A Survey on Different Techniques for Biometric Template Protection

P Jayapriya[1], R. R. Manimegalai[1], R. Lakshmana Kumar[2], Seifedine Kadry[3], Sanghyun Seo[4]

[1] Department of Information Technology, PSG College of Technology, India
[2] Department of Computer Applications, Hindusthan College of Engineering and Technology, India
[3] Department of Mathematics and Computer Science, Beirut Arab University, Lebanon
[4] School of Computer Art, College of Art and Technology, Chung-Ang University, Korea
jayapriy@gmail.com, yuqiao417@gmail.com, research.laksha@gmail.com, s.kadry@bau.edu.lb, sanghyun@cau.ac.kr

Abstract

Biometric applications are based on the static and non-static biometric characteristics such as voice, palm, and finger vein, gait, DNA, hand geometry, iris, fingerprint etc. This paper presents an overview of the two types of template protection techniques, namely, (i) feature transformation or cancelable biometric, and (ii) bio-cryptosystems. Combining both the techniques, i.e. feature transformation and bio-cryptosystems, provide a set of hybrid template protection schemes. Multimodal biometric templates are also protected using hybrid template protection schemes. This paper mainly focuses on providing a comprehensive overview of the template protection techniques and multimodal biometric systems for user authentication. In addition to this, the paper gives the overview of various attacks, issues and challenges in biometric recognition system.

Keywords: Template security, Bio-cryptosystems, Cancel-able biometrics, Muli-modal

1 Introduction

The term biometric is derived from two Greek words, namely, bio which means life and metric which means to evaluate. The measurement and evaluation of physical, behavioral and the soft characteristics of an individual is known as biometric analysis [1-3]. The physiological characteristics include traits such as fingerprint, face, iris, hand, and knuckle [4-6]. The behavioral characteristics include traits such as keystrokes, signature and voice. The soft characteristics include skin, hair, eye color, age, gender, height, and weight and body shapes [7]. Various biometric traits used in bio-metric applications are illustrated in Figure 1. Soft biometric qualities are combined with either the physical or behavioral characteristics to improve the accuracy of recognition [8-10]. Biometric traits are used to provide authentication

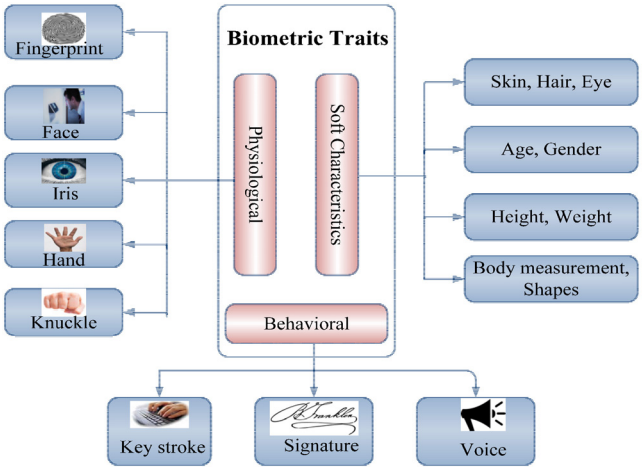


Figure 1. Biometric traits usedin security based applications

rights to access various sensitive data in organizations and industries [11-13]. Biometric trait of a person is encrypted using cryptography techniques to enhance the security [14-15, 17]. In security applications, securing the template is a key issue because, once the template is compromised, it cannot beused for authentication. Encrypting the template before storing it in the database mitigates this issue [18-20]. Bio-cryptosystem and cancelable biometrics are the two essential template protection schemes [21-25].

Combining cryptography with biometric enhances the security and exploits the benefits of both. Biometric applications that use crypto-algorithms for key generation and template protection are called bio-cryptosystems [26-29]. Bio-cryptosystems providestrong user authentication, efficientoperation and improved security in private and public sector applications such as control of security in border, crime, attendance recording, hacker prevention, payment system and access controls [30-32]. They can be broadly categorized into key release, key binding, and key generation bio-cryptosystems [33]. A bio-metric application can employ any one of the above mentioned techniques to maintain high level security

*Corresponding Author: Sanghyun Seo; E-mail: sanghyun@cau.ac.kr
DOI: 10.3966/160792642020092105011

[34-37].

Figure 2 shows the basic working principle of biometric system. The two phases involved in biometric system are: (i) enrollment phase and, (ii) verification phase. In enrollment phase, the biometric trait is acquired from the user. In the verification phase, the query template is compared with the template stored in the database. Similarities between the two templates are calculated by measuring and comparing the Euclidean distance [38].

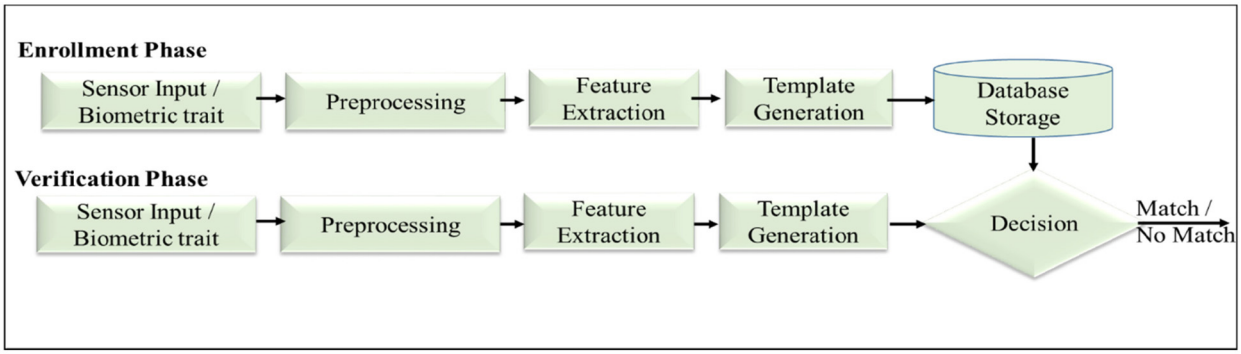


Figure 2. A typical biometric based authentication system

This paper is driven by recent methodologies and techniques in middle biometric template protection using both single-modal and multi-modal traits. A comprehensive survey on template protection schemes using multi-modal biometrics and cryptography techniques is presented in this paper. Rest of the paper is organized as follows: Section 2 discusses issues and challenges in bio-cryptosystem. Section 3presents the overview of the template protection schemes. Section 4 and 5 present the review on feature transformation and bio-cryptosystems. Section 6 discusses the authentication techniques based on multimodal biometrics. Section 7 presents strategies for improving performance metrics in biometric based authentication. Section 8 tabulates essential details of template protection schemes. Section 9 concludes the paper with the summary on biometric based authentication schemes.

2 Issues and Challenges in Biometric Based Authentication

Biometrics play vital role in authenticating an user to access the information stored in the database and also in transferring data in communication channels [41-44]. In biometric systems, the main issue in using the biometric trait for authentication is lack of secrecy and stability. Measuring the similarities between the two biometric templates extracted from two different users is known as inter-user similarity. Some of the issues and challenges in biometric based authentication are diversity, security, performance, accuracy, privacy, acceptability, distinctiveness, recoverability

Attack analysis is done to understand the strengths and weakness of biometric authentication by Xiao [15] and an effort is made to defeat the spoofing attacks to enhance security in multimodal biometrics. The attacks are shown in Figure 3. Table 1 presents the familiar biometric traits and their corresponding spoofing methods.

Several strategies for alteration, detection and liveness methods are discussed by Sousedik [36]. Fingerprint sensor spoofing methods during enrollment and Presentation Attack Detection (PAD) techniques are explained in subsequent subsections.

2.1 Fingerprint Sensor Spoofing Methods

Fingerprint spoofing technique is mainly classified into two classes, namely, indirect and direct casting. In direct casting, the original fingerprint is used to create the fake finger print. Covert fingerprints left by user are visualized and is used in creating the fake finger print. Presentation Attack Detection is used for fingerprint liveness and alteration as shown in Figure 4.

