Chapter 2
Literature Review

This chapter provides a review of literature on biometric systems, multibiometric systems and biometric template security. This chapter begins with a brief history of biometrics and biometric systems. Summaries of the reviewed literature on multibiometric systems in terms of sources of multiple evidences, levels and method of information fusion in multibiometric system are presented in this chapter. The chapter concludes with a review of literature on template security.

2.1 Introduction

The goal of the present investigation is to identify the appropriate biometrics and design approaches to employ in designing a multibiometric system. In order to overcome certain limitations of biometric system, multibiometric systems are designed. To get better perspectives of different issues related to design a multibiometric system, it is of great importance to review the experiences of earlier research efforts. This helps in sharpening the methodological and analytical tools used in the present study besides formulating appropriate concepts as relevant for the study. Several studies have been carried out in the past on multibiometric systems. Designing of multibiometric systems is now getting a new impetus with the soft computing techniques like ANN and fuzzy logics etc. in recent decades. The investigation also extends to the protection techniques of biometric template.

In the following sections, related work on biometric systems, multibiometric systems and biometric template security have been reviewed and summarized.

2.2 Related Work

Prior to the development of multibiometric systems, biometric systems were widely used by the researches for identification. Biometric systems have limitations such as non-universalities, intra-class variations, inter-class similarities etc. To handle certain limitations of biometric systems, multibiometric systems have been developed. As increasing in security and privacy, biometric template security has also come into picture. Related work on biometric systems, multibiometric systems and biometric template security is presented in the following sections.

2.2.1 Biometric Systems

The word biometrics is derived from the Greek words *bios* (meaning life) and *metron* (meaning measurement); biometric identifiers are measurements from living human body (Maltoni *et al*., 2009). Biometric systems have only become available over the last few decades although the history of biometrics starts in ancient civilizations e.g. Chinese and the Egyptians civilizations. Presently, the focus is on using iris recognition, fingerprint recognition, face recognition, retina recognition etc. and identifying characteristics authentication and improve security measures. This section provides literature review on iris recognition.

Iris recognition has been regarded as one of the most reliable biometrics technologies in recent years (Wildes, 1997). The idea of using iris structures for biometric recognition was proposed by Flom and Safir in 1936 (Kevin *et al*. 2008). However, it was not until 1987, when an unimplemented conceptual design of automated iris recognition was patented (Flom and Safir, 1987) and Daugman (1993) presented the implementation of first algorithm which proved iris characteristics as one of the best performance biometric modality. There are four main stages of the iris recognition system. They are (i) *Image acquisition*, (ii) *Image segmentation,* (iii) *Feature extraction* and (iv) *Matching or Classification*.

Many different techniques were used in every stage of iris recognition by different authors. Pioneering work on iris recognition was done by Daugman using Gabor wavelets. Some well known methods for iris segmentation are integro-differential operator (Daugman, 1993), edge detection using a Hough transform (Wildes, 1997), Morphologic operators (Mira and Mayer, 2003), Canny edge detection with a Hough

transform (Liu *et al*., 2003), pulling and pushing method (Zhaofeng *et al*., 2006) and active contours (Daugman, 2007). Variations of the edge detection method like Canny edge detection and Hough transform approach have since been used by a number of researchs (Kong and Zhang, 2001; Huang *et al*., 2002; Ma *et al*. 2002, 2003, 2004). Kong *et al.* (2001) presented a method for eyelash detection by using 1D Gabor filters.

Regarding feature extraction, iris recognition approaches can be divided into four major categories (Sun *et al*., 2005): (i) phase-based methods (e.g., Daugman, 2003), (ii) zero-crossing methods (e.g., Boles and Boashash, 1998), (iii) texture analysis based methods (e.g., Wildes, 1997) and (iv) Local intensity variation (Ma *et al*., 2004). Daugman (2003) employed 2-D Gabor wavelets to extract phase structure information of the iris to generate a 2048-bit iris. Boles and Boashash (1998) calculated only a one-dimensional wavelet transform's zero-crossings over concentric circles on the iris. Wildes (1997) represented the iris pattern using a four-level Laplacian pyramid and the quality of matching was determined by the normalized correlation results between the acquired iris image and the stored template. Lim *et al*. (2001) applied a 2-D Haar wavelet transform four times to decompose the iris image and constructed a compact code from the high-frequency coefficients. Ma *et al*. (2004) extracted the feature of the iris by using Key local variations. Iris is coded based on differences of discrete cosine transform (DCT) coefficients of rectangular patches (Monro *et al*., 2007). Many statistical methods namely Singular Value Decomposition (SVD), Principal Component Analysis (PCA) and Independent Component Analysis (ICA) were used to extract iris features by many authors (Huang *et al.,* 2002; Dorairaj *et al.*, 2005; Chitte *et al.*, 2011; Shashi Kumar *et al*., 2011).

