the following. First, the number of sub-pixels in a share (m); this parameter represents the loss in resolution from the original image to the resultant target image and it needs to be as small as possible such that the target image is still visible. In addition, the m sub-pixels need to be in the form of a $v \times v$ matrix where $v \in \mathbb{N}$ in order to preserve the aspect ratio of the original image. Second, α, which is the relative difference in the Hamming weight of the combined shares corresponding to a white pixel and that of a black pixel in the original image; this parameter represents the loss in contrast and it needs to be as large as possible to ensure visibility of the target pixel. Finally, the size of the collection of C_0 and C_1, r, which represents the number of possibilities for B. This parameter does not directly affect the quality of the target image.

The scheme can be illustrated by a $(2, 2)$ VCS example which is shown in Figure 6.5. One pixel of the original image corresponds to four pixels in each share. Therefore, six patterns of shares are possible. Based on this, the following collection of matrices are defined:

$C_0 = \{$all the matrices obtained by permuting the columns of $\begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{bmatrix}\}$

$C_1 = \{$all the matrices obtained by permuting the columns of $\begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}\}$

This 2-out-of-2 visual cryptography scheme has the parameters m = 4, $\alpha = 1/2$ and r = 6. A secret image is encrypted by selecting shares in the following manner. If the pixel of the secret binary image is white, the same pattern of four pixels for both shares is randomly selected which is equivalent to randomly selecting a boolean matrix B from the collection C_0. If the pixel of the original image is black, a complementary pair of patterns is randomly picked which is equivalent to selecting a boolean matrix B from the collection C_1. Condition (1) and (2) can be easily tested to validate this (2,2) VCS. The last condition which is related to the security of the scheme can be verified by taking any row from $B_0 \in C_0$ and $B_1 \in C_1$ and observing that they have the same frequency of black and white values.

6.2.2 Gray-level Extended Visual Cryptography Scheme (GEVCS)

VCS allows one to encode a secret image into n sheet images, each revealing no information about the original. Since these sheets appear as a random set of pixels, they may pique the curiosity of an interceptor by suggesting the existence of a secret image. To mitigate this concern, the sheets could be reformulated as natural images as stated by Naor and Shamir [129]. Ateniese

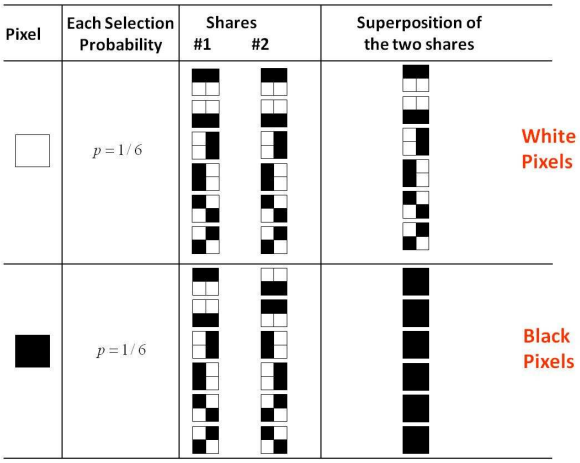


Figure 6.5: Illustration of a 2-out-of-2 scheme with 4 sub-pixel construction

et al. [130] introduced such a framework known as the Extended Visual Cryptography scheme. Nakajima and Yamaguchi [11] proposed a theoretical framework to apply Extended Visual Cryptography on grayscale images (GEVCS) and also introduced a method to enhance the contrast of the target images. The Gray-level Extended Visual Cryptography Scheme (GEVCS) operates by changing the dynamic range of the original and host images, transforming the gray-level images into meaningful binary images (also known as halftoned images) and then applying a boolean operation on the halftoned pixels of the two hosts and the original image. However, some of these pixels (in the host and the original) have to be further modified. This is explained in more detail below.

Digital Halftoning and Pixel Expansion

Digital Halftoning is a technique for transforming a digital gray-scale image to an array of binary values represented as dots in the printing process [131]. Error diffusion is a type of halftoning technique in which the quantization error of a pixel is distributed to neighboring pixels which have not yet been processed. Floyd and Steinberg [132] described a system for performing error diffusion on digital images based on a simple kernel. Their algorithm could also be used to produce output images with more than two levels. So, rather than using a single threshold to produce a binary output, the closest permitted level is determined and the error, if any, is diffused to the neighboring pixels according to the chosen kernel. Therefore, grayscale images are quantized to a number of levels equalling the number of sub-pixels per share, m. During the dithering process

at the pixel level, any continuous tone pixel is expanded to a matrix of black and white sub-pixels defined by the gray level of the original pixel. The proportion of white sub-pixels in this matrix is referred to as pixel transparency. In our application, the host images used for encrypting a private face image and the private image itself are converted to halftoned images.

Encryption

The encryption process is applied on a pixel-by-pixel basis using the three halftoned images (the two hosts and the original image). The arrangement of the sub-pixels in the shares of both the hosts has to be controlled such that the required transparency (the number of white sub-pixels) of the target pixel is obtained. The arrangement is determined based on the pixel transparencies triplet. (t_1, t_2, t_T). t_1, t_2 and t_T are transparencies of the entire sub-pixel region for share 1, share 2 and the target, respectively.

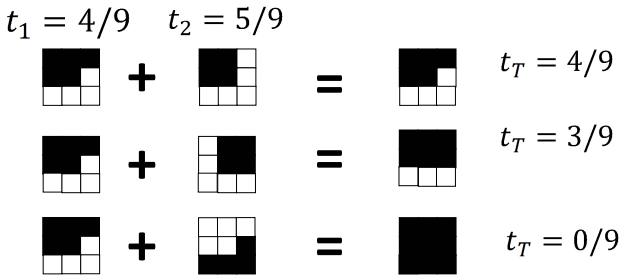


Figure 6.6: Examples of sub-pixel arrangement

The security of the scheme is also important. Therefore, during encryption, a Boolean matrix B is randomly selected from a set of 2 x m Boolean matrices $C_{t_T}^{t_1,t_2}$ for every pixel in the original image. This is the primary difference between this scheme and Naor-Shamir's scheme: in the latter only a single collection of matrices is required which depends on the number of hosts and the pixel expansion (m). Nakajima and Yamaguchi describe in detail the method to compute this collection of Boolean matrices [11].

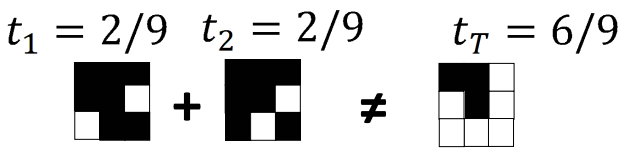


Figure 6.7: Example of impossible arrangements

However, as shown in Figure 6.7, there are cases when the required transparency for the corresponding pixel in the target image cannot be obtained, no matter how the shared sub-pixels are rearranged. Therefore, to determine if it is possible to obtain the target transparency by rearranging the transparent (white) sub-pixels in the shares, the target transparency must be within the following range (condition (T1)) [11]:

$$t_T \in [max(0, (t_1 + t_2 - 1)), min(t_1, t_2)], \tag{6.2}$$

where, t_1, t_2 and $t_T (\in [0, 1])$ are the transparencies of the entire pixel region for share 1, share 2 and the target, respectively. The range of each of these transparencies for the entire image corresponds to the dynamic range of the pixel intensities of the respective images. Assuming that the dynamic ranges of the transparencies of the two sheets are the same, $[L, U] \subseteq [0, 1]$, all the triplets, (t_1, t_2, t_T), would satisfy condition (T1) if and only if the dynamic range of the target fulfils condition (T2) [11]:

$$t_T \in [max(0, (2U - 1)), L]. \tag{6.3}$$

Nakajima and Yamaguchi [11] described a method to enhance the image quality (contrast) and decrease the number of violated triplets by performing an adaptive dynamic range compression. In their method, the dynamic range of the sheets and the target are modified as $t_1, t_2 \in [L, L + K] \subseteq [0, 1]$and $t_T \in [0, K] \subseteq [0, 1]$, respectively, where L denotes the lower bound of the sheets' dynamic range and K is a fixed value. It is clear that 0 is the most appropriate value for the lower bound of the target to ensure that the target is darker than both sheets [11]. However, after enhancing the contrast, it is necessary to consider condition (T1) again before encryption. Thus, if a triplet violates condition (T1), the gray levels of the conflicting triplets are adjusted and the resulting errors diffused to the nearby pixels. Consequently, both halftoning and encryption are done simultaneously to facilitate this adjustment.

To perform this adjustment, a $3D$-space is defined using the transparencies of the pixels in the three images: the x-axis represents the transparencies of the pixels in share 1, the y-axis represents the transparencies of the pixels in share 2 and the z-axis represents the transparencies of the pixels in the target image. Any point in this space is characterized by a triplet representing transparencies in the three images. The volume corresponding to the points for which reconstruction is possible (Figure 6.6) is determined. Every point outside this volume is adjusted. Assume a point

$p'(t'_1, t'_2, t'_T)$ outside the determined volume. To encrypt this triplet without degrading the images, p' will be replaced with p" where $p"(t"_1, t"_2, t"_T)$ is the closest point to p' in the constructed volume. Thus, the transparencies of the corresponding pixels in share 1, share 2, and target will become $t"_1, t"_2$ and $t"_T$, respectively. If condition (T1) is violated, the errors are calculated and diffused using an error-diffusion algorithm to the nearby pixels. These steps are summarized in Figure 6.8.

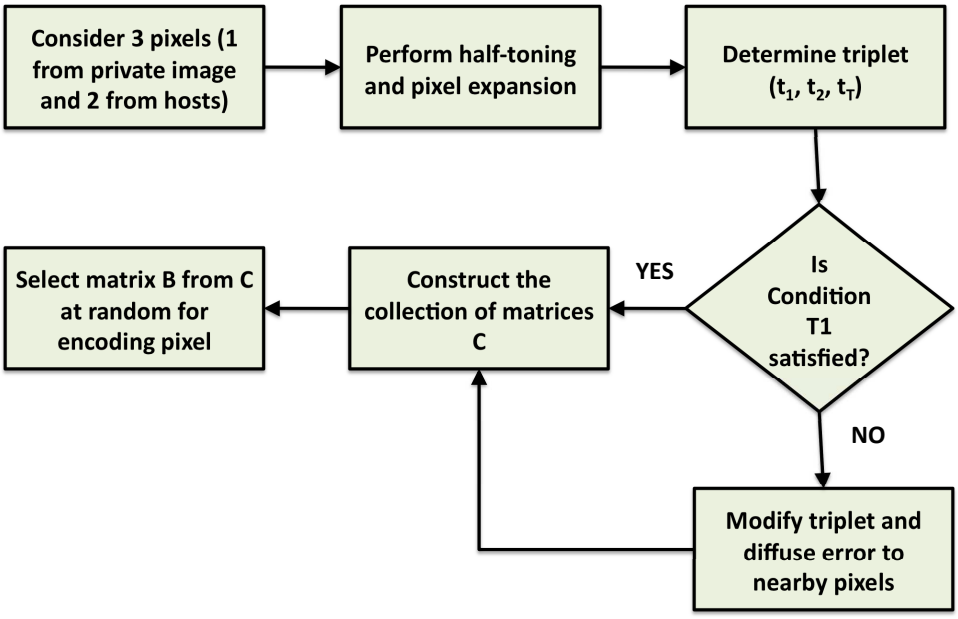


Figure 6.8: Flowchart for illustrating GEVCS at the pixel-level

6.3 Securing A Private Face Image by Mixing Host Images

Let $P = \{H_1, H_2, \ldots, H_N\}$ be the public dataset containing a set of candidate host images that can hide the assigned private face image, O. The first task is to select two host images H_i and H_j, $i \neq j$ and $i, j = 1, 2, \ldots N$ from P. Note that due to variations in face geometry and texture between the images in the public dataset and the private face image, the impact of the target image on the sheet images and vice versa may become perceptible. This issue can be mitigated if the host images for a particular private image are carefully chosen. Figure 6.9 shows the block diagram that illustrates the key steps of the proposed approach. These steps will be explained in

more detail in the following sub-sections.

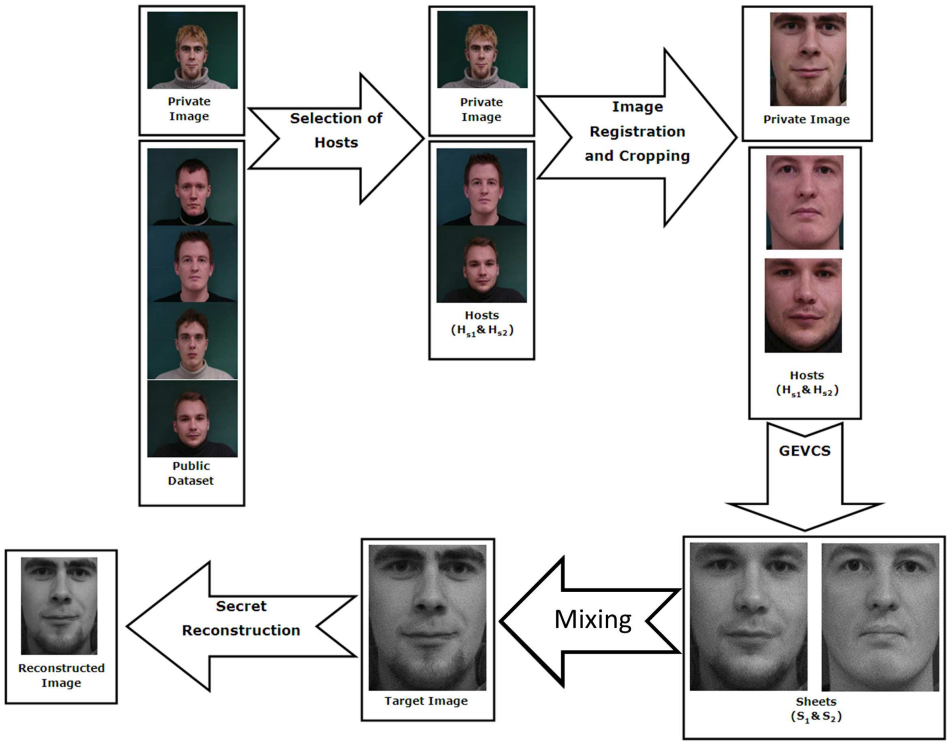


Figure 6.9: Block diagram of the proposed approach for storing and matching face images

6.3.1 Active Appearance Model

The proposed approach essentially selects host images that are most likely to be compatible with the private image based on geometry and appearance. But the similarity measures from an automated face recognition systems are not adequate to select the compatible host face images from a public dataset. In this work, the Verilook SDK[†] is used to generate the similarity scores. We found that the similarity score between the private image and a candidate host image in a public dataset is small or almost equal zero, because it is an impostor score form the preceptive of a face matcher. So using a face matcher are not the suitable way to select compatible hosts. Therefore, an Active Appearance Model (AAM) [133] that characterizes the shape and texture of the face is utilized to determine the similarity between the private face image and candidate host images (Figure 6.9). The steps for building the AAM and using it for locating predefined landmarks on face features, as shown in Figure 6.10, is discussed in detail in [134] and [133] and

[†]http://www.neurotechnology.com

is summarized below.