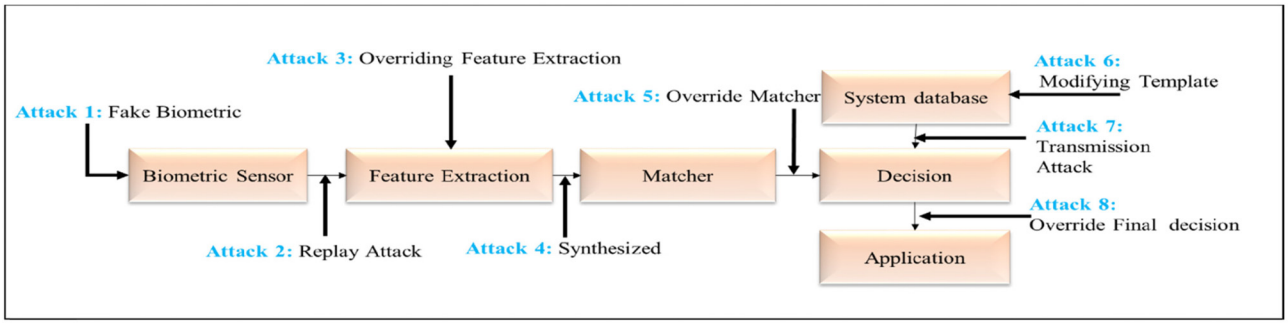


Figure 3. Possible attacks in applications using biometric authentication

Table 1. Biometric traits and spoofing methods

Biometric Traits	Spoofing Techniques and Methods			Anti-spoofing Techniques
	Spoofing Technique	Direct Casting	Indirect Casting	
Finger print	Use of fake fingers with mouldings using substances such as plastic and gelatine	Fake fingerprint using moulds such as latex, silicone, gelatine etc.	Digitized fingerprints, enhanced merits using image editing softwares	Liveness detection using sensors to detect temperature, heartbeat, skin resistance etc.
Face	Stored face image stolen for authentication	2D surfaces are used against 2D face recognition system	Different lighting and facial expressions	Use of facial thermo-grams
Voice	Stolen voices from telephone calls	Mimicry voice or sound	Voice recording in front of a speaker recognition system	Use of additional biometrics
Iris	Use of different types of contact lens and photo quality papers	Printout of an eye-image with high resolution printers can fool biometric scanner	Iris pattern is reconstructed from iris code	Liveness detection using multiple images of the same eye, variations in pupil dilation

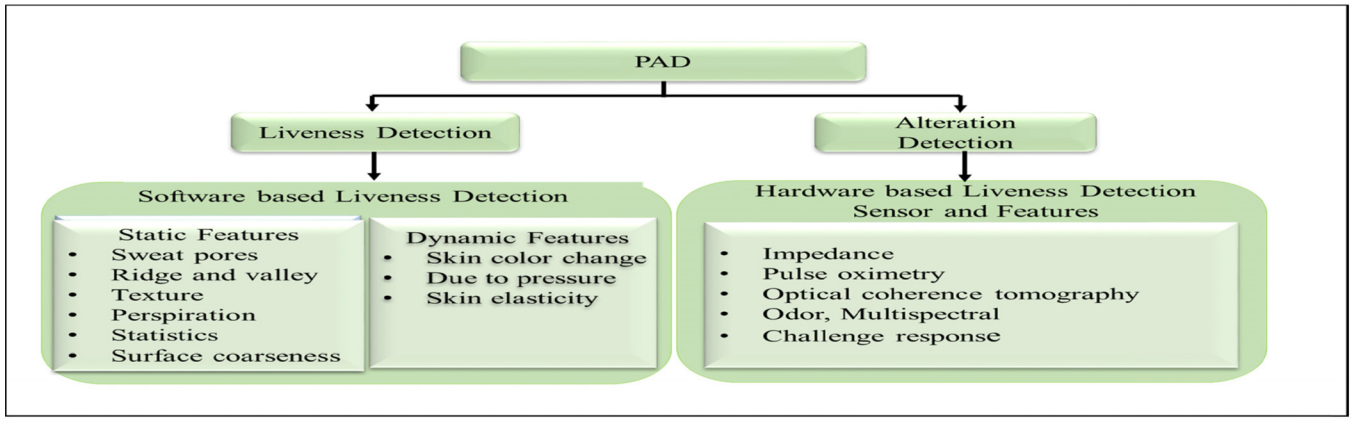


Figure 4. Presentation attack detection methods

3 Biometric Template Protection Schemes

Biometric authentication is implemented in various real time applications such as Automatic Teller Machine (ATM), Aadhaar identity, banking, and e-passport. Therefore, the security and privacy of biometric data, i.e. the template, is a major concern. The biometric templates are stored in encrypted form and require keys for decrypting the template. Literature survey indicates that there is a possibility for reconstructing the original biometric data from the template stored in database using Hill climbing attacks [38]. The general classification of existing template protection schemes is shown in Figure 5.

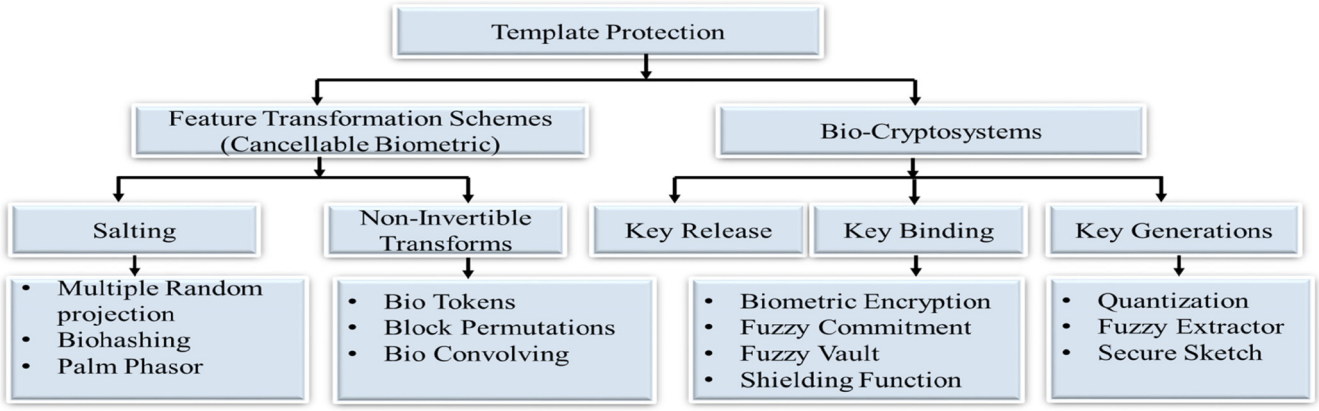


Figure 5. Classification of template protection schemes

3.1 Feature Transformation Using Cancelable Biometrics

In the cancelable biometric, one-way function is used to transform the template before storing it in the database. The biometric template can be revoked and re-enrolled using another transformation function, if it is compromised. Multiple cancelable templates can be constructed for one biometric trait and can be used for different applications [38-39]. Cancelable biometric can be generated using, (i) Biometric Salting and (ii) Non-invertible transforms.

3.1.1 Bio-salting and Feature transformation

In salting, features extracted from the biometric trait are transformed using a user-specific password or key. Since the key is an important parameter for transformation, it should be protected. Bio-salting techniques include bio-hashing, palm phasor and biophasoring [40]. Various operations in bio-salting technique are illustrated in Figure 6.

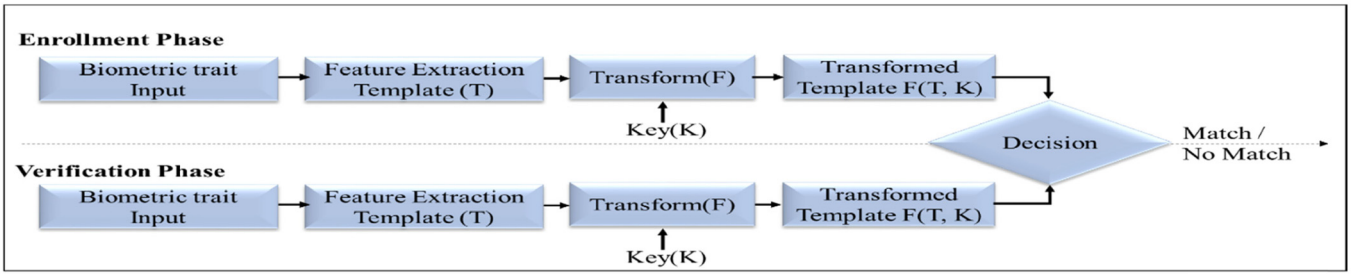


Figure 6. The process of bio-salting

3.1.2 Non-Invertible Transformation

The biometric template is protected using a non-invertible transform function, so that the original biometric cannot be re-constructed even if the key and the transformed template are known. The non-invertible transform methods are classified into biotokens, block permutations, bio-convolving etc. [40]. The process of non-invertible transform is shown in Figure 7.

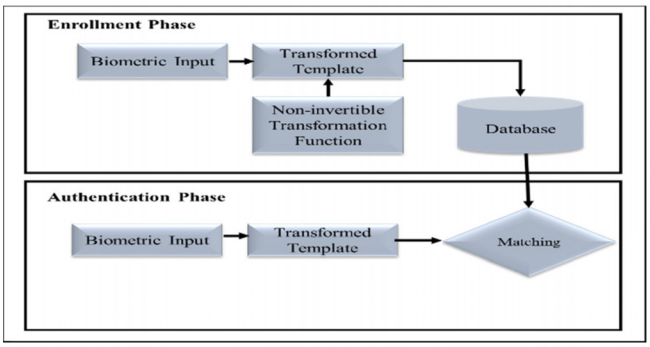


Figure 7. Process of non-invertible transformation

3.2 Bio-Cryptosystems

Bio-cryptosystems can be categorized into (i) key release based, (ii) key binding based, and, (iii) key generation based systems.

3.2.1 Key Release Based Bio-cryptosystem

In key-release based biometric systems, cryptographic keys are secured and stored in the user database record

3.2.2 Key Binding Based Bio-cryptosystem

In key binding systems, the cryptographic key is used to protect the biometric template. Thebiometric template and key are stored in a database and their combination is known as helper data or secure sketch [38].

Variations in the biometric template are corrected by employing Error Correction Code (ECC) [1, 5]. Four well-known methods that use key binding are (i) fuzzy vault and (ii) fuzzy commitment (iii) biometric encryption and, (iv) shielding functions. A typical Key binding bio-cryptosystem is shown in Figure 8.