Different distance measures (such as Hamming distance and Euclidean distance) were used for matching in iris recognition by Boles *et al*. (1998) and Huang *et al*. (2002) and others. Both the probabilistic and non probabilistic distance measures such as Bayes, Euclidean, K-Nearest Neighbor were used by Chandra Murty *et al*. (2009) to classify iris pattern. Lim *et al*. (2001) and Rashad *et al*. (2011) adopted a modified competitive learning neural network (LVQ) for classification. Neural network was used for iris pattern classification by Abiyev *et al*. (2008), Araghi *et al*. (2010) and Wagdarikar *et al*. (2010). SVM was also employed as classifier by many authors (Li *et al*., 2003; Shashi-Kumar *et al*., 2011).

2.2.2 Multibiometric Systems

This section presents some of the work carried out on multibiometric systems. As multibiometric system is to be one of the prominent solutions in biometrics for various applications in near future, a large number of works has been carried on and a long list of articles has been addressing this topic. The present review work focuses on the survey of various sources of information under five scenario (i) multiple sensors (ii) multiple algorithms (iii) multiple instances (iv) multiple samples and (v) multiple biometric traits (Rose *et al*., 2006).

Chang *et al*. (2005) used the 2D texture content of a person's face obtained by using a CCD camera and the 3D surface shape of the face using a range sensor in face recognition system and observes that this combination performs significantly better than using either 3D or 2D alone. Many authors have used thermal infrared and visible light facial images in face recognition (Socolinsky *et al.*, 2004; Chen *et al*., 2005). Marcialis and Roli (2004) used optical and capacitive fingerprint sensor to capture fingerprint. Table 2.1 summarizes other representative work in the multi-sensor multibiometrics literature.

Table 2.1 Multi-sensor Biometric Systems

Authors	**Sensors**	**Level of Fusion**	**Fusion Methodology**
Marcialis and Roli, 2004	Optical and capacitive fingerprint Sensors	Match score	Sum and product rules; logistic regression
Chen *et al*., 2005	2D camera and range scanner for face	Match score	Weighted sum and product rules
Ross and Govindarajan, 2005	Red, Green, Blue channels for face	Feature; match score	Feature selection and concatenation; sum rule

Lu *et al*. (2003) have employed three different feature extraction schemes based on Principal Component Analysis (PCA), Linear Discriminant Analysis (LDA) and Independent Component Analysis (ICA) to encode a single face image for face recognition system. It is observed that the system is robust to a variety of intra-class variations with the use of different feature sets. Authors further conclude that the identification rate of the biometric system can enhanced by combining multiple face classifiers. Han *et al*. (2005) worked out a context-based gait recognition system in which two gait recognition classifiers based on the walking surface are combined. Table 2.2 summarizes other representative work in the multi-algorithm multibiometrics

literature.

Table 2.2 Multi-algorithm Systems

Authors	**Representations**	**Level of Fusion**	**Fusion Methodology**
Ross *et al*. 2003, Marcialis and Roli 2005.	Fingerprint (minutiae and texture features)	Match score	Likelihood ratio, sum, weighted sum and product rules, perceptron
Lu *et al*. 2003, Ross and Govindarajan 2005	Face (PCA, LDA, ICA)	Feature, Match score	Sum and max rules, nearest neighbor, RBF network, feature selection and concatenation
Kumar *et al*. 2003	Hand (geometry and texture features)	Feature; Match score	Feature concatenation; sum rule
Kinnunen *et al*. 2004	Voice (LPCC, MFCC, ARCSIN, FMT features)	Feature; Match score; Decision	Feature concatenation; sum rule; majority voting
Fierrez-Aguilar *et al*. 2005	Signature (global and local features)	Match score	Sum and max rules, SVM
Kumar and Zhang 2005	Palmprint (Gabor, line, appearance-based)	Match score; Decision	Sum rule (for Gabor and line features) followed by product rule; SVM; neural network; AND rule

In Automated Fingerprint Identification Systems (AFIS), the required ten-print information from a subject can be obtain with the help of sensors that are able to rapidly acquire impressions of all ten fingers and thus, reduce the user's inconvenience. Multi-instance systems are especially beneficial for users whose biometric traits cannot be reliably captured due to inherent problems (Ross *et al*., 2006).