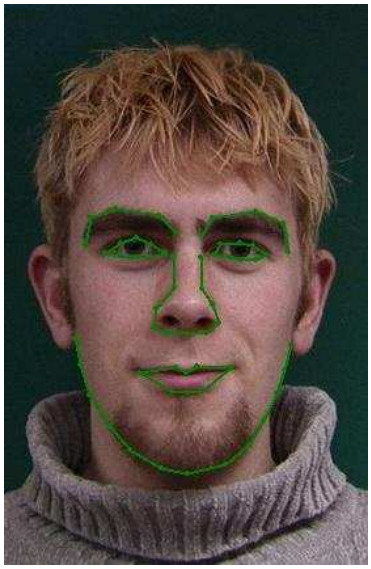


Figure 6.10: Example of an annotated face

Building the Active Appearance Model

Four steps are needed for building a basic Active Appearance Model (AAM) from a set of training images.

Annotate the training set First, for each face image in the training dataset, its face features are annotated manually by landmarks of a pre-defined shape. Each shape X_j is stored in a vector format, where $j \in 1, .., s$ and s is the number of training images. This representation does not include any information about the connection between landmarks. Thus,

$$X_j = [x_{1j}, x_{2j}, x_{3j}, \ldots, x_{nj}, y_{1j}, y_{2j}, y_{3j}, \ldots y_{nj}]^T, \tag{6.4}$$

where n is the number of landmarks used to locate and annotate face features.

Building the shape model A shape alignment process is performed to remove the effects of affine transformations (translation, scaling and rotation). Then the Principle Component Analysis (PCA) is used to construct a simple linear model of shape variability across the training images:

$$\mathbf{X} = \bar{\mathbf{X}} + \Phi_s \mathbf{b_s}. \tag{6.5}$$

Here, $\bar{\mathbf{X}}$ is the mean shape vector, Φ_s is a matrix describing the modes of variation derived from the training set and $\mathbf{b_s}$ is the shape model parameters vector.

Building the texture model All images in the training set are warped to the mean shape by utilizing the annotated landmarks. Next, the pixel values in each warped image is consolidated to create a texture vector. Then, a photometric normalization is used to minimize the effects of lighting changes on the texture vector. The normalized texture vector is $\mathbf{g}$:

$$\mathbf{g} = [g_1, g_2, g_3 \ldots g_m]^T, \tag{6.6}$$

where m is the number of pixels within the image. Then, PCA is used to linearly model the texture vectors as in equation6.7.

$$\mathbf{g} = \bar{\mathbf{g}} + \Phi_g \mathbf{b_g}. \tag{6.7}$$

Here, $\bar{\mathbf{g}}$ is the mean texture vector, Φ_g is the modes of variation matrix and $\mathbf{b_g}$ is the texture model parameter vector.

Building the combined Active Appearance Model (AAM) Shape and texture are often correlated [134] and, so, PCA is once again used to construct a compact model from $\mathbf{X}$ and $\mathbf{g}$ resulting in a set of combined parameters C. This helps in synthesizing an image with a given shape $\mathbf{X}$ and texture $\mathbf{g}$ using one set of parameters $\mathbf{C}$ as shown below.

$$\mathbf{X} = \bar{\mathbf{X}} + \Phi_s \mathbf{C}, \tag{6.8}$$

$$\mathbf{g} = \bar{\mathbf{g}} + \Phi_g \mathbf{C}. \tag{6.9}$$

Annotating an Image

A randomly selected template model is initially generated and an image based on the corresponding model parameters is synthesized. The error between the input image (I_{image}, that has to be annotated) and the synthesized image ($I_{synthesized}$) needs to be minimized. The solution is found by varying two sets of parameters: the combined model parameters $\mathbf{C}$ and the pose parameters (translation, scaling and rotation).

6.3.2 Selection of Hosts

For selecting compatible hosts, the cost of registering (aligning) each image in the public dataset with the private image is computed as T_c. These costs are sorted in order to locate two host images, H_{s1} and H_{s2}, which have the smallest registration cost. However, as will be shown in the experiments section, this cost alone is not sufficient. So the texture is used as an additional criteria and the cost associated with this is denoted as A_c. Therefore, the final cost F_c, which is associated with each host image, is the sum of the normalized transformation cost T_c and the normalized appearance cost A_c. The simple min-max normalization technique is used to normalize both costs.

Transformation Cost T_c

This cost measures the amount of geometric transformation necessary to align two images based on the annotated landmarks generated by the AAM. Given the set of correspondences between these finite sets of points on two face images, a transformation $T : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ can be estimated to map any point from one set to the other. While there are several choices for modeling this geometric transformation, the thin plate spline (TPS) model is used [135]. The transformation cost, T_c, is the measure of how much transformation is needed to align the two face images by utilizing the thin plate spline model, which is the bending energy necessary to perform the transformation.

Appearance Cost A_c

First, the private face image (O) and the host image (H) are normalized by warping them to the mean shape, $\bar{\mathbf{X}}$, resulting in shape-free texture images O' and H'. Figures 6.11 shows an example of a shape-free image for a private face image. This normalization step uses the mean shape computed during the AAM training phase. Each shape-free image is represented as a texture vector (equation 6.6).

Both O' and H' can be expressed by the texture model parameter vector, $\mathbf{b_g}$. In order to get these basis vectors, each image is projected onto the texture space by using the stored modes of variation, Φ_g:

$$\mathbf{b_g} = \Phi_g^{-1} \cdot \{\mathbf{g} - \bar{\mathbf{g}}\} \tag{6.10}$$

Figure 6.11: The shape-free image of annotated face image in Figure 6.10

The appearance cost, A_c, is defined as the Manhattan distance between the basis vectors corresponding to O' and H'.

6.3.3 Image Registration and Cropping

In this step, the global affine transformation component of the thin plate spline model is used to align the two selected host images (H_{s1} ,H_{s2}) with the secret image (O). Next, the aligned hosts and the secret image are cropped to capture only the facial features which have been located by AAM as illustrated in Figure 6.10.

6.3.4 Secret Encryption and Reconstruction By Mixing Host Images

GEVCS is used to hide the secret image, O, in the two host images H_{s1} and H_{s2} resulting in two sheets denoted as S_1 and S_2, respectively. S_1 and S_2 are mixed by superimposing them in order to reveal the secret private image. The final target image is obtained by the reconstruction process that reverses the pixel expansion step to retain the original image size.

6.4 Experiments and Results

The performance of the proposed technique was tested on two different databases: the IMM and XM2VTS databases. These databases were used since the facial landmarks of individual images were annotated and available online. These annotations were necessary for the AAM scheme. The IMM Face Database [136] is an annotated database containing 6 face images each of 40 different subjects; 3 of the frontal face images per subject were used in the experiments. 27

subjects were used to construct the private dataset and the remaining 13 were used as the public dataset. The XM2VTS frontal image database [105] consists of 8 frontal face images each of 295 subjects. 192 of these subjects were used to construct the private dataset and 91 subjects were used to construct the pubic dataset. The remaining subjects were excluded because several of their face images could not be processed by the commercial matcher. The composition of the public dataset is shown in Figure 6.12. Figure 6.13 shows examples of the proposed approach when dataset D in Figure 6.12 is used as the public dataset (here $[L = 0, K = 0.75]$ and the pixel expansion value m is 36). The AAM for each database was constructed using the face images (one per subject) from the public dataset.

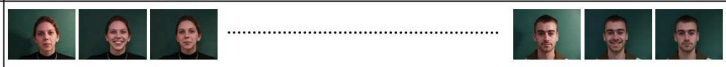
In the following experiments, the match scores were generated using the Verilook SDK[‡]. In order to establish a baseline, the images in the private database were first matched against each other. This resulted in an EER of $\sim$ 6% for the IMM database and $\sim$ 2% for the XM2VTS database.

Computational time We evaluated the time complexity of the approach using $Matlab$®-2013a on a PC with $Intel$® i7 CPU @2.8GHz and 8GB memory. The elapsed time of decomposing a private face image into two host image is 1.5 seconds.

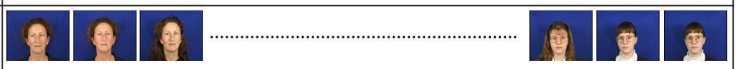
6.4.1 Experiment 1

In this experiment, the impact of varying the number of images in the public dataset was investigated (datasets A, B, C, D and E were used). The selection of hosts from the public dataset was based only on the transformation cost. The experiment consisted of matching the mixed private images against each other. EERs using the 5 public datasets are shown in Tables 6.1 and 6.2. For the IMM database in Table 6.1, it is clear that adding more images to the public dataset initially improves the result. However, dataset E results in the worst EER with respect to the other datasets. This drop in performance could be attributed to the inclusion of an individual with a beard in the public dataset: the absence of the appearance cost led to the selection of this host image even for those private face images that did not possess a beard, thereby affecting the mixed images.

[‡]http://www.neurotechnology.com

Name of Dataset	Images in the Public dataset
Dataset A	
Dataset B	
Dataset C	
Dataset D	
Dataset E	
Dataset F	
Dataset G	 39 face images, three different frontal face images for each subject.

(a) IMM Database

Name of Dataset	Images in the Public dataset
Dataset A	
Dataset B	
Dataset C	
Dataset D	
Dataset E	
Dataset F	 91 face images
Dataset G	 273 face images, three different frontal face images for each subject.

(b) XM2VTS Database

Figure 6.12: Images in the public datasets for both the IMM and XM2VTS databases

Table 6.1: Equal Error Rates (%) when using different public datasets with K = 0.567 and m=16

Dataset	IMM Database	XM2VTS Database
A	9.7	21.9
B	7.7	21.8
C	6.3	21.7
D	5.6	21.4
E	11.4	22

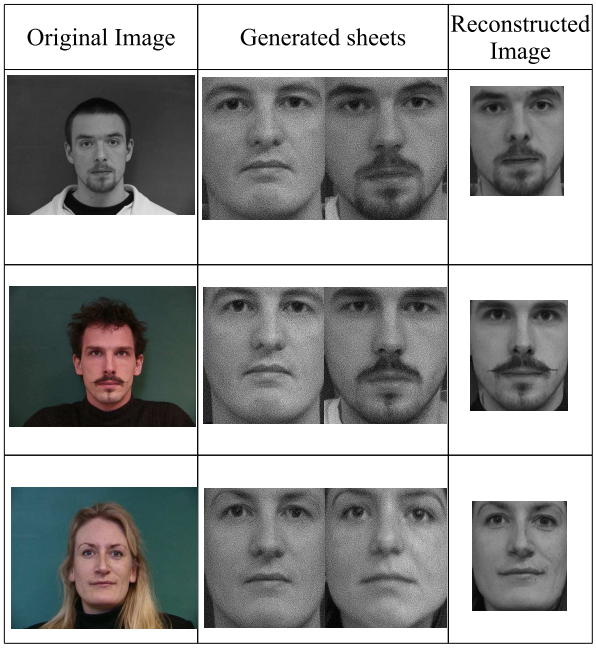


Figure 6.13: Illustration of the proposed approach using images from the IMM Database

Table 6.2: Equal Error Rates (%) when using different public datasets with K = 0.875 and m=36

Dataset	IMM Database	XM2VTS Database
A	2.2	6.4
B	2.1	6.4
C	2	6.2
D	2	6
E	3.4	10.2

6.4.2 Experiment 2

In this experiment, the appearance cost was added to the criterion to select the host images and it is clear that this solves the problem encountered in experiment 1. Dataset E is used in this experiment to select the hosts (H_1, H_2). Tables 6.3 and 6.4 show the EERs of the mixed images when host images are selected using (a) the transformation cost T_c only and (b) the sum of the normalized transformation cost T_c and appearance cost A_c.

From both the above experiments it is also apparent that K = 0.875 and m=36 results in better matching performance.