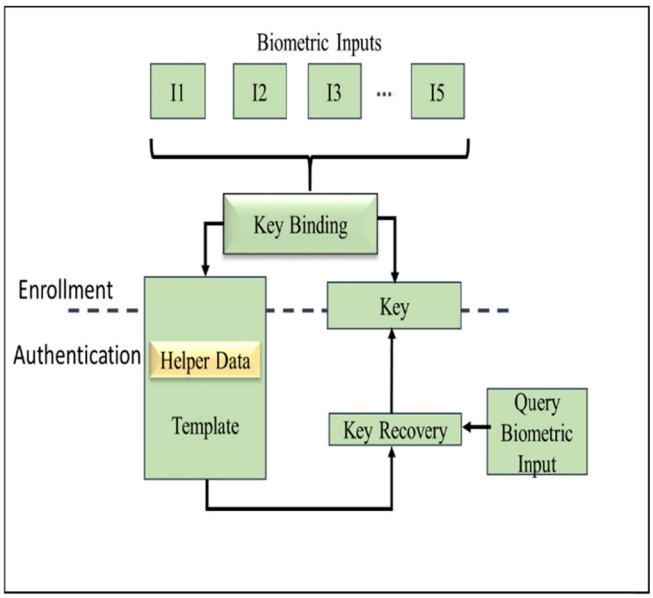


Figure 8. A typical key binding based bio-cryptosystems

3.2.3 Key Generation Based Bio-cryptosystem

In key generation, the crypto-key which is directly generated from the biometric samples during enrollment phase is stored in the database. If the key generation is done without the helper data, then there is no possibility for reconstructing the biometric template [6, 15]. The processes involved in key generation based bio-cryptosystems are shown in Figure 9.

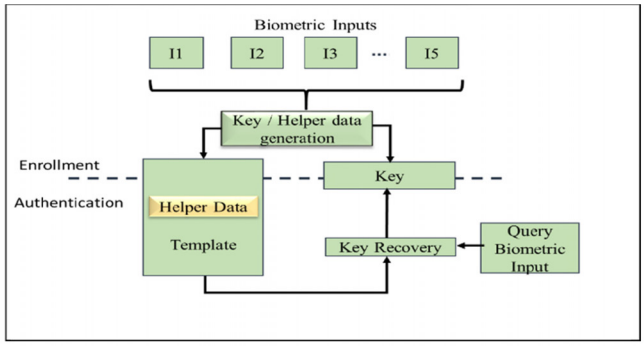


Figure 9. A typical key generation based bio-cryptosystems

4 Authentication Techniques Based on Feature Transformation

Various techniques have been proposed for template protection in the literature to improve the transformations for cancelable biometric. This section discusses authentication techniques based on feature transformation. Overview of authentication techniques based on feature transformation is given in Table 2.

4.1 Bio-Salting

Salting is done by adding random bits to the secret key. Bio-hashing, bio-convolving etc. are used for creating cancelable template. Lacharme [45] has proposed a hashing algorithm for protecting the template of the fingerprint. The biohashing algorithm is used to enhance the accuracy and execution of the biometric scheme. In [46], Belguechi et al. have discussed an adaptation of bio-hashing using local matching and produced a cancelable template to secure the fingerprint. Sandhya et al. [32] have proposed Delaunay triangulation algorithm in feature extraction for fingerprint template protection scheme.

Table 2. Authentication techniques based on feature transformation

Ref	Description	Biometrics	Results Achieved / Parameters Improved				Merits/Demerits / Limitations
			FAR	FRR	EER	GAR	
[31]	Delaunay triangulation algorithm Based on FS_INCIR, FS_AVGLO Cancelable template is generated by multiplying the user key with complex vector	Fingerprint, FVC2004, and FVC 2002	Supports irreversibility and recoverability				Alignment free face images Storage of template takes more space and takes more time for identity matching
[35]	Adaptive bloom filter Biometric template protection, compression of biometric data nd acceleration of biometric identification	Iris, CASIA-v3	The template is compressed to 20-40% from original size and the 5% of bit is reduced during the comparison				Template protection is improved Not surveyed with unknown auxiliary data
[45]	Biohashing algorithm Hashing technique for template protection	Finger print, FVC2002-DB2	-	-	0%	100%	Template protection is improved Not surveyed with unknown auxiliary data
[46]	Bio-hashing using local matching algorithm Cancellable template is generated using local matching	Finger print, FVC2002	-	-	6.68%	-	Privacy preservation and security are improved
[47]	ECC-free key binding scheme, Modified Random Graph-based Hamming Embedding transform (MRGHE), Minutiae vicinity decomposition	Finger print, FVC2004	0.16%	11%	-	89%	Security and privacy is improved Accuracy is low with high entropy Not limited tobinary feature representation
		Finger print, FVC 2002	0.061%	3%	-	97%	
[48]	Bloom filter based Secure Multiparty Computation (SMC) protocol based on SHADE and Yao's garbled circuit protocol	Iris, IIITD DB version 1.0	Provides unlinkability and irreversibility				Speed, efficiency and performance are improved Small amount of information is leaked from the stored data
[49]	Modified Bloom filter based Log Gabor filter and Dyadic wavelet transform	Iris, CASIA-IrisV1	0.01%	.8%		99.2%	Increases the recognition speed Provides high level of security No significant degradation of biometric performance

4.2 Non-Invertible Transformations

In non-invertible transformation, thecancelable template is generated and stored in the database in which it is hard to invert the template. Rathgeb et al. [35] have described an adaptive bloom filter using iris code to improve the template protection. Bringer et al. [48] have proposed a Secure Multiparty Computation (SMC) protocol to improve secure matching score.

5 Authentication Techniques Based on Bio-cryptosystems

This section discusses the authentication techniques based on bio-cryptosystems that are available in the literature. As specified in Section 2, authentication techniques based on bio-cryptosystems are divided into (i) Key release, (ii) Key binding and, (iii) Key generationsystems. The summary of authentication techniques based on bio-crypto systems is presented in Table 3.

Table 3. Authentication techniques based on bio-cryptosystem

Ref	Description	Biometrics	Results Achieved / Parameters Improved				Merits/Demerits / Limitations
			FAR	FRR	EER	GAR	
[10]	Cascade Linear Discriminant (CLD) Analysis, Generalized Symmetric Max Minimal Distance in Subspace(GSMMDS)	Face	00009%	0.074%	-	-	Non-intrusive Consumes large data storage
[16]	Two-layer error correction technique (Hadamard and Reed-Solomon codes)	Iris, 70 iris samples	0.5%	0.5%	-	99.5%	Generates different biometric keys using single biometric Provides good security with better performance and achieves less error rate
			Generates 140-bit length key				
[17]	Lattice Mapping based fuzzy commitment scheme and K-nearest Neighborhood (k-NN) classification	Biometric	Accuracy is improved				Original biometric is not stored It is possible to generate different keys from the same biometric characteristics
[18]	Modified vector quantization	Biometrics	0%	6%	-	-	Provides high security expensive
			Generates 128-bit length encryption key				
[21]	Fuzzy vault	FVC2002 DB2	0%	-	-	90% Where N=10	No data leakage Prone to various attacks such as brute force attack, dictionary attack, Attack via Record Multiplicity (ARM)
		MSU-DBI	0%	-	-	87.5%	
[22]	Fuzzy commitment – SHA1 Secure Hash Algorithm	Finger print, FVC2002	0%	-	-	75%	Improves fuzzy vault algorithms True minutiae is displayed clearly No security analysis is done
[24]	Designing a protocol The biometric crypto keys generates session keys for one communication session	Biometrics	0%	0.63%	-	-	No need for third party authentication and costly third party certificates.
			Generates 54-bit length key				
[29]	Fuzzy Extractor - Hamming distance method	Iris, CASIA DB	4.42%	9.67%	-	90.33%	Issues in key management and key bit length generation
[37]	Texture based Fuzzy Extractor, Local Direction Pattern(LDP) and Gabor filter for feature extraction, Fuzzy Commitment	Finger print, FVC2000 DB	0%	-	-	76%	Quality of the biometric is improved using center point and tessellation Effective error correcting code
			Generates 76-bit length key				
[50]	Fuzzy commitment, Shannon approximation model		0%	3.72%	-	96.22%	Overall complexity is reduced Shift key function is not implemented The template consumes time and more large memory space
			400 bit length of crypto key is generated				

Table 3. Authentication techniques based on bio-cryptosystem (continue)

Ref	Description	Biometrics	Results Achieved / Parameters Improved				Merits/Demerits / Limitations
			FAR	FRR	EER	GAR	
[51-53]	Biometric Encryption	Fingerprint	Complex valued arrays with floating point description are used in Key generation				Encryption and decryption can be done using key
[54]	Shielding Function	Biometric	Delta-contracting and epsilon revealing are the parameters which is used in shielding function				Prevents threats from misuse of user templates
[55]	Gabor filtering, reliable component scheme	Fingerprint, FVC 2000	-	-	4.2%	95.8%	Noise correction is done after quantization
[56]	Shielding function and WFMT method	Finger print	-	-	3.8%	-	There is enough entropy for managing the secret
[57]	Finger vein-high dimensional space self–stabilization algorithm	Finger vein	0.8%	-	0.5%	99.9%	Supports high level of security and error rate is reduced
			Generates 256-bit length key				
[58]	Biometric-based encryption and decryption scheme, water marking Key is generated	Finger print	Total execution time of the proposed algorithm is 0.204s				Reduces the security threats and there is no need to store asymmetric key Issues in standardizing binary bit data without loss of information
[59]	K-means algorithm, Standard Encryption algorithms	Handwritten Signature	0%	0%	-	100%	Robust encryption keys can be generated Stability of the key is an issue
[60]	Robust hashing function and cryptographic function MD5, SHA-1, Singular Value Decomposition (SVD)	Face, ORL face database	5% to 10% tolerance factor is achieved				Security and privacy of the face database are improved Limited number of images used for testing
[61]	Fuzzy extractor – Secure Sketch scheme	Fingerprint, FVC database DB3 and DB4	19% and 20% accuracy for Scenario1 and Scenario2 respectively Leakage on identities is 4.9 bits in both Scenarios				Key strength and privacy are measured.
[62]	Secure Sketch, Two level quantization	Biometric data	Generates < 450 bits key				Supports security and protection
[62-64]	Key generation Scheme, interval-mapping scheme	Iris, CASIA v3	5%	5%	-	95%	Biometric templates encrypted form of biometric is stored in the database

5.1 Authentication Techniques Based on Key Binding

In key binding techniques, the key or biometric template is not revealed to the impostor. One of the techniques used in key-binding is fuzzy vault template protection technique. Nandhakkumar et al. [21] have proposed afully automatic implementation of the fuzzy vault scheme based on fingerprint minutiae.