In multi-sample Systems, the query image was compared with the three stored impressions (templates) taken during enrollment and the maximum score was considered the fused score (Simon-Zorita *et al*., 2003). Authors reported that their method improved the recognition accuracy. A fingerprint recognition system equipped with a small size sensor may acquire multiple dab prints of an individual's finger in order to obtain images of various regions of the fingerprint and these impressions are fused to create a composite image under a mosaic scheme. Many approaches have been proposed in Jain *et al.* (2003), and Ryu *et al.* (2006). The main issues in a multi-sample (mosaic) system are determination of the number of samples to be acquired and presents from an individual. In this approach, the procured samples represent the variability as well as the typicality of the individual's biometric data. Hence, the desired relationship between the samples has to be established before-hand in order to optimize the benefits of the integration strategy (Maltoni *et al*., 2009). For example, a face recognition system utilizing both the frontal- and side-profile images of an individual may stipulate that the

side-profile image should be a three-quarter view of the face (Hill *et al*., 1997). Alternately, Uludag *et al*. (2004) discussed new scheme in which the system can select the "optimal" subset from set of fingerprint samples automatically, that would best represent the individual's variability. Table 2.3 summarizes other representative work in the multi-sample and multi-instance multibiometrics literature.

Table 2.3 Multi-instance and Multi-sample Systems

Authors	**Representations**	**Level of Fusion**	**Fusion Methodology**
Prabhakar and Jain 2002	Fingerprint (2 impressions, 2 fingers)	Match score	Likelihood ratio computed from non-parametric joint density estimates
Jain and Ross 2002a	Fingerprint (multi-impressions)	Sensor; feature	Mosaicing of templates at the image level; mosaicing of minutiae sets
Zhou *et al.* 2003	Face (sequence of images from video)	Match score	Temporal integration
Cheung *et al*. 2004	Voice (multiple utterances)	Match score	Zero sum fusion after sorting of scores
Yu *et al*. 2005	Iris (left and right)	Match score	Double threshold and backpropagation algorithm

Both serial and parallel acquisition architectures are found in literature. Generally, physically related biometric traits are conveniently and cost-effectively acquired simultaneously. For example, palmprint and hand-geometry information are acquired using Olympus C-3020 digital camera (Kumar *et al*., 2003), face and iris information are acquired using CCD digital camera (Zhang *et al*., 2007) and multi-instance fingerprint (Uhl and Wild, 2009) can be acquired in parallel using a single camera/sensor. On the other hand, physically unrelated biometric traits (e.g., fingerprint and iris) or multiple instances of the same trait (e.g., iris images from both the eyes) need to be acquired; the acquisition is usually done sequentially.

In the serial or cascade mode, the biometric information is sequentially processed. This architecture may have advantages such as it can improve user convenience as well as allow fast and efficient searches in large scale identification tasks. In a cascaded multibiometric system, if the identity of the user is found to be sufficiently confident after processing the first biometric source, the other biometric information of the user may not be required. Further, if the system is faced with the task of identifying the user from a large database, it can utilize the outcome of each matcher to successively prune the database, thereby making the search faster and more efficient. Thus, a cascaded

system can be more convenient to the user and generally requires less recognition time when compared to its parallel counterpart. In literature, the parallel architecture is the commonly proposed information processing method of the multibiometric systems. This architecture utilizes more evidence about the user in recognition process and hence, reduces the error rate of biometric systems (Ross and Jain, 2003; Snelick *et al*., 2005).

The work on fusion schemes of multibiometrics is discussed under sensor level fusion, feature level fusion, score level fusion, rank level fusion and decision level fusion (ANSI, 2006).