Table 6.3: Equal Error Rates (%) when different selection criteria are used with K = 0.567 and m=16

Selection Criteria	IMM Database	XM2VTS Database
T_c	11.4	22
T_c + A_c	8	21

Table 6.4: Equal Error Rates (%) when different selection criteria are used with K = 0.875 and m=36

Selection Criteria	IMM Database	XM2VTS Database
T_c	3.4	10.2
T_c + A_c	2	6

6.4.3 Experiment 3

The purpose of this experiment was to determine if the mixed face images upon reconstruction could be successfully matched against the original private face images. To evaluate this, the public Dataset A in Figure 6.12, consisting of two fixed face images as hosts, was used. For each subject in the private dataset, one frontal face image was selected[§] as the secret image to be encrypted by mixing the two host face images. The visual cryptography scheme was invoked with contrast $K = 0.875$ and a pixel expansion factor of $m = 36$. The mixed images were observed to match very well with the original images resulting in an EER of $\sim$ 0% in the case of the IMM database and 0.5% in the case of the XM2VTS database. On other hand, when either of the sheets were matched against the original images, the resultant EERs were greater than 45%.

[§]In the case of IMM database, the face sample exhibiting neutral expression and diffuse light was selected

6.4.4 Experiment 4

The purpose of this experiment was to determine if the mixed face images could be successfully matched against those images in the private dataset that were not used in Experiment 3. To establish this, for each subject in the reconstructed dataset, N frontal face images were chosen from the private database to assemble the gallery ($N = 2$ for IMM and $N = 3$ for XM2VTS). The matching exercise consisted of comparing the reconstructed face images (from Experiment 1) against these gallery images (not used in Experiment 1). An EER of $\sim$ 2% was obtained for the IMM database. This performance, in this case, was even better than that of the original images (EER $\sim$ 6%). The improvement could be due to the contrast enhancement of the private face images that occurs when increasing the dynamic range of the sheets resulting in improved quality of the reconstructed secret image. For the XM2VTS database, the obtained EER was $\sim$ 6% which is still comparable with the 2% obtained when matching the original images.

6.4.5 Experiment 5

By using public Dataset D and m = 16 and 36, sheet images were created with different contrast values: $K = 0.567, 0.6888, 0.75, 0.875$. Table 6.5 reports the Equal Error Rates (EERs) for these different values of K. Here, the matching procedure was the same as that of Experiment 4. For both databases, $K = 0.875$ results in better performance than the other values. This improvement could be due to the contrast enhancement of the target images that occurs by increasing the dynamic range of the sheets and, consequently, the quality of the mixed image.

Table 6.5: Equal Error Rates (%) for different values of K and m = 16. The choice of K is based on [11]

K	IMM Database	XM2VTS Database
0.567	10.7	21.4
0.6888	6.5	17.5
0.75	7.8	16
0.875	5.9	15

6.4.6 Experiment 6

Next, the effect of pixel expansion on the final reconstructed image was tested. Figure 6.14 shows that details of the sheets can appear on the final image for higher values of m. The impact

of m on matching performance is shown in Table 6.7. Here, the matching procedure was the same as that of Experiment 4. The host images were selected from Dataset D with $K = 0.567$. As shown in Figure 6.14, the pixel expansion value affects the number of gray-levels in the reconstructed image, and this impacts the amount of detail appearing in it. Therefore, when m is 100, the visual details of the sheet images appear on the reconstructed image resulting in a drop in overall performance.

(a) m=4 (b) m=16 (c) m=36 (d) m=100

Figure 6.14: Examples of mixed images for a subject with different values for the pixel expansion factor, m

6.4.7 Experiment 7

In this experiment, the possibility of exposing the identity of the secret image by using the sheet images in the matching process is investigated. For this experiment, the sheet images for 3

Table 6.6: Equal Error Rates (%) for different values of K and m = 36. The choice of K is based on [11]

K	IMM Database	XM2VTS Database
0.567	5.3	12.6
0.6888	5	6.5
0.75	4	6.3
0.875	2	6

Table 6.7: Equal Error Rates for different values of m (%)

m	IMM Database	XM2VTS Database
4	23.5	41
16	10.7	21.4
36	5.3	12.6
100	8	11

different face samples of the same subject were first computed. Next, the mixed images and the corresponding sheets were independently used in the matching process (i.e., sheet image 1 of all the private images were matched against each other; sheet image 2 of all the private images were matched against each other; mixed images of all the private images were matched against each other). Figure 6.15 shows that each subject in the private dataset has three reconstructed images. The public datasets used in this experiments were datasets A, F and G. This experiment resulted in three EERs: the first was a result of using the reconstructed mixed images for matching, while the second and the third EERs were a result of using the first sheet and second sheet, respectively, for matching. The results in Table 6.8 confirm the difficulty of exposing the identity of the secret face image by using the sheets alone.

Note that experiment 7 involves automatic host selection from the public dataset based on the registration cost, F_c, described earlier. The positive impact of automatic host selection is seen in Figure 6.15 where the selected host images (sheets) and the secret image are observed to have compatible expressions.

6.4.8 Experiment 8

Different applications may employ different public datasets for host image selection. Thus, the hosts selected for encrypting an individual's face image can differ across applications. This experiment seeks to confirm that cross-matching of the stored sheets across applications (and inferring identities) will not be feasible. To demonstrate this, the possibility of using host images from *different* public databases for encrypting the same identity (i.e., face image) was investigated. The experiment was set up as follows. Two face samples of each of the 192 subjects in the XM2VTS private dataset were randomly selected. For an arbitrary subject, let O_1 and O_2 denote the two face samples that were selected. Further, let O_1 be encrypted into sheets S_1^{IMM} and S_2^{IMM} using a public dataset from the IMM database. Similarly, let O_2 be encrypted into sheets S_1^{XM2VTS} and S_2^{XM2VTS} using a public dataset from the XM2VTS database. Let T_1 and T_2 denote the reconstructed face images pertaining to O_1 and O_2, respectively. The following matching exercises were conducted: (a) S_1^{IMM} against S_1^{XM2VTS}; (b) S_1^{IMM} against S_2^{XM2VTS}; (c) S_2^{IMM} against S_1^{XM2VTS}; (d) S_2^{IMM} against S_2^{XM2VTS}; (e) T_1 against T_2. The public datasets used in this experiment was the same as Experiment 7 (i.e., Datasets A , F and G). Table 6.9 shows the EERs for these matching experiments and it is clear that it is difficult to perform cross-

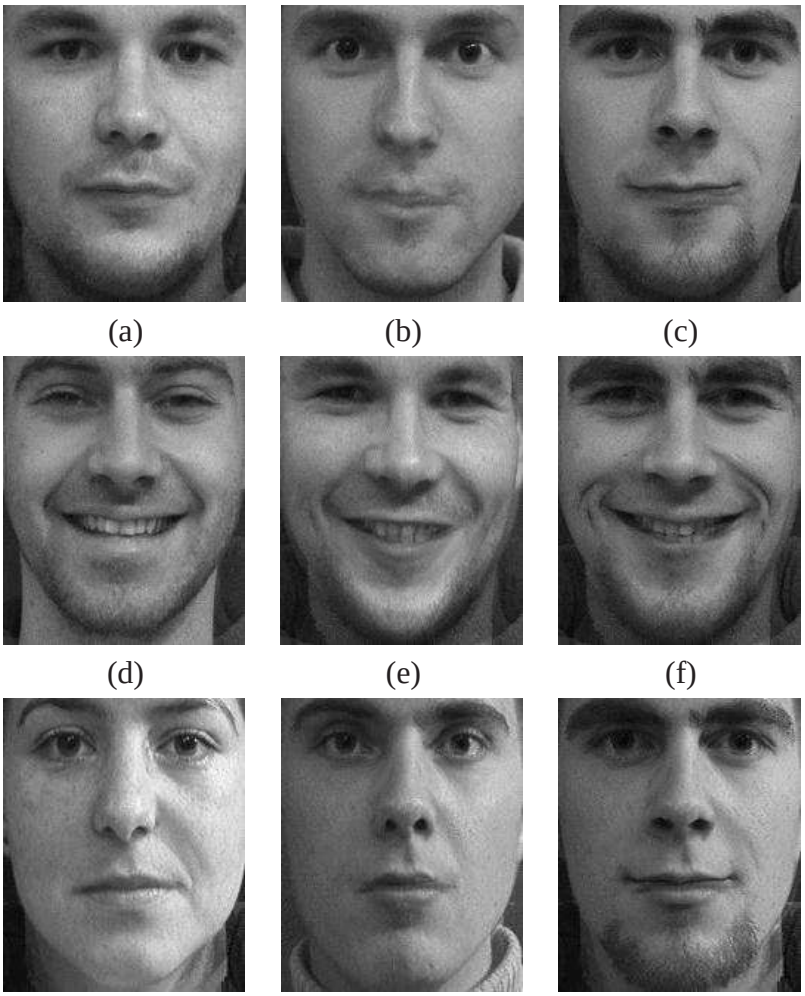


Figure 6.15: Examples from experiment 7 where (a), (d) and (g) are the first sheets and (b), (e) and (h) are the second sheets. (c), (f) and (i) are the corresponding mixed face images

Table 6.8: Equal Error Rates (%) for Experiment 7. Experiments confirm the difficulty of using sheet images to reveal the secret image

	EER (%)
Mixed vs Mixed	2.4
Sheet 1 vs Sheet 1	44.7
Sheet 2 vs Sheet 2	44.2

(a) IMM Database: Dataset A

	EER (%)
Mixed vs Mixed	6.2
Sheet 1 vs Sheet 1	36.0
Sheet 2 vs Sheet 2	33.8

(b) XM2VTS Database: Dataset A

	EER (%)
Mixed vs Mixed	7.4
Sheet 1 vs Sheet 1	35.7
Sheet 2 vs Sheet 2	40

(c) IMM Database: Dataset F

	EER (%)
Mixed vs Mixed	8.2
Sheet 1 vs Sheet 1	31.7
Sheet 2 vs Sheet 2	38.3

(d) XM2VTS Database: Dataset F

	EER (%)
Mixed vs Mixed	6.8
Sheet 1 vs Sheet 1	33.8
Sheet 2 vs Sheet 2	39.5

(e) IMM Database: Dataset G

	EER (%)
Mixed vs Mixed	9.2
Sheet 1 vs Sheet 1	37.8
Sheet 2 vs Sheet 2	39.3

(f) XM2VTS Database: Dataset G

matching across different applications. However, when the corresponding reconstructed images ($m = 36$ and $K = 0.875$) are compared, the resulting EER suggests the possibility of successful matching.

Table 6.9: Equal Error Rates (%) for Experiment 8

Matching	EER (%)
S_1^{IMM} vs S_1^{XM2VTS}	47.4
S_1^{IMM} vs S_2^{XM2VTS}	48.2
S_2^{IMM} vs S_1^{XM2VTS}	50
S_2^{IMM} vs S_2^{XM2VTS}	46.3
T_1 vs T_2	13.6

(a) Datasets A

Matching	EER (%)
S_1^{IMM} vs S_1^{XM2VTS}	49
S_1^{IMM} vs S_2^{XM2VTS}	49.5
S_2^{IMM} vs S_1^{XM2VTS}	49
S_2^{IMM} vs S_2^{XM2VTS}	48.5
T_1 vs T_2	4.4

(b) Datasets F

Matching	EER (%)
S_1^{IMM} vs S_1^{XM2VTS}	48.3
S_1^{IMM} vs S_2^{XM2VTS}	50
S_2^{IMM} vs S_1^{XM2VTS}	48.6
S_2^{IMM} vs S_2^{XM2VTS}	50
T_1 vs T_2	4.8

(c) Datasets G

6.5 Summary

This chapter explored the possibility of decomposing faces for imparting privacy to private face images. The contribution of this chapter includes a methodology to protect the privacy of a face database by decomposing an input private face image into two independent face images such that the private face image can be reconstructed by mixing these modified host face images. The proposed algorithm selects the host images that are most likely to be compatible with the secret image based on geometry and appearance. GEVCS is then used to encrypt the private image in the selected host images. It is observed that when the encrypted host images (i.e., sheets) are mixed they are similar to the original private images. The study on the effect of various parameters (K and m) on the matching performance suggests that there is indeed a relation

between the quality of the reconstructed secret and these parameters. Finally, experimental results demonstrate the difficulty of exposing the identity of the secret image by using only one of the sheets; further individual sheets cannot be used to perform cross-matching between different applications. Increasing the pixel expansion factor, m, can lead to an increase in the storage requirements for the sheets. In the recent literature there have been some efforts to develop a visual cryptography scheme without pixel expansion [137] [138]. But no such scheme currently exists for generating sheets that are not random noisy images. Thus, more work is necessary to handle this problem.

6.5.1 Research Contribution

- Introducing a new privacy structure for de-identifying face images.
- Proposing an approach to utilize visual cryptography schemes for face privacy.

Chapter 7

Finger'iris'print

7.1 Introduction

In the previous chapters we discussed different approaches to generate a mixed biometric image. The mixed images have the following properties: (a) incorporate characteristics from component images, and (b) can be used directly in the feature extraction and matching stages of an existing biometric system. However, we only discussed approaches to mix images of a single biometric trait (i.e., mixing fingerprints, faces and irises). In this chapter, we demonstrate that the concept of mixing biometrics can be extended to mix *different* biometric traits such as fingerprints with irises. By mixing samples from these two different traits, a new, unique, and revocable biometric image can be generated. Specifically, the goal here is generating a new mixed image that inherits its uniqueness from a finger impression and an iris image. The uniqueness of a fingerprint is determined by the topographic relief of its ridge structure and the presence of certain ridge irregularities termed as minutiae. Whereas the human iris, which is the annular part between the pupil and the white sclera, contains intricate textural details. The iris and fingerprint patterns are believed to be unique to each eye and to each finger, respectively. Therefore, the process of iris or fingerprint recognition is done by analyzing these patterns and comparing it with that of an entry in the gallery.