A lattice mapping based fuzzy commitment scheme forCryptographic key generation from biometric data is proposed in [17]. A novel fuzzy commitment scheme for generating iris-based cryptographic keys for authentication and cryptographic data protection is proposed in [50]. A 400-bit length crypto- key is generated independently and is combined with biometric data by applying the XOR-partner information.

Biometric Encryption (BE) algorithm is proposed for key management process [51]. In [51-53], the biometric encryption algorithm is developed using a biometric image to generate the key. The key generated from the biometric encryption algorithm is used to link and retrieve the digital key. In [54], the δ contracting and ┼- revealing functions are used in pre-processingfor biometric authentication. The concept introduced by Tulys [54] uses shielding functions. In [55], a reliable component scheme is applied for the fingerprint inorder to achieve 4.2% EER and the secret 40-bit length. In [56], the shielding functions and the WFMT method are used in fingerprint based key binding scheme to solve issues in the key management bio-cryptosystems.

5.2 Authentication Techniques Based on Key Generation

In the key generation bio-cryptosystems, the key generated from biometric template is directly stored in the database. Chang et al. [10] have proposed an algorithm to generate stable cryptographic keys from the unstable biometric data.

A modified vector quantization approach is proposed in [18] to overcome the variability in

biometric key generation where basic idea is partitioning feature space into subspaces and partitioning subspaces into cells. Hao et al. [16] have proposed a secured approach to combine iris biometric with cryptographic applications.

A simple and effective protocol to share crypto-biometric keys in secured manner is proposed in [24] which generate session keys that are valid only for one communication session. Alvarez Marino et al. [29] have proposed a fuzzy extractor scheme based on hamming separation system for key generation.

Imamverdiyev et al. [37] have proposed texture based feature extractor strategy to improve the template protection. The finger print used for key generation is enhanced using center point and tessellation. Local Direction Pattern (LDP), Local Binary Pattern (LBP) and Gabor filter are the feature extraction techniques used in feature extraction.

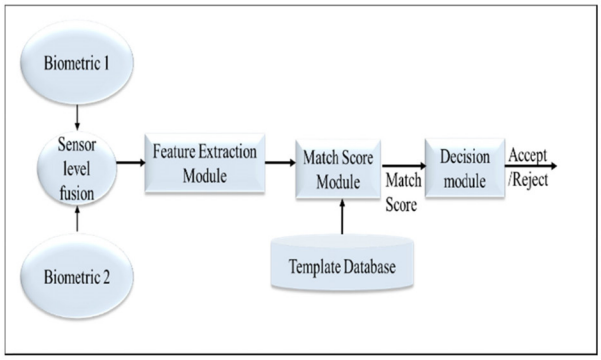
Wu et al. [57] have proposed Finger Vein-High dimensional Space (FVHS) self-stabilization algorithm to improve user authentication in Cloud. It reduces the number of weak network keys.

A biometrics-based encryption/decryption scheme to generate a unique key using fingerprint is proposed in [58]. In [59], the biometric keys are generated from the live biometrics. A robust hash function which is a one way-transformation that is used to secure the biometric based authentication is proposed in [60]. The simplified asymmetric setting and secure sketch scheme based on the fuzzy extractor are presented in [61]. The key strength and privacy issues are the parameters analysed and measured to improve the key generation in biometric secure system. To solve the above issue in [62] two-level quantization is constructed which is more effective than the natural method of assigning one bit to each coefficient. Rathgeb and Uhl [63-64], have proposed an iris biometric interval-mapping scheme for generating the cryptographic keys.

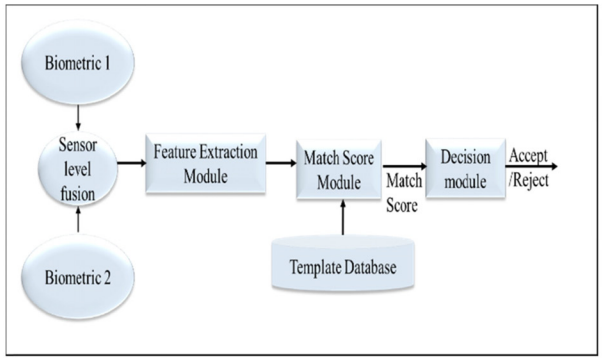
6 Authentication Techniques Using Multi-modal Biometrics

Multimodal biometric combines more than one biometric trait to improve the accuracy in authentication. Single modal biometric authentication cannot warranty 100% identification rates and 0% false acceptance and rejection rates. This limitation can be overcome by using multimodal biometrics, as it is difficult to defeat two or three biometric systems [13]. Multimodal authentication can be performed using the following modes: (i) Serial Mode (ii) Parallel Mode.

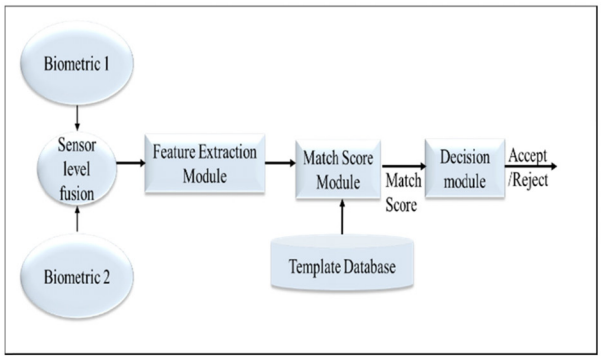
Fusion of two or more biometric traits can be done at various levels: (i) sensor level: multiple raw features extracted from different sensors are combined; (ii) feature; (iii) score level; (iv) decision level, (v) rank level. Variouslevels of fusions are illustrated in Figure 10.



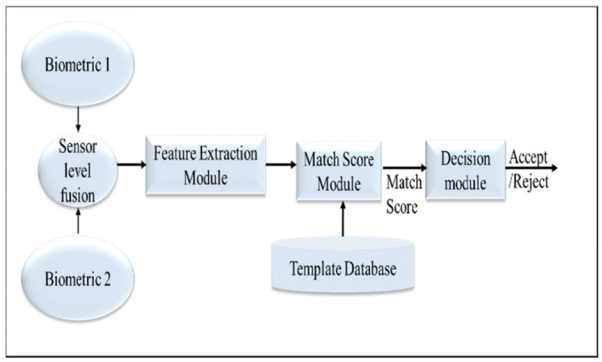
(a) Sensor level fusion in multimodal biometrics



(b) Feature level fusion in multimodal biometrics



(c) Score level fusion in multimodal biometrics



(d) Decision level fusion in multimodal biometrics

Figure 10. Different types of fusion levels in biometric authentication (a) sensor level fusion, (b) feature level fusion, (c) score level fusion, (d) decision level fusion

Faunder-Zanny [13] havedone analysis of fusion at various levels in order to improve the performance ofidentification. Various levels of fusion shown in Figure 10 are analysed in [13]. Seno et al. [4] have proposed a co-located model and separated model for network authentication system with multimodal biometrics to improve the processing speed

Zewail et al. [11] have proposed a weighted averaging and parzen classifier for fusion to improve the system reliability and efficiency. A prototype of a biometric verification system based on the fusion of palmprint and facial features is proposed in [19] for physical access control.

Cheung et al. [20] have proposed intra and intermodal two-level fusion strategies for audio-visual biometric authentication. The result shows that intermodal and intramodal are complementary to each other and that SVM-based intermodal fusion is superior to linear combination.

Roy et al. [33] have proposed fusion at the score level for multimodal framework that optimizes and integrates the iris and face features. Weak and strong classifiers to improve the speed and memory constraint of multimodal biometric recognition are proposed in [65]. The candidate's list at each stage. In [65], the performance is evaluated for both the single and the multimodalor measuring the effectiveness of the approach. The disadvantage of using cascade is the increasing complexity when more number of stages are added.

Lumini et al. [66] have proposed a combination of biometric matcher level fusion to improve the recognition performance. Veluchamy et al. [67] have proposed a multimodal biometric recognition system by combining the finger knuckle and finger vein images. Jagadiswary et al. [68] have proposed a modified RSA-decryption algorithm for the key generation process to enhance verification accuracy of multimodal biometrics.