Karanwal *el al*. (2010) took two images of face and finger and fused at sensor level. After taking images, wavelet decomposition is performed on both images using Discrete Wavelet Transform (DWT), followed by a fusion of decomposition of two images which produces fused image of low resolution. Then, SIFT features extracted from the fused image. After extracting SIFT features, matching is performed.

Examples of feature level fusion schemes can be found in Chibelushi *et al.* (1997) using voice and lip shape modals, Chang *et al.* (2003) using ear and face traits, Kumar *et al*. (2005) using hand geometry and palmprint traits, Ross and Govindarajan (2005) using face and hand geometry, George (2008) based on Face and fingerprint modals, Yang *et al.* (2008) using face and palmprint traits, and Chin *et al*. (2009) based on palmprint and fingerprint.

Nandakumar *et al*. (2008) proposed that a framework for the optimal combination of match scores that is based on the likelihood ratio test. The distributions of genuine and impostor match scores are modeled as finite Gaussian mixture model. Experimentations on three multibiometric databases i.e. the NIST-Multimodal XM2VTS-Benchmark and WVU-Multimodal databases have reported that the proposed fusion framework achieves consistently high performance compared to commonly used match score fusion techniques based on score transformation and classification.

Giot *et al*. (2010) have presented a low cost and usable multimodal system based on keystroke dynamics and 2D face recognition combining at match score level. Different fusion methods have been seen tested on a database containing two kinds of biometric template for 100 users. The various different fusion methods *viz*. min, max, sum and weighted sum have been employed, and are configured with genetic algorithm.

Kaur *et al*. (2010) have combined the matching scores of modalities i.e. speech

and signature using product of likelihood ratio test. Matcher scores are simply added with no normalization. The scores are neither rescaled, nor weighted to account for different in matcher accuracy.

Mahesh and Swamy (2011) have adopted fusion at the matching score level using palmprint and speech. The authors have reported the promising improvement of overall accuracy of the biometric systems.

Wang *et al*. (2011) have proposed multimodal biometric algorithm for face and iris. In this system, face features are extract based on eigenface method and iris features using 2D even Gabor filter and then normalize using z-score model. The normalized features are combined in series and take Euclidean distance as a matcher. The authors have reported that the proposed system outperforms single biometrics with sum and weighted sum rule fusion.

Kazi *et al*. (2012) have reported that face and signature based multibiometric system outperforms single face/signature biometric systems. The authors have adopted matching score level fusion, and face and signature trait of the user simple are fused by sum rule fusion technique.

Benaliouche and Touahria (2014) investigated the performance from three different approaches *viz*. classical sum rule, weighted sum rule, and fuzzy logic method in a multimodal biometric system of iris and fingerprints. The scores were normalized using min-max method and fused at the matching score and the decision levels. Authors reported that the fuzzy logic method for the matching scores combinations outperforms the other two methods. Table 2.4 summarizes other representative work in the multibiometrics literature.

Melnik *et al.* (2003) have employed rank level fusion which attempts to find a tradeoff between the general preference for specific matchers and the confidence in specific results (as indicated by the ranks).

Abaza and Ross (2009) have presented techniques for performing multibiometric fusion at the rank level. By incorporating quality information in the fusion rule, it was observed that the performance of rank-level fusion schemes can be significantly improved. Examples of Rank Level fusion schemes can be found in Gokberk *et al*. (2005) and Chin *et al.* (2009).

Some of the classifier Decision fusion methods are Bayesian decision fusion (Kryszczuk *et al*., 2007), the Dempster-Shafer theory of evidence (Bera *et al*., 2015), behavior knowledge space (Huang and Suen, 1995), Multivariate Polynomial Model (Toh, 2004), "AND" and "OR" rules (Daugman, 2012) and k-NN neighborhood classifier (Toh *et al*., 2002).