The mixing process of fingerprint and iris begins by decomposing the fingerprint image into two different components, viz., the continuous and spiral components. The continuous component defines the local ridge orientation, and the spiral component characterizes the minutiae locations [74]. Next, the spiral component of the iris is computed by locating minutiae on the iris

texture; in order to avoid loss of information due to normalization [66], a segmented iris image (i.e., annular region) is used directly in the minutiae determination step. A Gabor filter is applied to capture the iris texture and the minutiae considered to be the centroids of iris regions that result in consistent filter responses. Finally, the continuous component of the fingerprint is combined with the spiral of the iris image to create a new biometric image. This new and unique biometric image appears as a fingerprint image and has been denoted in this work as a *fing'iris'print*.

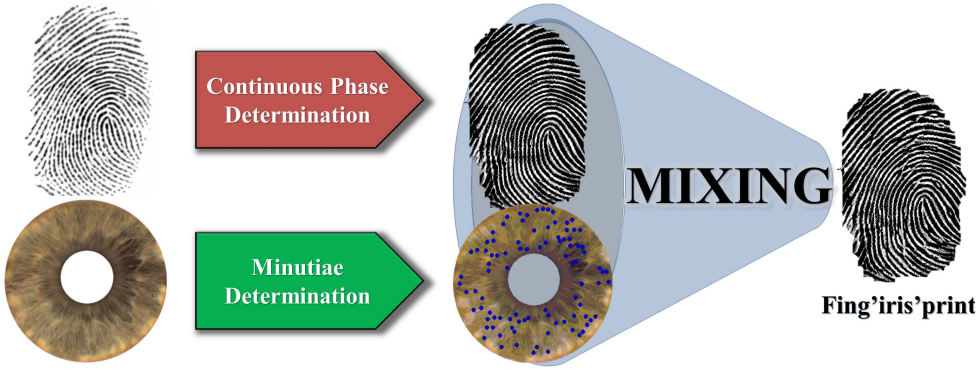


Figure 7.1: Illustration of the proposed approach to generate a *fing'iris'print*.

This work confirms that (a) a new biometric image (i.e., fing'iris'print) can be created by fusing two different biometric traits (i.e., a fingerprint and an iris); (b) the new fing'iris'print can potentially be used for authentication; and (c) it can be used to obscure the information present in an individual's fingerprint and iris images, and can be stored in a central database instead of the original templates. Therefore, this approach can be used to generate a cancelable template (i.e., the template can be reset if the fing'iris'print is compromised), and different applications can mix different fingers with an iris image from the right or left eye, thereby ensuring that the identities enrolled in one application cannot be matched against the identities in another application.

Section 7.2 presents the proposed approach of generating a fing'iris'print by fusing a fingerprint with an iris image. Section 7.3 reports the experimental results and section 7.4 summarizes the chapter.

7.2 Generating Fing'iris'print

Fingerprints have been fused with irises at the feature [139, 140], score [141], rank [142] levels. The only work, based on our knowledge, that generates an image by fusing the raw

data of different biometric traits is Noore et al.'s work [58]. They developed a fusion algorithm based on multi-level discrete wavelet transform to fuse images of four biometric traits (i.e., face, iris, fingerprint, and signature). The resultant image [58] is a scrambled image that cannot be used directly in the matching step; therefore, special reconstruction procedures are needed to reconstruct the original images and to perform authentication. This exposes the original biometric templates to eavesdroppers during every identification/verification attempt.

In contrast, the mixed image generated in our work (i.e., fing'iris'print) has the following properties: (a) incorporates characteristics from the fingerprint and iris images, (b) can be used directly in the feature extraction and matching stages of an existing fingerprint system, and (c) obscures the identity of the component images. As shown in Figure 7.1, there are three distinct phases in the generation of a fing'iris'print: determining continuous phase of the fingerprint, determining minutiae of the iris, and mixing.

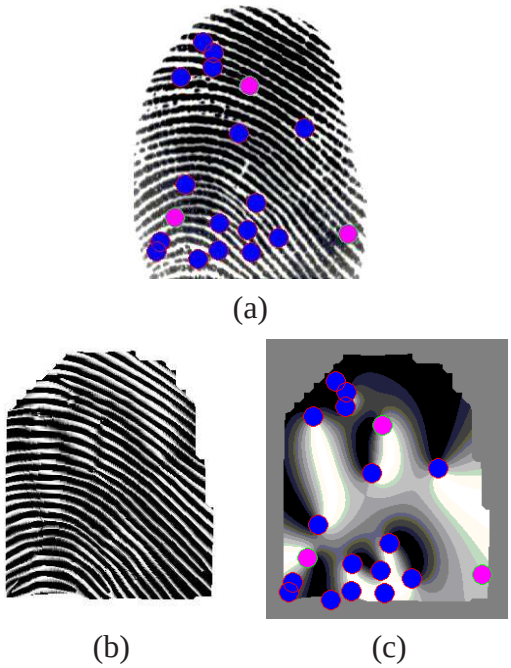
7.2.1 Continuous Phase Determination

The ridge flow of a fingerprint can be represented as a 2D Amplitude and Frequency Modulated (AM-FM) signal [74]:

$$F(x,y) = a(x,y) + b(x,y)cos(\Psi^F(x,y)) + n(x,y), \tag{7.1}$$

where $F(x,y)$ is the intensity of the original image at (x,y), $a(x,y)$ is the intensity offset, $b(x,y)$ is the amplitude, $\Psi^F(x,y)$ is the phase and $n(x,y)$ is the noise. Based on the Helmholtz Decomposition Theorem [75], the phase can be uniquely decomposed into the continuous phase and the spiral phase, $\Psi^F i(x,y) = \psi_c^F(x,y) + \psi_s^F(x,y)$. As shown in Figure 7.2, the cosine of the continuous phase, i.e., the continuous component $cos(\psi_c^F(x,y))$, defines the local ridge orientation, and the cosine of the spiral phase, i.e., the spiral component $cos(\psi_s^F(x,y))$, characterizes the minutiae locations.

Since ridges and minutiae can be completely determined by the phase [74], we are only interested in $\Psi^F(x,y)$. The other three parameters in Equation (7.1) contribute to the realistic textural appearance of the fingerprint. To mix a fingerprint with an iris, first, the phase $\Psi^F(x,y)$ of the component fingerprint must be reliably estimated; this is termed as demodulation [74] [143]. Next, the phase ($\Psi^F(x,y)$) of the fingerprint image is decomposed into a continuous



(a) (b) (c)

Figure 7.2: Decomposing a fingerprint. (a) A fingerprint image. (b) Continuous component, $\cos(\psi_c^F(x,y))$. (c) Spiral component, $\cos(\psi_s^F(x,y))$. The blue and pink dots represent ridge endings and ridge bifurcations, respectively.

phase ($\psi_c^F(x,y)$) and a spiral phase ($\psi_s^F(x,y)$) [75]. The continuous phase $\psi_c^F(x,y)$ pertaining to the fingerprint will be added during the mixing process to the generated spiral phase ($\psi_c^I(x,y)$) from the iris image in order to construct the fing'iris'print image. In the following sub-section, the detailed steps for locating iris minutiae, in order to generate the spiral phase ($\psi_s^I(x,y)$) of an iris image, is described.

7.2.2 Iris Minutiae

Before discussing our proposed approach for determining iris minutiae, the properties of ideal iris minutiae is defined below.

Repeatability Given two iris images of the same eye, acquired during different sessions, the determined minutia should be found in the same position in both images. Specifically, determination of iris minutiae should be invariant and robust regardless of the presence of noise (e.g., eyelids, eyelashes, reflections, or occlusions); the use of different sensors; and the different image properties like size, compression, or format.

Distinctiveness Given two iris images of two different eyes, the determined minutiae should have good discriminatory ability over different eyes. Specifically, any two persons should be sufficiently different in terms of iris minutiae.

Quantity The number of determined iris minutiae should be sufficient, such that the generated fing'iris'print has a reasonable number of minutiae to be processed by a fingerprint matcher. Specifically, the average number of minutiae of fing'iris'prints should be close to the average number of minutiae in the original fingerprints (i.e., for FVC2002-db2, which is the database used in our experiments, the average number of minutiae is 45). Ideally, the number of detected minutiae should be adaptable over a large range by simple and intuitive parameters. Also they should reflect the textural content of an iris image to provide a compact representation.

In fingerprint literature [35], there are many well established techniques that extract " ideal"* minutiae from fingerprint images. These techniques are reasonably stable and robust to fingerprint impression conditions. *But* the texture of an iris is varied, random, and scrambled in comparison with the texture of a fingerprint; so it is difficult to use the same minutiae-extraction approaches that are widely used in fingerprint recognition systems. Therefore, rather than using a few typical minutial structures to describe the local texture information, our approach will utilize existing iris processing methods.

Daugman's phase encoding technique is the most common and promising among the different iris recognition approaches [64] [65] [69]. Figure 7.3 shows the processing chain of the traditional iris recognition system following Daugman's approach [70]. First, a camera acquires an image of an eye and the iris annular region is segmented. Next, the annular iris is geometrically normalized, i.e., unwrapped from raw image coordinates to pseudo-polar coordinates. A texture filter is applied to the normalized iris image, and the filter responses are quantized into a binary representation (i.e., iris code). The comparison between two iris codes is done by computing the fractional hamming distance as a dissimilarity measure.

In this chapter, the same technique will be utilized to extract the local features of the iris image, i.e., iris minutiae. However, in our approach, the filter will be applied to the annular iris region due to the following reasons.

- During the mixing step (see section 7.2.3), the fingerprint component (i.e., the continuous

*Based on the enumerated properties of ideal minutiae.

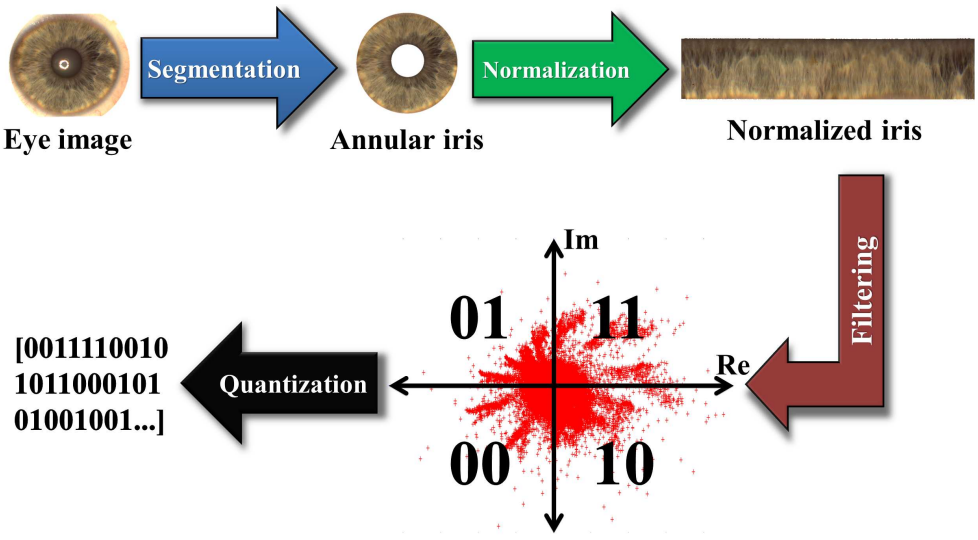


Figure 7.3: Diagram of Daugman's approach for encoding an iris image.

phase) is pre-aligned to a common coordinates, such that its core (where ridge orientation changes abruptly) is at the center of the new image. Therefore, by using the annular iris image, after the mixing process, the locations of the iris minutiae points will be around the core point of the fing'iris'print which will be similar to the distribution of minutiae in a fingerprint [†].

- Unwrapping the annular iris into normalized image can be regarded as a sampling process, with the inherent possibility of aliasing that may deteriorate the discriminability of the iris's texture.

The steps for extracting iris minutiae from annular iris images are described below.

Applying a Gabor filter on the annular iris

A log-Gabor filter is used for capturing the local feature of the annular iris image. So, first, a Fourier transform is applied to the iris image, and then the values are multiplied by the log-Gabor filter. The frequency response of a log-Gabor filter is given as;

$$G(f) = \exp \frac{-(log(f/f_0))^2}{(log(\sigma/f_0))^2}, \tag{7.2}$$

[†]Zhu et al. [144] show that minutiae are not uniformly distributed but tend to cluster around core points.

where f_o represents the center frequency and σ is the bandwidth of the filter [116]. Next, an inverse Fourier transform is applied, yielding a complex-valued filter response for each point in the image (see Figure 7.4). In a traditional iris recognition system, each complex number is quantized to two bits; the first bit is set to one if the real part of the complex number is positive, and the second bit is set to one if the imaginary part is positive. In our work, the goal is finding key responses that can be noted as iris minutiae from the responses of the whole image. Therefore, we applied a sequence of pruning steps on the iris responses in order to locate consistent responses that will be utilized to locate iris minutiae.

Pruning filter responses

Our goal is to prune the phase responses to find the most consistent and reliable points that can be marked as iris minutiae. The concept that some responses are less consistent than others was first mentioned by Bolle et al. [145]. Since then, many researchers have investigated and studied the consistence (i.e., fragility) of the phase responses [146]. Hollingsworth et al. [146] demonstrated that by masking responses near the axes of the complex plane could dramatically decrease the false rejection rate of an iris template. Note that, the inconsistency of the responses does not measure the stability or robustness of the iris texture. The inconsistency of an iris region occurs when the inner product between the log-Gabor filter and a particular region of the annular iris produces a response with a value close to the complex plane axes [147] [146].