Mehrotra et al. [69] have proposed an improved classifier which uses multimodal biometric score to generate good quality training data. Sandhya [70] has proposed Query-Based Biometric Systems (QBBS) for the soft multibiometrics framework to improve privacy-perseverance. Thasiyabi et al. [71] have proposed multi-algorithmic approach for the multimodal biometric fusion involving fingerprint and face.

Amirthalingam et al. [72] have proposed a Particle Swarm Optimization (PSO) algorithm to improve the biometric data security. Meraoumia et al. [73] have proposed a Phase-Correlation Function (PCF) algorithm to enhance the execution of the multimodal biometric system for person recognition. In [90], the authors proposed bloom filters for template protection. To enhance the privacy protection the newly protected weighted feature level fusion is proposed. The hybird template protection for biometric authentication which takes the benefits of both the techniues [91]. The hybird template protection based on random orthonormal project for template protection which guaranteed with fuzzy commitment protocol. Details about various multimodal biometric techniques are presented in Table 3.

Table 4. Summary of multimodal biometric techniques

Ref	Description	Biometrics	Results Achieved / Parameters Improved				Merits/Demerits / Limitations
			FAR	FRR	EER	GAR	
[4]	Co-located model and separated model Two prototypes, Type A and Type B, for network authentication are proposed	Face, Fingerprint, Signature	-	-	-	-	Combines serial and parallel systems Improves the performance of the recognition
[11]	Steerable pyramid decomposition and log-Gabor filtering Integrates the soft and hard biometrics		-	-	-	-	Provides better evaluation and efficient management of authentication system
[13]	Opinion level and decision level Various levels of fusion in multimodal biometrics are analysed	Iris, fingerprint	0.0882	0.00002	-	-	Improves template security
[19]	Fusion biomodel Fusion at match score level	Palmprint, Facial features	-	-	-	-	Improves performance of the system
[20]	Support vector machine Intra and inter-level fusions are used	Audio-visual,	11%	11%	-	89%	Simplifies verification
[33]	Fuzzy C-means clustering with the level set (FCMLS), Genetic and Evolutionary feature extraction Optimises and integrates fusion at score level	Iris and face	-	-	-	100%	Supports less computational time

Table 4. Summary of multimodal biometric techniques (continue)

Ref	Description	Biometrics	Results Achieved / Parameters Improved				Merits/Demerits / Limitations
			FAR	FRR	EER	GAR	
[65]	Weak and strong classifiers Reduces the enrollment users list	Iris, Finger print	-	-	-	-	Improves speed and reduced memory Increases the complexity of the whole system
[66]	Ensemble classifiers Analysis on various fusion techniques, score level fusion is used Fingerprint	Various datasets	-	-	-	-	Increases usability and lower sensitivity
[67]	Fraction theory and Firefly algorithm, and K-Neural Network - SVM classifiers Weighted score level fusion is used	Finger knuckle and finger vein images	4%	4%	-	96%	Improves performance and recognition
[68]	Modified RSA-decryption algorithm Feature level fusion is used	Fingerprint, retina and finger vein	0.01%	4.7%	-	95.3%	Improves verification accuracy, Supports higher security against anti-spoofing
[69]	Incremental and Granular learning in RVM (IGRVM) [69] Preserves the sparse property of the original RVM classifier	Multi-modal biometrics	0.10%	.86%	-	99.14%	Supports scalability Reduces testing time
[70]	Query-based biometric system Proposes privacy preserving frame work	Face, fingerprint, height, weight, age, gender	1%	1%	-	99%	Provides privacy without effecting the performance of the system Prone to attacks
[71]	PCA and Modular kernel PCA	Fingerprint, face	10%	11.11%	-	90%	Reduces FAR and FRR Requires large amount of time and memory
[72]	Modified Region growing, Local Gabor XOR pattern, Particle Swarm Optimization (PSO)	Face, Ear	0%	-		90%	Reduces the noise
[73]	Phase Correlation Function (PCF) Multimodal Biometrics for person recognition	Face, Fingerprint, Signature	.4%	.4%	-	99.6%	Enhances the execution speed Supports high security

7 Improving the Performance and Quality of Biometrics Based Authentication

In biometric applications, biometric trait is acquired through sensors. The acquired image has different types of noise due to illumination, environment, and humidity. If the quality of the biometric image is too low, then, the feature extraction will not provide accurate results. Therefore, pre-processing techniques are used to remove the noisy data in order to improve the quality of the image. Normalization and histogram equalization are the most properly used pre-processing techniques. The performance of the biometric application depends on the following factors: (i) False Acceptance Rate (FAR): The unauthorized person is identified incorrectly as authorized person is known as false acceptance rate and (ii) False Rejection Rate (FRR): The authorized person is rejected as unauthorized person.

Various algorithms and techniques are used to improve the quality of the biometric images are summarized in Table 5.

Palm print capturing devices, pre-processing, verification algorithms and related fusion algorithms for real-time palmprint identification in large databasesare presented in [23]. Finger print image rotation based on minutiae and singular point features is analysedin [25]. In order to enhance the low-quality of the finger print image, a novel method is proposed in [28]. It is the first methodwhich estimates local orientation of the fingerprint ridge and valley.

The quality assessment algorithms to enhance the finger print image arepresented in [31]. Various algorithms for improving the qualityof acquired image along with their descriptions are listed in Table 4. A novel fingerprint fuzzy vault scheme based on ridge features with the goal of improving its performance for distorted fingerprint images is proposed in [34].

Table 5. Algorithms used for improving the quality measures in fingerprint

Ref	Name of the Algorithm/ Technique	Description of the proposed solution	Results
[74]	Frequency Domain Analysis (FDA) Uses Machine Computing Score(MCS) and Human Excepted Score (HES)	Operates in a block-wise manner. The quality measure is used to rank the performance of a fingerprint.	15.89% of trend error
[75]	Gabor (GAB) improves the quality Bank of Gabor filter, Orientation Certainty Level (OCL), Ridge-valley Structure (LCS), Ridge-valley Uniformity (RVU), Frequency Domain Analysis (FDA), Radial Power Spectrum (POW) and Orientation Flow (OF)	Feature operates on per-pixel level	Highest correlation with utility was obtained using the Orientation Flow (OF)
[76]	Gabor-Shen (GSH) quality	Gabor filter with variance algorithm used to improve the quality of the finger print image.	94.4% accuracy Increased the computation speed
[77]	Local Clarity Score (LCS), Global Clarity Score (GCS) and Global Orientation Quality Score (GOQS) are measured and are used to calculate the Overall Image Quality (OIQ)	Ridge flow continuity and absolute orientation difference are measured between blocks and its neighbour block	15.8910% of trend error
[78]	Orientation certainty level (OCL)	Measuring the strength of the energy concentration along dominant ridge flow orientation in block -wise manner	Score provides low quality and invalid fingrprint
[79]	Global finer image quality Measuring two quality indices such as (i) measures the energy concentration on frequency domain as global feature, (ii) measures spatial coherence in local region.	Radio power spectrum is a power of maximum signal power in a defined frequency band of the global radial Fourier spectrum.	1.94% EER

Hilal et al. [80] have proposed elastic strips standardization approach to enhance the iris recognition. Approximated Pupil Center (APC) and Pupil Gravity Center (PGC) are used in normalization to improve the system performance in matching.

The study of various problems in finger quality enhancement and the solution for those problems are analysed in [80]. The evaluation of the quality metric on the enrolment selection is presented in [81]. The analysis of different compression techniques to improve the performance of ear biometric recognition system is presented in [82]. The statistical-based and dynamic pre-processing techniques to enhance the low-quality of the fingerprint biometric are proposed in [83].

Fernandez-Saavedra et al. [84] have discussed about the impact of small fingerprint scanners quality and the performance of the system. Ross and Govindarajan [85] have proposed a feature level fusion technique to enhance the performance of the face and the hand biometrics.

Yan and Bowyer [86] have proposed an on-line method for the ear segmentation to enhance the execution of the ear biometric system. Passi and Kumar [87] have proposed FFT based features, DCT, Haar wavelet and log Gabor to enhance the execution of the IRIS confirmation. The three local features computed under the frame work of phase congruency to improve the Finger Knuckle print recognition accuracy is proposed in [88]. The local orientation, local phase, and local congruency are the three features extracted and fused at score level. Local features are again combined with the global features, Fourier transform co-efficient is used to validate the recognition of finger Knuckle print. The best verification result is achieved with EER 0.356% for benchmark FKP database. The quality measurement of the biometric is detailed in Table 6.