Table 2.4 Multimodal Biometric Systems using Score Level Fusion

Modalities Fused	**Authors**	**Level of Fusion**	**Fusion Methodology**
Face, fingerprint and voice	Jain *et al*., 1999	Match score	Likelihood ratio
Face, voice and lip movement	Frischholz *et al*., 2000	Match Score, decision	Weighted sum rule; majority voting
Face and iris	Wang *et al*., 2003	Match score	Sum rule; weighted sum rule; Fisher's linear discriminant; neural network
Face, fingerprint and hand geometry	Ross and Jain, 2003	Match score	Sum rule; decision trees; linear discriminant function
Fingerprint and hand geometry	Toh *et al*., 2003	Match score	Reduced multivariate polynomial model
Face and gait	Kale *et al*., 2004	Match score	Sum and product rules
Fingerprint, hand geometry and voice	Toh *et al*., 2004	Match score	Weighted sum rule
Face and voice	Snelick *et al*., 2005	Match score	Sum, product, min, max and median rules
	Vajaria *et al*., 2007	Match score	Sum rule; max rules
Face, fingerprint	Ricardo *et al*., 2009	Match score	Likelihood ratio using fuzzy logic.
Face, ear	Darwish *et al*., 2009	Match score	Principal Component Analysis
Face, finger veins	Razzak *et al*., 2010	Match score	Weighted Fuzzy fusion
Face, palmprint	Raghavendra *et al*., 2010	Match score	Gaussian Mixture Model (GMM) ; Monte Carlo sampling based hypothesis testing

2.2.3 Biometric Template Security

This section presents the survey of biometric template security methods. The recent strategies for generating cancelable biometric templates are mainly reviewed in this section.

Juels *et al*. (1999) combined techniques of error correcting codes and cryptography to achieve a type of cryptographic primitive referred to as fuzzy commitment scheme.

Juels *et al*. (2002) introduced fuzzy vault. Clancy *et al*. (2003) proposed the first practical fuzzy vault scheme named *fingerprint vault* by locking minutiae points of fingerprint. A set of minutiae points is mapped onto a polynomial and chaff points are randomly added to construct the vault. During authentication, Reed-Solomon codes are applied to reconstruct the polynomial out of which a 128-bit key is recreated.

Ratha *et al*. (2001) introduced cancelable biometric based on noninvertible geometric transformations e.g. morph the original biometric templates in signal domain prior to feature extraction. The distorted biometric template does not match with the original template, while the two instances of distorted template match among themselves.

Teoh *et al*. (2006) employed the idea of using Random Projections for cancelable biometrics. Random Projections of discriminative features were used as cancelable biometric templates. Random Projections and Random Permutations on different regions of the iris were applied for cancelability in Pillai *et al*. (2010, 2011).

BioHashing was proposed by Goh and Ngo (2003) as an extension of random projection. In BioHashing (Teoh *et al*., 2004), the BioHash code is generated by inner product with the biometric feature vector with a set of orthogonal pseudo-random vectors based on a user-specific tokenized random number (TRN). Other representative work in biometric template security literature is presented in Table 2.5.

Table 2.5 Biometric Template Security Methods

Approach	**Authors**	**Modality**	**Methodology**
Salting	Connie et al. 2005	Palmprint	PalmHashing
	Teoh *et al*. 2006	Face	Random multi-space quantization technique
	Chong et al. 2006	Iris	BioHashing
Non-invertible	Ratha *et al*., 2001	Face	Grid morphing and block permutation
	Zuo *et al*., 2008	Iris	Shifting and combining rows in the unwrapped iris image
	Rathgeb *et al*., 2013	Iris	Adaptive Bloom filter-based cancelable transform
Key-binding schemes	Hao *et al*., 2006	Iris	Fuzzy commitment scheme
	Wu *et al*., 2008	Iris	Fuzzy vault
	Li *et al*., 2009	Fingerprint	Shielding functions
Biometric Key-Generation	Davida *et al*.,1999	Iris	Private Template Scheme
	Vielhauer *et al*., 2006	Signature	Quantization Schemes
Data Hiding	Jain *et al*., 2002b	Face and fingerprint	Watermarking in spatial domain
	Vatsa *et al*., 2004	Face and iris	Watermarking in frequency domain

2.3 Chapter Summary

This chapter has provided a comprehensive review of the current status of research in field of biometric system, multibiometric system and biometric template security techniques. The prime focus of literature review was to identify methodological and design tools to be employed for the present study besides formulating appropriate concepts relevant for the study.

Previous studies have shown that iris is one of the most acceptable biometric. Previous studies on multibiometric systems have shown that information fusion at match score level is most commonly employed. It is also observed that cancelable biometrics is most commonly used biometric template security technique. In the following chapter, a detailed background on biometric systems and biometric template security are presented.