Therefore, as shown in Figure 7.4, to prune the responses of an iris as suggested in [147] [146], a series of adaptive thresholding was performed (see Figure 7.4). The first pruning step eliminated responses corresponding to a portion of filter responses ($th_c\%$) closest to the axes. Then, to exclude the outliers that, in some cases, are due to the specular highlights, a second threshold parameter (th_o) is set for that purpose: real and imaginary responses greater than $th_o\%$ of the filter responses are eliminated.

The final pruning is done by considering responses only in a portion of the first quadrant of the complex plane. Specifically, the responses with angles outside the interval α_θ were eliminated. In this work, we have empirically set the values of these parameters to be as follows: $th_c = 90\%$, $th_o = 99\%$, and $\alpha_\theta = [30, 60]$.

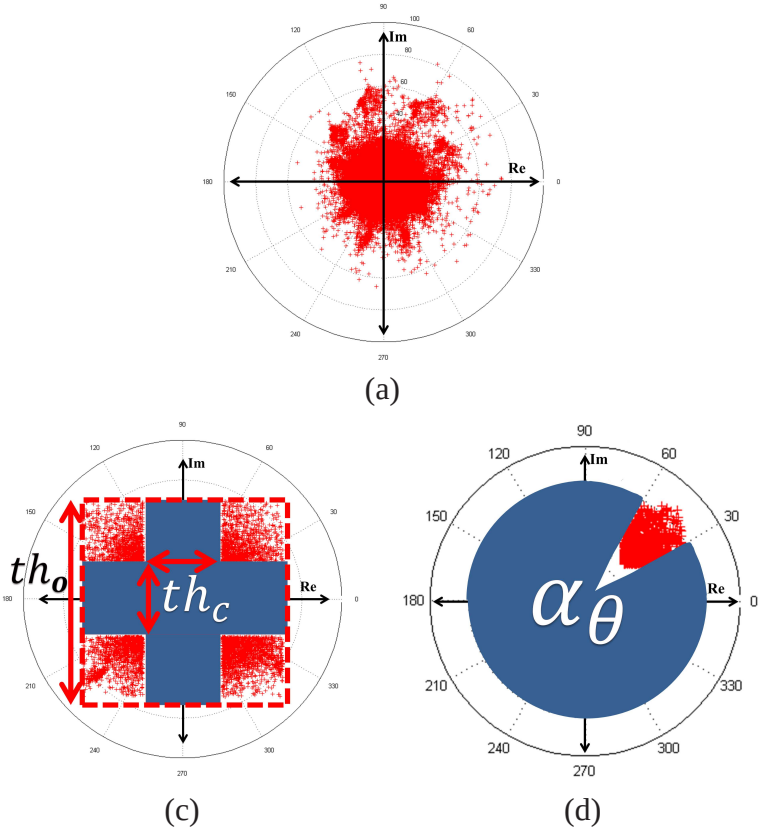
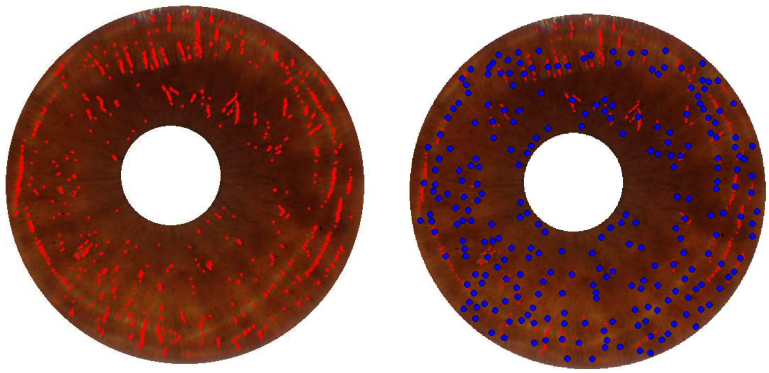


Figure 7.4: Polar plots of the complex-valued responses of an annular iris image after (b) applying the filter, (c) pruning using th_c and th_o, and (d) pruning using α_θ.

Locating the minutiae

After pruning, the number of remaining responses is still large because of the rich detailed texture of the iris image. Figure 7.5-b shows the remaining responses on the annular iris image. To resolve this, the remaining responses have to be broken up into meaningful subsets. Therefore, a hierarchical clustering algorithm that constructs clusters based on distance connectivity, where the cutoff distance is 5, is used to cluster the remaining iris responses. Finally, the barycenter of these clusters is considered to be the iris minutiae.



(a) (b)

Figure 7.5: Annotating the phase responses on the annular iris after (a) pruning (i.e., red dots) and (b) finding the barycenter of their clusters (i.e., blue dots).

Constructing the iris spiral phase (ψ_s^I)

To mix an iris with the continuous phase of a fingerprint, a spiral phase, $\psi_s^I(x, y)$ which corresponds to the minutiae of the iris has to be computed:

$$\psi_s^I(x, y) = \sum_{n=1}^{N} p_n \tan^{-1}((x - x_n)/(y - y_n)), \tag{7.3}$$

where p_n is the polarity value, x_n and y_n denote the coordinates of the n^{th} minutia, and N denotes the total number of iris minutiae.

Appending this function to a continuous phase of a fingerprint image will cause phase jumps resulting in minutiae. Depending upon the polarity value (+1 or -1), a minutia is generated on the ridge pattern. The relation between the polarity, p_n, and the occurrence of ridge ending or bifurcation is dependent on the gradient direction of the cosine of the continuous phase. Hence,

the spiral phase causes an abrupt change in the local fringe density by either inserting or deleting a ridge based on the polarity and the appending location within the continuous phase. In this work, the polarity value will be set to +1. This means that the type of a fing'iris'print minutia (i.e., ending or bifurcation) will be based on the fingerprint pattern at the appending location of an iris minutia.

Moreover, as shown in Figure 7.6-a, appending the spiral phase of an annular iris to a continuous phase of a fingerprint can result in a visually unrealistic fingerprint image. This is due to difference in the spatial distribution and frequencies of iris minutiae and real fingerprint minutiae. To resolve this issue (see Figure 7.6-b), the spiral phase of each iris minutia is tuned to the corresponding local ridge frequency and orientation of the fingerprint component by using Gabor bandpass filters [78].

The form of the Gabor elementary function that is oriented at an angle 0° is given as;

$$G(x,y) = \exp\left\{-\frac{1}{2}\left[\frac{x^2}{{\delta^2}_x} + \frac{y^2}{{\delta^2}_y}\right]\right\}\cos(2\pi f x), \tag{7.4}$$

where f represents the local ridge frequency of the fingerprint where iris minutia will be appended, and δ_x and δ_y are the space constants of the filter envelope along x and y axes, respectively. Their values determine the trade between enhancement and spurious artifacts. In this work, we have empirically set the values of δ_x and δ_y to be 5 (as suggested in [78]). Note that the filters have been tuned to the corresponding local ridge orientation of fingerprint component at the appended iris minutiae by rotating the elementary kernel.

7.2.3 Mixing

Prior to mixing, the continuous component of the fingerprint image is pre-aligned to a common coordinate system by utilizing a reference point and its orientation. In this work, Nilsson et al.'s [148][149] approach to detect the reference points was adopted. This approach has the advantage of being able to extract the position and spatial orientation of the reference point simultaneously. The reference point is used to translate the component to the center of the annular iris image and its orientation is used to find a rotation angle about the reference point. This angle rotates the fingerprint component to make the reference orientation orthogonal to the horizontal axis.

(a) (b)

Figure 7.6: (a) An example of a fing'iris'print that looks unrealistic. (b) Enhancing the appearance by using Gabor bandpass filters tuned to the orientation and frequency of the continuous component.

Let F and I be a fingerprint and an annular iris image, respectively, $\psi_c^F(x, y)$ be the continuous component determined from F, and $\psi_s^I(x, y)$ be the spiral component determined from I. A fing'iris'print (MFI) can be generated as:

$$MFI = \cos(\psi_c + \psi_s). \tag{7.5}$$

The continuous phase of F is combined with the spiral phase of I which generates a new biometric image MFI.

7.3 Experiments and Discussion

The proposed approach to generate fing'iris'prints was tested using a fingerprint and an iris dataset. The iris dataset was taken from the UPOL [‡] iris database. The UPOL database has high quality iris images of the left and right eye of 64 users which are mostly unoccluded by eyelids or lashes. The used dataset consists of 2 samples of the left eye resulting in a total of 128 iris images which were manually segmented and converted to grayscale. In order to establish a baseline performance, an open source Matlab implementation [116] based on the Daugman's approach

[‡]http://www.inf.upol.cz/iris/

[117] was used to encode and match the irises. For each iris, one image was added to the probe set (P_I) and the other one was added to the gallery, G_I. Matching the probe set against the gallery set resulted in a rank-1 accuracy of $\sim 99\%$ and EER of $\sim 0\%$.

The fingerprint dataset was taken from the FVC2002-DB2 database. In this work, we used the first 2 impression of the first 64 fingers in the FVC2002-DB2 database resulting in a total of 128 fingerprint images (as in the case of the iris dataset). The baseline performance of the fingerprint dataset was determined by adding one impression of each finger to the probe set and the other to the gallery set. Matching the probe set (P_F) against the gallery set (G_F) by using the verifinger SDK[§] resulted in a rank-1 accuracy of $\sim 99\%$ and EER of $\sim 0\%$.

With regards to generating fing'iris'prints for obscuring the original component images, the following key questions are raised:

1. Can two mixed impressions pertaining to the same identity be successfully matched?
2. Can the original fingerprint and the fing'iris'print be linked?
3. Can the original iris and the fing'iris'print be linked?

It is essential to assure that the proposed approach prevents identity linking, by preventing the possibility of successfully matching the original fingerprint or iris image with the mixed image.

Computational time We evaluated the time complexity of the proposed approach using $Matlab$®-2013a on a PC with $Intel$® i7 CPU @2.8GHz and 8GB memory. As shown in Figure 7.1, there are three main steps for generating a fing'iris'print: Continuous phase Determination, Iris Minutiae Determination and Mixing. Table 7.1 shows the elapsed time of each step.

Table 7.1: Elapsed time of generating a fing'iris'print as shown in Figure 7.1

Task	Time (seconds)
Continuous phase Determination	10
Iris Minutiae Determination	0.5
Mixing	1
Total	11.5

[§]http://www.neurotechnology.com

7.3.1 Matching Performance

The purpose of this experiment was to report the matching performance of fing'iris'print. The annular iris of each eye in the probe set P_I were mixed with a fingerprint image from the probe set P_F resulting in a new probe set MFI_P consisting of 64 fing'iris'prints. The corresponding pairs of fingerprints in G_F were also mixed with annular iris in G_I resulting in a new gallery set MFI^G consisting of 64 fing'iris'prints. Figure 7.7 shows examples of mixed image. In this work, the parameters of the log-Gabor filter, i.e., $(1/f_o)$ the center wavelength and (σ/f_o) the bandwidth of the filter, were set to be 12 and 0.5, respectively. By matching the probe and gallery sets of fing'iris'prints, the obtained rank-1 accuracy was $\sim$ 92% and the EER was $\sim$ 10%. This indicates the possibility of matching fing'iris'prints. However, further work should be done to improve the rank-1 accuracy. Currently, different parameters values (i.e., th_c, th_o, α_{theta}, and clustering cutoff) along with different methods to locate iris minutiae are being examined. Note that the Gabor filter parameters have no noticeable effect on the results as shown in Tables 7.2 and 7.3.

Table 7.2: Equal Error Rates for different values of the center wavelength

$1/f_o$	EER (%)
6	10.3
12	10
18	11
24	11.7

Table 7.3: Equal Error Rates for different values of the bandwidth of the filter

σ/f_o	EER (%)
0.25	10.2
0.5	10
1.5	11
2	12

7.3.2 Exposing the original identities from fing'iris'prints

In this experiment, the possibility of exposing the identity of the FVC2002-DB2 fingerprint image or UPOL iris image by using the fing'iris'print images was investigated.

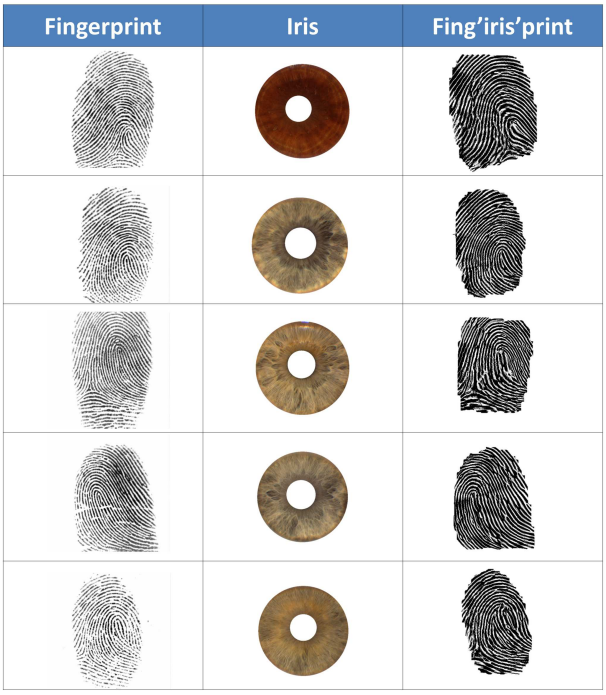


Figure 7.7: Examples of fing'iris'print where fingerprints are from the FVC2002-DB2 dataset and irises are from UPOL dataset.

First, the impressions in MFI_G were matched against the original fingerprint images in P_F. The resultant rank-1 accuracy was 0% and the EER was more than 43%. Second, the annular iris in P_I was matched against fing'iris'print impressions in MFI_G. But the mixed images are fingerprint images that share only the minutiae locations of the annular iris images. Therefore, to perform the experiment, the minutiae location of the fing'iris'print and the annular iris were matched using a point pattern matching algorithm utilizing the RANdom SAmple Consensus (RANSAC) method [150]. The resultant rank-1 accuracy was 0% and the EER was 48%.