Table 6. A Summary of biometric quality measurement

Ref	Name and Description the Algorithm / Technique	Biometrics	Description
[2]	Image restoration algorithms (a) Heuristic regression-based, (b) Scatter Matrices, (c) LMS type algorithm	Any biometric Image	Improves quality and efficiency of the image 9.370968 and 11.484837 % mean error/pixel
[9]	Asymmetric matching algorithms	Biometric images	Lack in analysing the feature extraction technique Improves accuracy in biometric matching
[23]	Line-, subspace- and statistic-based verification algorithms	Palm print	Issues which are not well addresses are stability of the principles lines and the wrinkles Supports privacy of the image

Table 6. A summary of biometric quality measurement (continue)

Ref	Name and Description the Algorithm / Technique	Biometrics	Description
[25]	Feature rotation is recommended	Finger print	7% key bits affected due to feature transformation 96% accuracy
[28]	Orientation diffusion filtering	Finger print	Automatic and reliable estimation methods are a challenging task for low and very low quality of prints Increases performance and recognition of the fingerprint
[31]	NIST (National Institute of Standards and Technology) Fingerprint Image Quality (NFIQ) algorithm	Finger print	Identifies best quality of the features Based on the dataset varies in FRR
[34]	Novel noise generation algorithm for chaff ridge technique	Finger print	Improves template security 75% accuracy
[80]	Elastic strips normalization (i) Approximated Pupil center (APC), (ii) Pupil Gravity Center (PGC)	Iris	Improves system performance in matching Achieves 10.69% decidability for PGC
[81]	Calculating intra-class and inter-class matching scores and again calculating global EER value from the new match scores	Finger print	Less investigation on various quality measurement 11.34%, 13.48%, 11.61%, 11.52% EER for Bozorth3 1.16%, 1.70%, 1.15%, 1.42% EER for SDK
[82]	Feature extraction: Local binary pattern (LBP), Local phase quantization (LPQ), Histogram of orientation gradients (HOG), Binarised statistical image features (BSIF)	Ear	The test work is not stimulated on real surveillance footage Improves performance of recognition
[83]	Statistical-based and dynamic	Finger print	Enhances the binarised images 89.1% accuracy
[84]	Worsening the quality and error rates as the fingerprint scanner is reduced	Finger print	Reducing fingerprint size worsens in quality and increases error rate
[89]	Feature selection: Genetic Algorithm, Memetic Algorithm, and Practical Swarm Optimization Classification: K-Nearest Neighbors, SVM, Optimum path Forest and Euclidean Distance	ECG	Improves the recognition rate Feature extracted from the ECG signal provides high recognition rates

8 Discussion and Future Scope

In this survey the exisitng works based on authentication is evaluated in terms of accuracy, False Accpetance Rate (FAR), False Rejection Rate (FRR) and Equal Error Rate (EER). The algorithm, related biometric and merits and demerits of the related works are expalined for each section in Table 2, Table 3, Table 4 and Table 5. The survey expalins about working of the biometric systems and issues and challenges in using the biometric for authentication. The two types of template protection schemes such as cancelable biometric and biocrytposystems are presented in section 4 and 5.

The open research issues in biometric authentication are:

First, as per the serious survey the papers didn't dicussed about the attack analysis and computational cost which is still needs to be imporved.

Second, the liveness detection should be considered for the biometrics to avoid spoofing attacks..

Third, privacy and security of the biometric are still an open issue. The non-invertiabillity and recoverability are discussed in few papers. Still more investigation is need in imporving the security and privacy of the biometric.

Fourth, the quality of the biometric image is also plays a vital role is increasing the accuracy. Table 4 and Table 5 are mostly concenrated on improving the finger print quality.

9 Conclusion

Two main approaches for protecting the template are cancelable biometric and biometric cryptosystems. Both the approaches have their own pros and cons. This paper presents an overview of various bio-cryptosystems and cancelable biometric for template protection. Security and privacy of biometric systems are enhanced with the help of template protection schemes. This paper also discusses attacks, issues and challenges in using biometric authentication. Further, the paper also gives an overview of multimodal biometric which overcome the drawbacks in unimodal. The key idea behind this survey is combining the cancelable biometric and the bio-cryptosystem as a hybrid approach using the multimodal biometric, this

hybrid technique would increase both the security and accuracy of the system for authentication as well protection of the biometric template.

References

[1] N. Ratha, J. Connell, R. Bolle, Enhancing Security and Privacy in Biometrics-Based Authentication Systems, *IBM Systems Journal*, Vol. 40, No. 3, pp. 614-634, 2001. Doi: 10.1147/sj.403.0614.

[2] C. Cocianu, L. State, V. Panayiotis, On A Certain Class of Algorithms for Noise Removal in Image Processing: A Comparative Study, *Proceeding International Conference on Information Technology: Coding and Computing*, Las Vegas, NV, USA, 2002, pp. 111-116.

[3] J. Dugelay, J. Junqua, C. Kotropoulos, R. Kuhn, F. Perronnin, I. Pitas, Recent Advances in Biometric Person Authentication, *IEEE International Conference on Acoustics, Speech, and Signal Processing*, Orlando, FL, USA, 2002, pp. IV-4060-IV-4063.

[4] S. Seno, T. Sadakane, Y. Baba, T. Shikama, Y. Koui, N. Nakaya, A Network Authentication System with Multi-Biometrics, *9th Asia-Pacific Conference on Communications*, Penang, Malaysia, 2003, pp. 914-918.

[5] C. Soutar, D. Roberge, A. Stoianov, R. Gilroy, B. V. K. Vijaya Kumar, Biometric Encryption Using Image Processing, *Proceedings SPIE*, Vol. 3314, pp. 178-188, April, 1998.

[6] A. Bodo, *Method for Producing a Digital Signature with Aid of a Biometric Feature*, Germany: German patent DE 42 43 908 A1, 1994.

[7] E. Tabassi, C. L. Wilson, C. I. Watson, *Fingerprint Image Quality*, NIST Technical Report NISTIR 7151, August, 2004.

[8] P. Grother, E. Tabassi, Performance of Biometric Quality Measures, *IEEE Transactions on Pattern Analysis And Machine Intelligence*, Vol. 29, No. 4, pp. 531-543, April, 2007.

[9] M. Gamassi, M. Lazzaroni, M. Misino, V. Piuri, D. Sana, F. Scotti, Accuracy and Performance of Biometric Systems, *Proceedings of the 21st IEEE Instrumentation and Measurement Technology Conference*, Como, Italy, 2004, pp. 510-515.

[10] Y. J. Chang, W. Zhang, T. Chen, Biometrics-based Cryptographic Key Generation, *IEEE International Conference on Multimedia and Expo*, Taipei, Taiwan, 2004, pp. 2203-2206.

[11] R. Zewail, A. Elsafi, M. Saeb, N. Hamdy, Soft and Hard Biometrics Fusion for Improved Identity Verification, *The 47th Midwest Symposium on Circuits and Systems*, Hiroshima, Japan, 2004, pp. I-225- I-228.

[12] A. Jain, S. Pankanti, S. Prabhakar, L. Hong, A. Ross, Biometrics: A Grand Challenge, *Proceedings of the 17th International Conference on Pattern Recognition*, Cambridge, UK, 2004, pp. 935-942.

[13] M. Faundez-Zanuy, Data fusion in Biometrics, *IEEE Aerospace and Electronic Systems Magazine*, Vol. 20, No. 1, pp. 34-38, January, 2005.

[14] Y. Chen, S. Dass, A. Jain, Fingerprint Quality Indices for Predicting Authentication Performance, in: T. Kanade, A. Jain, N. K. Ratha (Eds.), *Audio- and Video-Based Biometric Person Authentication, AVBPA 2005, Lecture Notes in Computer Science*, Springer, Berlin, Heidelberg, 2005, pp. 160-170.

[15] Q. Xiao, Security Issues in Biometric Authentication, *Proceedings from the Sixth Annual IEEE Systems, Man and Cybernetics (SMC) Information Assurance Workshop*, West Point, NY, USA, 2005, pp. 8-13.

[16] F. Hao, R. Anderson, J. Daugman, Combining Crypto with Biometrics Effectively, *IEEE Transactions on Computers*, Vol. 55, No. 9, pp. 1081-1088, September, 2006.

[17] G. Zheng, W. Li, C. Zhan, Cryptographic Key Generation from Biometric Data Using Lattice Mapping, *18th International Conference on Pattern Recognition (ICPR'06)*, Hong Kong, China, 2006, pp. 1-4.

[18] S. Hoque, M. Fairhurst, G. Howells, F. Deravi, Feasibility of Generating Biometric Encryption Keys, *Electronics Letters*, Vol. 41, No. 6, pp. 309-311, March, 2005.

[19] S. Ribaric, I. Fratric, K. Kis, A Biometric Verification System Based on the Fusion of Palmprint and Face Features, *ISPA Proceedings of the 4th International Symposium on Image and Signal Processing and Analysis*, Zagreb, Croatia, 2005, pp. 12-17.

[20] M. C. Cheung, M. W. Mak, S. Y. Kung, A Two-Level Fusion Approach to Multimodal Biometric Verification, *IEEE International Conference on Acoustics, Speech, and Signal Processing*, Philadelphia, PA, USA, 2005, pp. V-485- V-488.

[21] K. Nandakumar, A. Jain, S. Pankanti, Fingerprint-Based Fuzzy Vault: Implementation and Performance, *IEEE Transactions on Information Forensics and Security*, Vol. 2, No. 4, pp. 744-757, December, 2007.

[22] F. Chafia, C. Salim, B. Farid, A Biometric Crypto-system for Authentication, *International Conference on Machine and Web Intelligence*, Algiers, Algeria, 2010, pp. 434-438.

[23]A. Kong, D. Zhang, M. Kamel, A Survey of Palmprint Recognition, *Pattern Recognition*, Vol. 42, No. 7, pp. 1408-1418, July, 2009.

[24] S. Kanade, D. Petrovska-Delacretaz, B. Dorizzi, Generating and Sharing Biometrics Based Session Keys for Secure Cryptographic Applications, *Fourth IEEE International Conference on Biometrics: Theory, Applications and Systems*, Washington, DC, USA, 2010, pp. 1-7.

[25] P. Zhang, J. Hu, C. Li, M. Bennamoun, V. Bhagavatula, A Pitfall in Fingerprint Bio-Cryptographic Key Generation, *Computers & Security*, Vol. 30, No. 5, pp. 311-319, July, 2011.

[26] D. Gonzalez Martinez, F. Gonzalez Castano, E. Argones Rua, J. Alba Castro, D. Rodriguez Silva, Secure Crypto-Biometric System for Cloud Computing, *International Workshop on Securing Services on the Cloud*, Milan, Italy, 2011, pp. 38-45.

[27] P. Li, X. Yang, H. Qiao, K. Cao, E. Liu, J. Tian, An Effective Biometric Cryptosystem Combining Fingerprints with Error Correction Codes, *Expert Systems with Applications*, Vol. 39, No. 7, pp. 6562-6574, June, 2012.

[28] C. Gottschlich, C. Schönlieb, Oriented Diffusion Filtering for Enhancing Low-Quality Fingerprint Images, IET Biometrics, Vol. 1, No. 2, pp. 105-113, June, 2012.

[29] R. Álvarez Mariño, F. Hernández Álvarez, L. Hernández Encinas, A Crypto-biometric Scheme Based on Iris-templates with Fuzzy Extractors, *Information Sciences*, Vol. 195, pp. 91-102, July, 2012.

[30] C. Toli, B. Preneel, Provoking Security: Spoofing Attacks Against Crypto-biometric Systems, *World Congress on Internet Security*, Dublin, Ireland, 2015, pp. 67-72.

[31] M. Olsen, V. Šmida, C. Busch, Finger Image Quality Assessment Features – Definitions and Evaluation, *IET Biometrics*, Vol. 5, No. 2, pp. 47-64, June, 2016.

[32] M. Sandhya, M. Prasad, R. Chillarige, Generating Cancelable Fingerprint Templates Based on Delaunay triangle Feature Set Construction, *IET Biometrics*, Vol. 5, No. 2, pp. 131-139, June, 2016.

[33] K. Roy, J. Shelton, B. O'Connor, M. Kamel, Multibiometric System using Fuzzy Level Set, and Genetic and Evolutionary Feature Extraction, *IET Biometrics*, Vol. 4, No. 3, pp 151-161, September, 2015.

[34] T. Nguyen, Y. Wang, Y. Ha, R. Li, Performance and Security-Enhanced Fuzzy Vault Scheme Based on Ridge Features for Distorted Fingerprints, *IET Biometrics*, Vol. 4, No. 1, pp. 29-39, March, 2015.

[35] C. Rathgeb, F. Breitinger, C. Busch, H. Baier, On Application of Bloom Filters to Iris Biometrics, *IET Biometrics*, Vol. 3, No. 4, pp. 207-218, December, 2014.

[36] C. Sousedik, C. Busch, Presentation Attack Detection Methods for fingerprint recognition systems: a survey, *IET Biometrics*, Vol. 3, No. 4, pp. 219-233, December, 2014.

[37] Y. Imamverdiyev, A. Teoh, J. Kim, Biometric Cryptosystem Based on Discretized Fingerprint Texture Descriptors, *Expert Systems with Applications*, Vol. 40, No. 5, pp. 1888-1901, April, 2013.

[38] A. K. Jain, A. Ross, U. Uludag, Biometric Template Security: Challenges and Solutions, *13th European Signal Processing Conference*, Antalya, Turkey, 2005, pp. 1-4.

[39] P. Polash, M. Paul, M. Gavrilova, Cancelable Biometrics: Securing Face Template, *International Journal on Artificial Intelligence Tool*, Vol. 4, No.1, pp. 25-34, June, 2012.

[40] V. M. Patel, N. K. Ratha, R. Chellappa, Cancelable Biometrics: A Review, *IEEE Signal Processing Magazine*, Vol. 32, No. 5, pp. 54-65, September, 2015.

[41] U. Uludag, S. Pankanti, S. Prabhakar, A. Jain, Biometric Cryptosystems: Issues and Challenges, *Proceedings of the IEEE*, Vol. 92, No. 6, pp. 948-960, June, 2004.

[42] L. M. Dinca, G. P. Hancke, The Fall of One, the Rise of Many: A Survey on Multi-Biometric Fusion Methods, *IEEE Access*, Vol. 5, pp. 6247-6289, April, 2017.

[43] G. Karimovich, K. Turakulovich, Biometric Cryptosystems: Open Issues and Challenges, *International Conference on Information Science and Communications Technologies*, Tashkent, Uzbekistan, 2016, pp. 1-3.

[44] A. Jain, A. Nandakumar, K. Ross, 50 Years of Biometric Research: Accomplishments, Challenges, and Opportunities, *Pattern Recognition Letters*, Vol. 79, pp. 80-105, August, 2016.

[45] P. Lacharme, Revisiting the Accuracy of the Biohashing Algorithm on Fingerprints, *IET Biometrics*, Vol. 2, No. 3, pp. 130-133, September, 2013.

[46] R. Belguechi, E. Cherrier, C. Rosenberger, S. Ait-Aoudia, Operational Bio-Hash to Preserve Privacy of Fingerprint Minutiae Templates, *IET Biometrics*, Vol. 2, No. 2, pp. 76-84, June, 2013.

[47] Z. Jin, A. Teoh, B. Goi, Y. Tay, Biometric Cryptosystems: A New Biometric Key Binding and Its Implementation for Fingerprint Minutiae-Based Representation, *Pattern Recognition*, Vol. 56, pp. 50-62, August, 2016.

[48] J. Bringer, C. Morel, C. Rathgeb, Security Analysis and Improvement of Some Biometric Protected Templates based on Bloom Filters, *Image and Vision Computing*, Vol. 58, pp. 239-253, February, 2017.

[49] D. Sadhya, S. Singh, Providing Robust Security Measures to Bloom Filter Based Biometric Template Protection Schemes, *Computers & Security*, Vol. 67, pp. 59-72, June, 2017.

[50] S. Adamovic, M. Milosavljevic, M. Veinovic, M. Sarac, A. Jevremovic, Fuzzy Commitment Scheme for Generation of Cryptographic Keys Based on Iris Biometrics, *IET Biometrics*, Vol. 6, No. 2, pp. 89-96, March, 2017.

[51] C. Soutar, D. Roberge, A. Stoianov, R. Gilroy, B. Vijaya Kumar, Biometric Encryption: Enrollment and Verification Procedures, *Proceedings SPIE*, Vol. 3386, pp. 24-35, March, 1998.

[52] P. Ramasamy, V. Ranganathan, S. Kadry, R. Damaševičius, T. Blažauskas, An Image Encryption Scheme Based on Block Scrambling, Modified Zigzag Transformation and Key Generation Using Enhanced Logistic: Tent Map, *Entropy*, Vol. 21, No. 7, 656, July, 2019.

[53] C. Soutar, D. Roberge, A. Stoianov, R. Gilroy, B. Vijaya Kumar, Biometric Encryption, *ICSA Guide to Cryptography*, McGraw-Hill, 1999.

[54] L. Jean-Paul, P. Tuyls, New Shielding Functions to Enhance Privacy and Prevent Misuse of Biometric Templates, *4th International Conference on Audio- And Video-Based Biometric Person Authentication*, Guildford, UK, 2003, pp. 393-402.

[55] P. Tuyls, A. H. M. Akkermans, T. A. M. Kevenaar, G. J. Schrijen, A. M. Bazen, R. N. J. Veldhuis, Practical Biometric Authentication with Template Protection, *International Conference on Audio- and Video-Based Biometric Person Authentication*, Hilton Rye Town, NY, USA, 2005, pp. 436-446.

[56] H. Li, M. Wang, L. Pang, W. Zhang, Key Binding Based on Biometric Shielding Functions, *Fifth International Conference on Information Assurance and Security*, Xi'an, China, 2009, pp. 19-22.

[57] Z. Wu, L. Tian, P. Li, T. Wu, M. Jiang, C. Wu, Generating Stable Biometric Keys for Flexible Cloud Computing Authentication using Finger Vein, *Information Sciences*, Vol. 433-434, pp. 431-447, April, 2018.

[58] K. Ankit, J. Rekha, Biometrics as a Cryptographic Method for

Network Security, *Indian Journal of Science and Technology*, Vol. 9, No. 22, pp. 1-6, June, 2016.

[59] S. Hoque, M. Fairhurst, G. Howells, Evaluating Biometric Encryption Key Generation using Handwritten Signatures, *2008 Bio-inspired, Learning and Intelligent Systems for Security*, Edinburgh, UK, 2008, pp. 17-22.

[60] Y. Sutcu, H. T. Sencar, N. Memon, A Secure Biometric Authentication Scheme Based on Robust hashing, *MM&Sec'05: Proceedings of the 7th Workshop on Multimedia and Security*, New York, NY, USA, 2005, pp. 111-116.

[61] Q. Li, M. Guo, E.-C. Chang, Fuzzy Extractors for Asymmetric Biometric Representations, *IEEE Workshop on Biometrics (In association with CVPR)*, Anchorage, AK, USA, 2008, pp. 1-6.

[62] Q. Li, E.-C. Chang, Robust, Short and Sensitive Authentication Tags Using Secure Sketch, *MM&Sec '06: Proceedings of the 8th workshop on Multimedia and security*, Geneva, Switzerland, 2006, pp. 56-61.