These results suggest that the original identity cannot be easily deduced from the mixed image. However, more formal analysis of different security aspects (such as the non-invertiblity and cancelability of the approach) is necessary.

7.4 Summary

In this chapter, the concept of mixing biometrics was exploited in the context of mixing different biometric traits, i.e., fingerprints with irises. A fingerprint image and an annular iris image are mixed in order to generate a fing'iris'print image. This mixed image incorporates

characteristics from the original fingerprint impression and the orignal iris image, and can be used directly in the feature extraction and matching stages of an existing fingerprint system. To mix a fingerprint with an iris, the fingerprint is decomposed into two components, viz., the continuous and spiral phases , and iris minutiae is extracted in order to generate the iris spiral phase. In the final step of mixing, the continuous phase of the fingerprint is combined with the spiral phase of the annular iris image resulting in a new fingerprint image. Our experiments conducted on fingerprint and iris datasets show that (a) the new biometric image (i.e., fing'iris'print) can potentially be used for authentication, and (b) the original fingerprint and iris images cannot be easily matched with the mixed image.

7.4.1 Research Contribution

- Designing a new cancelability structure for fingerprint and iris templates.
- Generating a fingerprint image from a fingerprint and iris image.
- Proposing an approach to extract iris minutiae by utilizing the concept of bit fragility.

Chapter 8

Conclusions and Future Work

8.1 Conclusions

The emergence of biometrics has facilitated the rapid authentication of individuals based on their biological traits. In a biometric system, each reference template stored in the database is usually associated with only a single individual. While individuals can be independently authenticated based on their respective biometric templates, in this thesis we investigated whether a single biometric template can be generated from multiple individuals. In other words, we explored the possibility of generating a biometric template representing a joint identity that inherits its characteristics from two different individuals. Mixing biometrics refers to the process of generating a new biometric signal by fusing signals of different biometrics instances pertaining to a single individual or different individuals. The generated mixed image incorporates characteristics from the original biometrics images, and can be used directly in the feature extraction and matching stages of an existing biometric system. The utility of mixing biometrics was demonstrated in two different applications. The first application dealt with the issue of generating a joint digital identity. The second application dealt with the issue of biometric privacy, where the concept of mixing was used for de-identifying or obscuring biometric images.

After introducing the concept of mixing biometrics and its benefits in the first chapter, in the second chapter we gave a brief introduction to biometric traits considered in this thesis.

In the third chapter, a method to mix fingerprint images was presented. It was demonstrated that the concept of “mixing fingerprints” could be utilized to (a) generate a new identity by mixing two distinct fingerprints and (b) de-identify a fingerprint by mixing it with another fingerprint.

In the fourth chapter, a method to mix face images was introduced. It was demonstrated that the concept of "mixing faces" could be used to generate virtual identities. The mixed face image is the mid-face in the morphing continuum between the two component faces and its position on this continuum is specified by the mixing parameters. Our experiments showed that (a) the mixed face representing a new identity can potentially be used for authentication, (b) the mixed face has similarities with both the original faces, and (c) the proposed method can be utilized to generate a database of virtual identities.

In the fifth chapter, iris images were mixed in order to (a) generate a virtual identity and (b) generate mixed images that have similarities with both the component iris images. To mix two irises, horizontal seams were copied from normalized iris images after sorting them based on their importance in the images. Experiments on the CASIA-v3 dataset show that (a) the mixed iris representing a new identity can potentially be used for authentication, (b) the mixed iris is similar to the original irises, and (c) the proposed method can be utilized to generate a database of virtual identities from a fixed iris dataset.

In the sixth chapter, we explored the possibility of decomposing faces for imparting privacy to private face images. We proposed a novel method to protect the privacy of a face database by decomposing an input private face image into two independent face images such that the private face image can be reconstructed by mixing these modified host face images. The proposed algorithm selects the host images that are most likely to be compatible with the private image based on geometry and appearance. The difficulty of exposing the identity of the private image by using only one of the modified hosts was demonstrated; further, individual hosts cannot be used to perform cross-matching between different applications.

Finally, we extended the concept of mixing to mix instances of *different* biometric traits. Specifically, a fingerprint image and an annular iris image were mixed in order to generate a fing'iris'print. To mix a fingerprint with an iris, the fingerprint was decomposed into two component, viz., the continuous and spiral phases, and iris minutiae was extracted in order to generate the iris spiral phase. Extracting the iris minutiae was done by using a one-dimensional log-Gabor filter. The ensuing iris responses were pruned in order to locate a few iris points that were labeled as iris minutiae. In the final step of mixing, the continuous phase of the fingerprint is combined with the spiral phase of the annular iris image resulting in a new fingerprint image. Experiments showed that (a) the new biometric image (i.e., fing'iris'print) can potentially be used for authen-

tication, and (b) the original fingerprint and iris images cannot be easily matched with the mixed image.

8.2 Future Research

We conclude this thesis by suggesting possible ways in which the research presented here may be expanded.

- The concept of mixing can be further generalized to develop a group authentication system [151]. In such a system, biometric images of a group of individuals can be used for authentication. The group authentication can be designed for group-oriented applications. This could be used in scenarios where the authentication is no longer based on a single individual unlike most of the conventional biometric systems. In group authentication, access is granted only if k or more of the authorized individuals are simultaneously providing their biometric traits.

- The performances of mixing fingerprints and generating fing'iris'print can be enhanced and improved by exploring alternate algorithms for pre-aligning the biometric images, and for decomposing and representing the texture of fingerprints and irises.

- In the fourth chapter, we discussed a technique to mix face images to generate an interpersonal face image that is similar to the original face images. As future work, different approaches can be investigated to generate a face image that is *dissimilar* to the original face images. Also, the possibility of combining more than two face images has to be studied. Another application would be the deliberate distortion of the soft biometric attributes such as age, gender, race, etc. of a person's face image by mixing it with a public face image (e.g., a celebrity) that has opposite attributes, as shown in Figure 8.1. While this perturbs the soft biometric attributes of the face, the mixed image can still be used to match with another face image of the person. But a more formal analysis is needed to derive a privacy measure that can be utilized to validate the usability of the technique.

- In chapter 7, the experimental results suggested that the identity corresponding to the original iris and fingerprint images cannot be easily deduced from the mixed image. However,

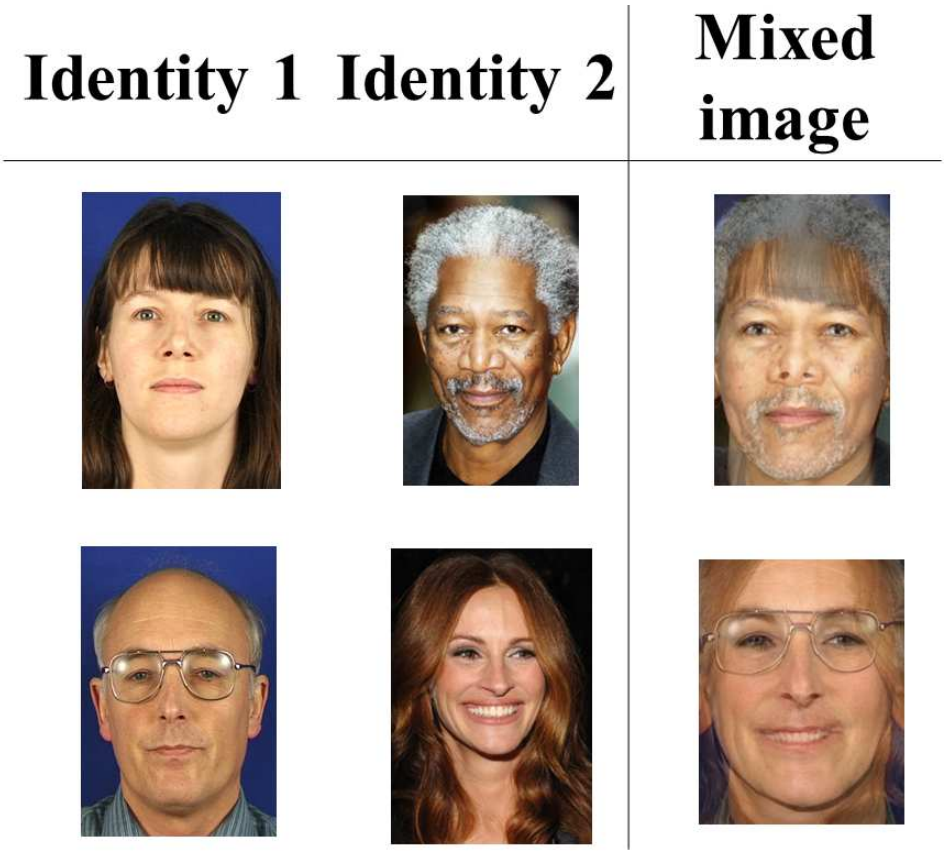


Figure 8.1: Examples of interpersonal face images. Here, the images to be mixed have different soft biometric attributes.

a more formal analysis of different security aspects (such as the non-invertiblity and cancelability of the approach) is necessary. Further, more investigation is needed to study if the similarity (i.e., compatibility) between the extracted iris minutiae and the component fingerprint minutiae could leak any information about the original fingerprint (i.e., the original identity). Therefore, in order to increase security and minimize the linkage, the similarity between the iris minutiae and the fingerprint should be measured and if there is a possibility to select between different pairs of irises and fingers, the pair with the least compatibility measure should be mixed.

Appendix A

Dissemination of Research Results

1. A. Othman and A. Ross, ”On Mixing Fingerprints,” IEEE Transactions on Information Forensics and Security (TIFS), Vol.8, Issue 1, pp. 260 - 267, January 2013.

2. A. Ross and A. Othman, ”Visual Cryptography for Biometric Privacy,” IEEE Transactions on Information Forensics and Security (TIFS), Vol. 6, Issue 1, pp. 70 - 81, March 2011.

3. A. Othman and A. Ross, ”Mixing Fingerprints For Generating Virtual Identities,” Proc. of IEEE International Workshop on Information Forensics and Security (WIFS), (Foz do Iguacu, Brazil), November/December 2011. Best Student Paper Award (Gold)

4. A. Ross and A. Othman, ”Mixing Fingerprints for Template Security and Privacy,” Proc. of the 19th European Signal Processing Conference (EUSIPCO), (Barcelona, Spain), August/September 2011.

5. A. Ross and A. Othman, Visual cryptography for face privacy, Proc. of SPIE Conference on Biometric Technology for Human Identification VII, (Orlando, USA), April 2010.

References

[1] Alphonse Bertillon, *Identification anthropométrique: instructions signalétiques*, Impr. administrative, 1893.

[2] Karl Pearson, *The life, letters and labours of Francis Galton*, vol. 3, CUP Archive, 1930.

[3] C Phéline, "Portraits en règle," *Identités: de Disderi au photomaton*, 1985.

[4] Brendan Klare and Anil K Jain, "On a taxonomy of facial features," in *Fourth IEEE International Conference on Biometrics: Theory Applications and Systems (BTAS)*. IEEE, 2010, pp. 1–8.

[5] S. Manvelyan, "Your beautiful eyes - http://www.surenmanvelyan.com," .

[6] Antoni Buades, Triet Le, Jean-Michel Morel, and Luminita Vese, "Cartoon+Texture Image Decomposition," *Image Processing On Line*, vol. 2011, 2011, `http://dx.doi.org/10.5201/ipol.2011.blmv_ct`.

[7] B. Hastings, "An integrated representation of fingerprint patterns," in 16^{th} *School of Computer Science & Software Engineering Research Conference, Yanchep, Western Australia*, June 2008.

[8] Marc Ghali, "Then and now - http://www.behance.net/gallery/then-now/9189373," .

[9] Ulric Collette, "Genetic portraits - http://genetic.ulriccollette.com//," .

[10] "Album cover of *Watch the throne*, jay-z and kanye west, defjam, 2011.," .

[11] M. Nakajima and Y. Yamaguchi, "Extended visual cryptography for natural images," *Journal of WSCG*, vol. 10, no. 2, pp. 303–310, 2002.

[12] E. Mordini and S. Massari, "Body, biometrics and identity," *Bioethics*, vol. 22, no. 9, pp. 488–498, 2008.

[13] J. Ashbourn, *Guide to Biometrics for Large-Scale Systems: Technological, Operational, and User-Related Factors*, Springer London, 2011.

[14] A.K. Jain, P.J. Flynn, and A. Ross, *Handbook of Biometrics*, Springer, 2007.

[15] A.K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no. 1, pp. 4 – 20, jan. 2004.

[16] M.R. Leary and J.P. Tangney, *Handbook of self and identity*, The Guilford Press, 2002.

[17] R. Clarke, "The digital persona and its application to data surveillance," *The information society*, vol. 10, no. 2, pp. 77–92, 1994.

[18] G. Agamben and translated from the French by Stuart J. Murray, "No to biopolitical tattooing," *Communication and Critical/Cultural Studies*, vol. 5, no. 2, pp. 201–202, 2008.

[19] A.K. Jain, A. Ross, and U. Uludag, "Biometric template security: Challenges and solutions," in *Proceedings of European Signal Processing Conference (EUSIPCO)*, 2005, pp. 469–472.

[20] "Nuclear weapon accident response procedures manual, Defense Threat Reduction Agency, 2005," `http://www.dtic.mil/whs/directives/corres/pdf/315008m.pdf/`.

[21] A. Ross, J. Shah, and A.K. Jain, "From template to image: reconstructing fingerprints from minutiae points," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 29, no. 4, pp. 544–560, 2007.