[63] C. Rathgeb, A. Uhl, An Iris-based Interval-mapping Scheme for Biometric Key Generation, *6th International Symposium on Image and Signal Processing and Analysis (ISPA)*, Salzburg, Austria, 2009, pp. 511-516.

[64] C. Rathgeb, A. Uhl, Privacy Preserving Key Generation for Iris Biometrics, *11th Joint IFIP TC6 and TC11 Conference on Communications and Multimedia Security (CMS 2010)*, Linz, Austria, 2010, pp. 191-200.

[65] A. Baig, A. Bouridane, F. Kurugollu, B. Albesher, Cascaded Multimodal Biometric Recognition Framework, *IET Biometrics*, Vol. 3, No. 1, pp. 16-28, March, 2014.

[66] A. Lumini, L. Nanni, Overview of the Combination of Biometric Matchers, *Information Fusion*, Vol. 33, pp. 71-85, January, 2017.

[67] S. Veluchamy, L. Karlmarx, System For Multimodal Biometric Recognition Based on Finger Knuckle and Finger Vein Using Feature-Level Fusion and K-Support Vector Machine Classifier, *IET Biometrics*, Vol. 6, No. 3, pp. 232-242, May, 2017.

[68] D. Jagadiswary, D. Saraswady, Biometric Authentication Using Fused Multimodal Biometric, *Procedia Computer Science*, Vol. 85, pp. 109-116, 2016.

[69] H. Mehrotra, R. Singh, M. Vatsa, B. Majhi, Incremental Granular Relevance Vector Machine: A Case Study in Multimodal Biometrics, *Pattern Recognition*, Vol. 56, pp. 63-76, August, 2016.

[70] D. Sadhya, S. Singh, Privacy Preservation for Soft Biometrics Based Multimodal Recognition System, *Computers & Security*, Vol. 58, pp. 160-179, May, 2016.

[71] V. Thasiyabi, R. Koshy, S. Satheesh, Biometric Fusion: Combining Multimodal and Multi Algorithmic Approach, *International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES)*, Paralakhemundi, India, 2016, pp. 618-620.

[72] G. Amirthalingam, G. Radhamani, New Chaff Point Based Fuzzy Vault for Multimodal Biometric Cryptosystem Using Particle Swarm Optimization, *Journal of King Saud University - Computer and Information Sciences*, Vol. 28, No. 4, pp. 381-394, October, 2016.

[73] A. Meraoumia, S. Chitroub, A. Bouridane, Fusion of Finger-Knuckle-Print and Palmprint for an Efficient Multi-Biometric System of Person Recognition, *2011 IEEE International Conference on Communications (ICC)*, Kyoto, Japan, 2011, pp. 1-5.

[74] E. Lim, K. A. Toh, P. Suganthan, X. Jiang, W. Y. Yau, Fingerprint Image Quality Analysis, *International Conference on Image Processing (ICIP)*, Singapore, 2004, pp. 1241-1244.

[75] M. Olsen, H. Xu, C. Busch, Gabor Filters as Candidate Quality Measure for NFIQ 2.0, *IAPR International Conference on Biometrics (ICB)*, New Delhi, India, 2012, pp. 158-163.

[76] L. Shen, A. Kot, W. Koo, Quality Measures of Fingerprint Images, in: J. Bigun, F. Smeraldi (Eds.), *Audio- and Video-Based Biometric Person Authentication, AVBPA 2001, Lecture Notes in Computer Science*, Springer, Berlin, Heidelberg, 2001, pp. 266-271.

[77] T. P. Chen, X. Jiang, W. Y. Yau, Fingerprint Image Quality Analysis, *International Conference on Image Processing*, Singapore, 2004, pp. 1253-1256.

[78] E. Lim, X. Jiang, W. Yau, Fingerprint Quality and Validity Analysis, *International Conference on Image Processing*, Rochester, NY, USA, 2002, pp. 1-4.

[79] Y. Chen, S. Dass, A. Jain, Fingerprint Quality Indices for Predicting Authentication Performance, in: T. Kanade, A. Jain, N. K. Ratha (Eds.), *Audio- and Video-Based Biometric Person Authentication, AVBPA 2005, Lecture Notes in Computer Science*, Springer, Berlin, Heidelberg, 2005, pp. 160-170.

[80] A. Hilal, P. Beauseroy, B. Daya, Elastic Strips Normalisation Model for Higher Iris Recognition Performance, *IET Biometrics*, Vol. 3, No. 4, pp. 190-197, December, 2014.

[81] Z. Yao, J. Le Bars, C. Charrier, C. Rosenberger, Literature Review Of Fingerprint Quality Assessment and Its Evaluation, *IET Biometrics*, Vol. 5, No. 3, pp. 243-251, September, 2016.

[82] C. Rathgeb, A. Pflug, J. Wagner, C. Busch, Effects of Image Compression on Ear Biometrics, *IET Biometrics*, Vol. 5, No. 3, pp. 252-261, September, 2016.

[83] O. Iloanusi, Effective Statistical-based and Dynamic Fingerprint Preprocessing Technique, *IET Biometrics*, Vol. 6, No. 1, pp. 9-18, January, 2017.

[84] B. Fernandez-Saavedra, R. Sanchez-Reillo, R. Ros-Gomez, J. Liu-Jimenez, Small Fingerprint Scanners Used in Mobile Devices: The Impact on Biometric Performance, *IET Biometrics*, Vol. 5, No. 1, pp. 28-36, March, 2016.

[85] A. Ross, R. Govindarajan, Feature Level Fusion of Hand and Face Biometrics, *Proceedings of the SPIE*, Vol. 5779, pp. 196-205, March, 2005.

[86] P. Yan, K. Bowyer, Biometric Recognition Using 3D Ear Shape, *IEEE Transactions on Pattern Analysis and Machine Intelligence*, Vol. 29, No. 8, pp. 1297-1308, August, 2007.

[87] A. Kumar, A. Passi, Comparison and Combination of Iris Matchers for Reliable Personal Authentication, *Pattern Recognition*, Vol. 43, No. 3, pp. 1016-1026, March, 2010.

[88] D. Zhang, G. Lu, L. Zhang, Local Features for Finger-Knuckle-Print Recognition, *Advanced Biometrics*, Springer, Cham, 2018, pp. 111-130.

[89] F. Silva Teodoro, S. Peres, C. Lima, Feature Selection for Biometric Recognition Based on Electrocardiogram Signals, *International Joint Conference on Neural Networks*, Anchorage, AK, USA, 2017, pp. 2911-2920.

[90] M. Gomez-Barrero, C. Rathgeb, G. Li, R. Ramachandra, J. Galbally, C. Busch, Multi-biometric Template Protection Based on Bloom Filters, *Information Fusion*, Vol. 42, pp. 37-50, July, 2018.

[91] T. A. T. Nguyen, T. K. Dang, D. T. Nguyen, A New Biometric Template Protection Using Random Orthonormal Projection and Fuzzy Commitment, *CoRR Journal*, pp. 1-11, April, 2019.

Biographies

P Jayapriya completed B.Sc., (CS), M.C.A. and M.E. Computer science (2016) and doing full time research in Department of Information Technology at PSG College of Technology, Coimbatore, Tamilnadu. She has 10 years teaching as teaching experience. She is a member of Indian Society for Technical Education. She presented paper in more than 15 national international conferences and two Scopus indexed journal. Her area of research are image processing, pattern recognition, and biometrics.

R. R. Manimegalai (M.E., Ph.D.) is presently working as a Professor and Head, Department of Computer Science and Engineering, PSG Institute of Technology and Applied Research, Coimbatore, India. She has published many papers in international/national journals and conferences. Her area of interest includes experience Security in Distributed Embedded and IoT Designs, FPGA/VLSI Algorithms and Testing, Image Processing. She has to her credit 22 years of teaching, research and industry.

R. Lakshmana Kumar is currently leading the technical team in Hindusthan College of Engineering and Technology, Coimbatore. Tamil Nadu. He is a Chief Research Scientist in a Canadian based startup in British Columbia. He has published many papers in international journals and conferences. His area of interest includes Artificial Intellligence and Blokchain. He holds the certification in Data Science from John Hopkins University, United States. He is a member in IEEE.

Seifedine Kadry has a Bachelor degree in 1999 from Lebanese University, MS degree in 2002 from Reims University (France) and EPFL (Lausanne), Ph.D. in 2007 from Blaise Pascal University (France), HDR degree in 2017 from Rouen University. At present his research focuses on Data Science, education using technology, system prognostics, stochastic systems, and probability and reliability analysis. He is an ABET program evaluator for computing, and ABET program evaluator for Engineering Tech.

Sanghyun Seo received his B.S. degrees in Computer Science and Engineering from Chung-Ang University, Seoul, Korea, in 1998 and M.S. and Ph.D. degrees in GSAIM Dep at Chung-Ang University, Seoul, Korea, in 2000 and 2010.He was the postdoctoral researcher at Chung-Ang University, in 2010, and the postdoctoral researcher at LIRIS Lab, Lyon 1 University from February 2011 to February 2013. He had worked at the ETRI (Electronics and Telecommunications Research Institute), DaeJeon, Korea, May 2013 to February 2016. He had worked at the Sungkyul University from March 2016 to February 2019. He is currently a faculty of College of Art and Technology at Chung-Ang University. His research interests are in the area of computer graphics, non-photorealistic rendering and animation, real-time rendering using GPU, VR/AR, Image processing, Computer vision and game technology.