[22] R. Cappelli, A. Lumini, D. Maio, and D. Maltoni, "Fingerprint image reconstruction from standard templates," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 29, no. 9, pp. 1489 –1503, sept. 2007.

[23] Jianjiang Feng and Anil K. Jain, "Fingerprint reconstruction: From minutiae to phase," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 33, no. 2, pp. 209 –223, Feb. 2011.

[24] Sheng Li and Alex C. Kot, "A novel system for fingerprint privacy protection," in *7th International Conference on Information Assurance and Security (IAS)*, dec. 2011, pp. 262 –266.

[25] S. Venugopalan and M. Savvides, "How to generate spoofed irises from an iris code template," *IEEE Transactions on Information Forensics and Security*, , no. 99, pp. 1–1, 2011.

[26] U. Uludag, S. Pankanti, S. Prabhakar, and A.K. Jain, "Biometric cryptosystems: issues and challenges," *Proceedings of the IEEE*, vol. 92, no. 6, pp. 948–960, 2004.

[27] A.K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," *EURASIP Journal on Advances in Signal Processing*, vol. 2008, pp. 1–17, 2008.

[28] C. Rathgeb and A. Uhl, "A survey on biometric cryptosystems and cancelable biometrics," *EURASIP Journal on Information Security*, , no. 1, pp. 1–25, 2011.

[29] G. I. Davida, Y. Frankel, and B. J. Matt, "On enabling secure applications through off-line biometric identification," in *IEEE Symposium on Security and Privacy*, 1998, pp. 148–157.

[30] N.K. Ratha, J.H. Connell, and R.M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," *IBM Systems Journal*, vol. 40, no. 3, pp. 614–634, 2001.

[31] A.A. Ross, K. Nandakumar, and A.K. Jain, *Handbook of Multibiometrics*, Springer-Verlag New York Inc, 2006.

[32] K. Nandakumar, *Multibiometric systems: Fusion strategies and template security*, Ph.D. thesis, Michigan State University, 2008.

[33] R.S. Blum and Z. Liu, *Multi-sensor image fusion and its applications*, CRC, 2005.

[34] A.K. Jain and S.Z. Li, *Encyclopedia of biometrics*, vol. 1, Springer, 2009.

[35] D. Maltoni, D. Maio, A.K. Jain, and S. Prabhakar, *Handbook of fingerprint recognition*, Springer-Verlag New York Inc, 2009.

[36] NK Ratha, JH Connell, and RM Bolle, "Image mosaicing for rolled fingerprint construction," in *Proceedings Fourteenth International Conference on Pattern Recognition (ICPR)*, aug. 1998, vol. 2, pp. 1651 –1653.

[37] A. Jain and A. Ross, "Fingerprint mosaicking," in *Proceedings IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP)*, may 2002, vol. 4, pp. IV–4064 –IV–4067.

[38] YS Moon, HW Yeung, KC Chan, and SO Chan, "Template synthesis and image mosaicking for fingerprint registration: an experimental study," in *Proceedings IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP)*, may 2004, vol. 5, pp. V – 409–12 vol.5.

[39] K. Choi, H. Choi, and J. Kim, "Fingerprint mosaicking by rolling and sliding," in *Audio- and Video-Based Biometric Person Authentication*. Springer, 2005, pp. 260–269.

[40] A. Ross, S. Shah, and J. Shah, "Image versus feature mosaicing: A case study in fingerprints," in *Proceedings of SPIE Conference on Biometric Technology for Human Identification III*. 2006, pp. 620208–1, Springer.

[41] Y. Zhang, J. Yang, and H. Wu, "A hybrid swipe fingerprint mosaicing scheme," in *Audio- and Video-Based Biometric Person Authentication*. 2005, vol. 3546 of *Lecture Notes in Computer Science*, pp. 293–302, Springer.

[42] D. Kwon, I.D. Yun, and S.U. Lee, "Rolled fingerprint construction using mrf-based non-rigid image registration," *IEEE Transactions on Image Processing*, vol. 19, no. 12, pp. 3255–3270, 2010.

[43] Geppy Parziale, Eva Diaz-Santana, and Rudolf Hauke, "The surround imager tm: A multi-camera touchless device to acquire 3D rolled-equivalent fingerprints," in *Audio- and Video-Based Biometric Person Authentication*. 2005, vol. 3546 of *Lecture Notes in Computer Science*, pp. 260–269, Springer.

[44] H. Choi, K. Choi, and J. Kim, "Mosaicing touchless and mirror-reflected fingerprint images," *IEEE Transactions onInformation Forensics and Security*, vol. 5, no. 1, pp. 52–61, March 2010.

[45] R. Rowe, K. Nixon, and P. Butler, "Multispectral fingerprint image acquisition," *Advances in Biometrics*, pp. 3–23, 2008.

[46] X. Liu and T. Chen, "Geometry-assisted statistical modeling for face mosaicing," in *Proceedings International Conference on Image Processing (ICIP)*, sept. 2003, vol. 2, pp. II – 883–6 vol.3.

[47] F. Yang, M. Paindavoine, H. Abdi, and A. Monopoli, "Development of a fast panoramic face mosaicking and recognition system," *Optical engineering*, vol. 44, 2005.

[48] R. Singh, M. Vatsa, A. Ross, and A. Noore, "A mosaicing scheme for pose-invariant face recognition," *IEEE Transactions on Systems, Man, and Cybernetics, Part B*, vol. 37, no. 5, pp. 1212–1225, 2007.

[49] K. Hollingsworth, T. Peters, K.W. Bowyer, and P.J. Flynn, "Iris recognition using signal-level fusion of frames from video," *IEEE Transactions on Information Forensics and Security*, vol. 4, no. 4, pp. 837–848, 2009.

[50] R. Jillela, A. Ross, and P.J. Flynn, "Information fusion in low-resolution iris videos using principal components transform," in *IEEE Workshop on Applications of Computer Vision (WACV)*, 2011, pp. 262–269.

[51] J. Zuo, N.K. Ratha, and J.H. Connell, "Cancelable iris biometric," in *IEEE 19th International Conference on Pattern Recognition (ICPR)*, 2008, pp. 1–4.

[52] S.G. Kong, J. Heo, B.R. Abidi, J. Paik, and M.A. Abidi, "Recent advances in visual and infrared face recognitiona review," *Computer Vision and Image Understanding*, vol. 97, no. 1, pp. 103–135, 2005.

[53] G. Bebis, A. Gyaourova, S. Singh, and I. Pavlidis, "Face recognition by fusing thermal infrared and visible imagery," *Image and Vision Computing*, vol. 24, no. 7, pp. 727–742, 2006.

[54] S.G. Kong, J. Heo, F. Boughorbel, Y. Zheng, B.R. Abidi, A. Koschan, M. Yi, and M.A. Abidi, "Multiscale fusion of visible and thermal ir images for illumination-invariant face recognition," *International Journal of Computer Vision*, vol. 71, no. 2, pp. 215–233, 2007.

[55] R. Singh, M. Vatsa, and A. Noore, "Integrated multilevel image fusion and match score fusion of visible and infrared face images for robust face recognition," *Pattern Recognition*, vol. 41, no. 3, pp. 880–893, 2008.

[56] R.-L. Hsu, *Face Detection and Modeling for Recognition*, Ph.D. thesis, Department of Computer Science and Engineering, Michigan State University, 2002.

[57] X. Lu and A.K. Jain, "Integrating range and texture information for 3d face recognition," in *Seventh IEEE Workshops on Application of Computer Vision (WACV)*, 2005, vol. 1, pp. 156–163.

[58] A. Noore, R. Singh, and M. Vatsa, "Robust memory-efficient data level information fusion of multi-modal biometric images," *Information Fusion*, vol. 8, no. 4, pp. 337–346, 2007.

[59] X.Y. Jing, Y.F. Yao, D. Zhang, J.Y. Yang, and M. Li, "Face and palmprint pixel level fusion and kernel dcv-rbf classifier for small sample biometric recognition," *Pattern Recognition*, vol. 40, no. 11, pp. 3209–3224, 2007.

[60] Jingwang Liu, Yan Hou, Jingyan Wang, Yongping Li, Quanquan Wang, Jiaju Man, Honglan Xie, and Jianhua He, "Fusing iris and palmprint at image level for multi-biometrics verification," in *Fourth International Conference on Machine Vision (ICMV 11)*. International Society for Optics and Photonics, 2011, pp. 83501Q–83501Q.

[61] B. Klare, A.A. Paulino, and A.K. Jain, "Analysis of facial features in identical twins," in *IEEE International Joint Conference on Biometrics (IJCB)*, 2011, pp. 1–8.

[62] W. Zhao, R. Chellappa, P.J. Phillips, and A. Rosenfeld, "Face recognition: A literature survey," *ACM Computing Surveys*, vol. 35, no. 4, pp. 399–458, 2003.

[63] Unsang Park and Anil K Jain, "Face matching and retrieval using soft biometrics," *Information Forensics and Security, IEEE Transactions on*, vol. 5, no. 3, pp. 406–415, 2010.

[64] K.W. Bowyer, K. Hollingsworth, and P.J. Flynn, "Image understanding for iris biometrics: A survey," *Computer Vision and Image Understanding*, vol. 110, no. 2, pp. 281–307, 2008.

[65] Kevin W Bowyer, Karen P Hollingsworth, and Patrick J Flynn, "A survey of iris biometrics research: 2008–2010," in *Handbook of iris recognition*, Mark J. Burge and Kevin W. Bowyer, Eds., Advances in Computer Vision and Pattern Recognition, pp. 15–54. Springer, 2013.

[66] J. Daugman, "How iris recognition works," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no. 1, pp. 21–30, 2004.

[67] Manisha Sam Sunder and Arun Ross, "Iris image retrieval based on macro-features," in *International Conference on Pattern Recognition (ICPR)*. IEEE, 2010, pp. 1318–1321.

[68] Feng Shen and Patrick J Flynn, "Iris matching by crypts and anti-crypts," in *IEEE Conference on Technologies for Homeland Security (HST)*. IEEE, 2012, pp. 208–213.

[69] Ajay Kumar and Arun Passi, "Comparison and combination of iris matchers for reliable personal authentication," *Pattern recognition*, vol. 43, no. 3, pp. 1016–1026, 2010.

[70] J.G. Daugman, "High confidence visual recognition of persons by a test of statistical independence," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 15, no. 11, pp. 1148–1161, 1993.

[71] Anil K Jain, Arun Arun Abraham Ross, and Karthik Nandakumar, *Introduction to biometrics*, Springer, 2011.

[72] R. Cappelli, "Sfinge: Synthetic fingerprint generator," in *Proc. Int. Workshop Modeling and Simulation in Biometric Technology*, 2004, pp. 147–154.

[73] B. Yanikoglu and A. Kholmatov, "Combining multiple biometrics to protect privacy," in *Proceedings of ICPR-BCTP Workshop*, August 2004, pp. 43–46.

[74] Kieran G. Larkin and Peter A. Fletcher, "A coherent framework for fingerprint analysis: are fingerprints holograms?," *Opt. Express*, vol. 15, no. 14, pp. 8667–8677, 2007.

[75] D.C. Ghiglia and M.D. Pritt, *Two-dimensional phase unwrapping: theory, algorithms, and software*, Wiley New York, 1998.

[76] Luminita A Vese and Stanley J Osher, "Modeling textures with total variation minimization and oscillating patterns in image processing," *Journal of Scientific Computing*, vol. 19, no. 1-3, pp. 553–572, 2003.

[77] Kieran G. Larkin, Donald J. Bone, and Michael A. Oldfield, "Natural demodulation of two-dimensional fringe patterns. I. General background of the spiral phase quadrature transform," *J. Opt. Soc. Am. A*, vol. 18, no. 8, pp. 1862–1870, 2001.

[78] Lin Hong, Yifei Wan, and A. Jain, "Fingerprint image enhancement: algorithm and performance evaluation," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 20, no. 8, pp. 777 –789, Aug. 1998.

[79] R. Thai, *Fingerprint image enhancement and minutiae extraction*, Ph.D. thesis, School of Computer Science and Software Engineering, The University of Western Australia, 2003.

[80] R. Goldstein, H. Zebker, and C. Werner, "Satellite radar interferometry- Two-dimensional phase unwrapping," *Radio Science*, vol. 23, no. 4, pp. 713–720, 1988.

[81] D.J. Bone, "Fourier fringe analysis: the two-dimensional phase unwrapping problem," *Applied Optics*, vol. 30, no. 25, pp. 3627–3632, 1991.

[82] Sergey O. Novikov and Valery S. Kot, "Singular feature detection and classification of fingerprints using hough transform," 1998, vol. 3346, pp. 259–269, SPIE International Workshop on digital image processing and computer graphics.

[83] N. Yager and A. Amin, "Fingerprint alignment using a two stage optimization," *Pattern Recognition Letters*, vol. 27, no. 5, pp. 317–324, 2006.

[84] S. Crihalmeanu, A. Ross, S. Schuckers, and L. Hornak, "A protocol for multibiometric data acquisition, storage and dissemination," Tech. Rep., Lane Department of Computer Science and Electrical Engineering, WVU, 2007.

[85] P. D. Kovesi, "MATLAB and Octave functions for computer vision and image processing," Centre for Exploration Targeting, School of Earth and Environment, The University of Western Australia, Available at: <http://www.csse.uwa.edu.au/∼pk/research/matlabfns/>.

[86] N.K. Ratha, S. Chikkerur, J.H. Connell, and R.M. Bolle, "Generating cancelable fingerprint templates," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, pp. 561–572, 2007.

[87] C. Lee, J.Y. Choi, K.A. Toh, and S. Lee, "Alignment-free cancelable fingerprint templates based on local minutiae information," *IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics*, vol. 37, no. 4, pp. 980–992, 2007.

[88] S. Chikkerur, NK Ratha, JH Connell, and RM Bolle, "Generating registration-free cancelable fingerprint templates," in *2nd IEEE International Conference on Biometrics: Theory, Applications and Systems*, 2008, pp. 1–6.

[89] Abhishek Nagar, Karthik Nandakumar, and Anil K. Jain, "Biometric template transformation: a security analysis," in *Proc. of SPIE, Electronic Imaging, Media Forensics and Security XII*, San Jose, Jan. 2010.

[90] Terrance E Boult, Walter J Scheirer, and Robert Woodworth, "Revocable fingerprint biotokens: Accuracy and security analysis," in *IEEE Conference on Computer Vision and Pattern Recognition (CVPR'07)*. IEEE, 2007, pp. 1–8.

[91] Abhishek Nagar, Karthik Nandakumar, and Anil K Jain, "Securing fingerprint template: Fuzzy vault with minutiae descriptors," in *19th International Conference on Pattern Recognition (ICPR)*. IEEE, 2008, pp. 1–4.

[92] Karthik Nandakumar, "A fingerprint cryptosystem based on minutiae phase spectrum," in *IEEE International Workshop on Information Forensics and Security (WIFS)*. IEEE, 2010, pp. 1–6.

[93] Andrew Beng Jin Teoh and David Chek Ling Ngo, "Biophasor: Token supplemented cancellable biometrics," in *9th International Conference on Control, Automation, Robotics and Vision, (ICARCV'06)*. IEEE, 2006, pp. 1–5.

[94] T. Valentine, "Face-space models of face recognition," *Computational, geometric, and process perspectives on facial cognition: Contexts and challenges*, pp. 83–113, 2001.

[95] Aude Oliva, Antonio Torralba, and Philippe G Schyns, "Hybrid images," in *ACM Transactions on Graphics (TOG)*. ACM, 2006, vol. 25, pp. 527–532.

[96] F. Galton, "Composite portraits, made by combining those of many different persons into a single resultant figure," *The Journal of the Anthropological Institute of Great Britain and Ireland*, vol. 8, pp. 132–144, 1879.

[97] G. Wolberg, "Image morphing: a survey," *The visual computer*, vol. 14, no. 8, pp. 360–372, 1998.

[98] M. Bichsel, "Automatic interpolation and recognition of face images by morphing," in *the Second International Conference on Automatic Face and Gesture Recognition*, 1996, pp. 128–135.

[99] D.A. Rowland and D.I. Perrett, "Manipulating facial appearance through shape and color," *Computer Graphics and Applications*, vol. 15, no. 5, pp. 70–76, 1995.

[100] G. Rhodes, R. Robbins, E. Jaquet, E. McKone, L. Jeffery, and C.W.G. Clifford, "Adaptation and face perception: How aftereffects implicate norm-based coding of faces," *Fitting the mind to the world: Adaptation and after-effects in high-level vision*, pp. 213–240, 2005.

[101] T. Terada, T. Fukui, T. Igarashi, K. Nakao, A. Kashimoto, and Y.W. Chen, "Automatic facial image manipulation system and facial texture analysis," in *IEEE Fifth International Conference on Natural Computation.*, 2009, vol. 6, pp. 8–12.

[102] J.Y. Baudouin and R. Brochard, "Gender-based prototype formation in face recognition.," *Journal of Experimental Psychology: Learning, Memory, and Cognition*, vol. 37, no. 4, pp. 888, 2011.

[103] B. Kamgar-Parsi, W. Lawson, and B. Kamgar-Parsi, "Toward development of a face recognition system for watchlist surveillance," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 33, no. 10, pp. 1925–1937, 2011.

[104] A. Goshtasby, "Piecewise linear mapping functions for image registration," *Pattern Recognition*, vol. 19, no. 6, pp. 459–466, 1986.

[105] K. Messer, J. Matas, J. Kittler, J. Luettin, and G. Maitre, "XM2VTSDB: The extended M2VTS database," in *Second International Conference on Audio and Video-based Biometric Person Authentication*, 1999, pp. 965–966.

[106] H. Lamba, A. Sarkar, M. Vatsa, R. Singh, and A. Noore, "Face recognition for look-alikes: A preliminary study," in *IEEE International Joint Conference on Biometrics (IJCB)*, 2011, pp. 1–6.

[107] Xiangqian Wu, Kuanquan Wang, David Zhang, and Ning Qi, "Combining left and right irises for personal authentication," in *Energy Minimization Methods in Computer Vision and Pattern Recognition*. Springer, 2007, pp. 145–152.

[108] Karen Hollingsworth, Kevin W Bowyer, Stephen Lagree, Samuel P Fenker, and Patrick J Flynn, "Genetically identical irises have texture similarity that is not detected by iris biometrics," *Computer Vision and Image Understanding*, vol. 115, no. 11, pp. 1493–1502, 2011.

[109] Y Li and M. Savvides, *Automatically Identifying Mislabelled Iris data: Case of Left vs. Right Irises*, Springer-Verlag, 2008.

[110] R. Abiantun and M. Savvides, "Tear-duct detector for identifying left versus right iris images," in *IEEE 37th Applied Imagery Pattern Recognition Workshop (AIPR)*, 2008, pp. 1–4.

[111] S. Bhat and M. Savvides, "Evaluating active shape models for eye-shape classification," in *IEEE International Conference on Acoustics, Speech and Signal (ICASSP)*, 2008, pp. 5228–5231.

[112] Shai Avidan and Ariel Shamir, "Seam carving for content-aware image resizing," *ACM Trans. Graph.*, vol. 26, July 2007.

[113] S. Shah and A. Ross, "Iris segmentation using geodesic active contours," *IEEE Transactions on Information Forensics and Security*, vol. 4, no. 4, pp. 824–836, 2009.

[114] J. Daugman, "Probing the uniqueness and randomness of iriscodes: Results from 200 billion iris pair comparisons," *Proceedings of the IEEE*, vol. 94, no. 11, pp. 1927 –1935, nov. 2006.

[115] "Casia-irisv3 database [online]. available: http://www.cbsr.ia.ac.cn/irisdatabase," .

[116] L. Masek and P. Kovesi, "Matlab source code for a biometric identification system based on iris patterns," 2003.

[117] J. Daugman, "Demodulation by complex-valued wavelets for stochastic pattern recognition," *International Journal of Wavelets, Multiresolution and Information Processing*, vol. 1, no. 1, pp. 1–17, 2003.

[118] YC Feng, P.C. Yuen, and A.K. Jain, "A hybrid approach for face template protection," in *Proc. of SPIE Conference of Biometric Technology for Human Identification, Orlando, FL, USA*, 2008, vol. 6944.

[119] Anil K. Jain and Umut Uludag, "Hiding biometric data," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 25, pp. 1494–1498, 2003.

[120] J. Dong and T. Tan, "Effects of watermarking on iris recognition performance," in *10th International Conference on Control, Automation, Robotics and Vision, 2008. ICARCV 2008*, 2008, pp. 1156–1161.

[121] N. Agrawal and M. Savvides, "Biometric data hiding: A 3 factor authentication approach to verify identity with a single image using steganography, encryption and matching," *Computer Vision and Pattern Recognition Workshop*, vol. 0, pp. 85–92, 2009.

[122] Elaine M. Newton, Latanya Sweeney, and Bradley Malin, "Preserving privacy by de-identifying face images," *IEEE Transactions on Knowledge and Data Engineering*, vol. 17, pp. 232–243, 2005.

[123] R. Gross, L. Sweeney, F. De la Torre, and S. Baker, "Model-based face de-identification," in *Computer Vision and Pattern Recognition Workshop (CVPRW'06)*, Los Alamitos, CA, USA, 2006, pp. 161–168, IEEE Computer Society.

[124] Dmitri Bitouk, Neeraj Kumar, Samreen Dhillon, Peter Belhumeur, and Shree K. Nayar, "Face swapping: automatically replacing faces in photographs," *ACM Trans. Graph.*, vol. 27, no. 3, pp. 1–8, 2008.

[125] B. Moskovich and M. Osadchy, "Illumination invariant representation for privacy preserving face identification," in *IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, 2010, pp. 154–161.

[126] S. Prabhakar, S. Pankanti, and AK Jain, "Biometric recognition: Security and privacy concerns," *IEEE Security & Privacy*, vol. 1, no. 2, pp. 33–42, March-April 2003.

[127] B. Thuraisingham and W. Ford, "Security constraint processing in a multilevel secure distributed database management system," *IEEE Transactions on Knowledge and Data Engineering*, vol. 7, no. 2, pp. 274–293, 1995.

[128] C. Soutar, D. Roberge, A. Stoianov, R. Gilroy, and B.V.K.V. Kumar, "Biometric encryption," *ICSA Guide to Cryptography*, 1999.

[129] Moni Naor and Adi Shamir, "Visual cryptography," in *EUROCRYPT*, 1994, pp. 1–12.

[130] G. Ateniese, C. Blundo, A.D. Santis, and D.R. Stinson, "Extended capabilities for visual cryptography," *Theoretical Computer Science*, vol. 250, no. 1-2, pp. 143–161, 2001.

[131] S.K. Shevell, *The science of color*, Elsevier Science Ltd., 2003.

[132] R.W. Floyd and L. Steinberg, "An adaptive algorithm for spatial greyscale," *SPIE Milestone Series*, vol. 154, pp. 281–283, 1999.

[133] T.F. Cootes, G.J. Edwards, C.J. Taylor, et al., "Active appearance models," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 23, no. 6, pp. 681–685, 2001.

[134] M. B. Stegmann, "Active appearance models: Theory, extensions and cases," Master's Thesis, Informatics and Mathematical Modelling, Technical University of Denmark, DTU, August 2000.

[135] F.L. Bookstein, "Principal warps: Thin-plate splines and the decomposition of deformations," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 11, no. 6, pp. 567–585, 1989.

[136] M. B. Stegmann, B. K. Ersbøll, and R. Larsen, "FAME – a flexible appearance modelling environment," *IEEE Trans. on Medical Imaging*, vol. 22, no. 10, pp. 1319–1331, 2003.

[137] Y.F. Chen, Y.K. Chan, C.C. Huang, M.H. Tsai, and Y.P. Chu, "A multiple-level visual secret-sharing scheme without image size expansion," *Information Sciences*, vol. 177, no. 21, pp. 4696–4710, 2007.

[138] T.L. Lin, S.J. Horng, K.H. Lee, P.L. Chiu, T.W. Kao, Y.H. Chen, R.S. Run, J.L. Lai, and R.J. Chen, "A Novel Visual Secret Sharing Scheme for Multiple Secrets without Pixel Expansion," *Expert Systems with Applications*, vol. 37, no. 12, pp. 7858 – 7869, 2010.

[139] Hunny Mehrotra, Ajita Rattani, and Phalguni Gupta, "Fusion of iris and fingerprint biometric for recognition," in *Proceedings of International Conference on Signal and Image Processing*, 2006, pp. 1–6.

[140] Vincenzo Conti, Carmelo Militello, Filippo Sorbello, and Salvatore Vitabile, "A frequency-based approach for features fusion in fingerprint and iris multimodal biometric identification systems," *IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews*, vol. 40, no. 4, pp. 384–395, 2010.

[141] Arun Ross, Ajita Rattani, and Massimo Tistarelli, "Exploiting the "doddington zoo" effect in biometric fusion," in *IEEE 3rd International Conference on Biometrics: Theory, Applications, and Systems, (BTAS'09)*. IEEE, 2009, pp. 1–7.

[142] A Jameer Basha, V Palanisamy, and T Purusothaman, "Efficient multimodal biometric authentication using fast fingerprint verification and enhanced iris features," *Journal of Computer Science*, vol. 7, no. 5, pp. 698, 2011.

[143] A. Othman and A. Ross, "On mixing fingerprints," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 1, pp. 260–267, January 2013.

[144] Yongfang Zhu, Sarat C Dass, and Anil K Jain, "Statistical models for assessing the individuality of fingerprints," *IEEE Transactions on Information Forensics and Security*, vol. 2, no. 3, pp. 391–401, 2007.

[145] Ruud M Bolle, Sharath Pankanti, Jonathan H Connell, and Nalini K Ratha, "Iris individuality: A partial iris model," in *Pattern Recognition, 2004. ICPR 2004. Proceedings of the 17th International Conference on*. IEEE, 2004, vol. 2, pp. 927–930.

[146] Karen P Hollingsworth, Kevin W Bowyer, and Patrick J Flynn, "Improved iris recognition through fusion of hamming distance and fragile bit distance," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 33, no. 12, pp. 2465–2476, 2011.

[147] Barzegar Nakissa and Moin M Shahram, "A new user dependent iris recognition system based on an area preserving pointwise level set segmentation approach," *EURASIP Journal on Advances in Signal Processing*, vol. 2009, 2009.

[148] Kenneth Nilsson and Josef Bigun, "Localization of corresponding points in fingerprints by complex filtering," *Pattern Recognition Letters*, vol. 24, no. 13, pp. 2135–2144, 2003.

[149] Sheng Li and A.C. Kot, "Fingerprint combination for privacy protection," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 2, pp. 350–360, 2013.

[150] Martin A Fischler and Robert C Bolles, "Random sample consensus: a paradigm for model fitting with applications to image analysis and automated cartography," *Communications of the ACM*, vol. 24, no. 6, pp. 381–395, 1981.

[151] Lein Harn, "Group authentication," *IEEE Transactions on Computers*, vol. 62, no. 9, pp. 1893–1898, 2013.