State of the Art in Biometric Key Binding and Key Generation Schemes

Abayomi Jegede[1,2], Nur Izura Udzir[1], Azizol Abdullah[1], Ramlan Mahmod[1]

[1]Faculty of Computer Science and Information Technology, Universiti Putra Malaysia

[2]Department of Computer Science, University of Jos, Nigeria.

Abstract**:** Direct storage of biometric templates in databases exposes the authentication system and legitimate users to numerous security and privacy challenges. Biometric cryptosystems or template protection schemes are used to overcome the security and privacy challenges associated with the use of biometrics as a means of authentication. This paper presents a review of previous works in biometric key binding and key generation schemes. The review focuses on key binding techniques such as biometric encryption, fuzzy commitment scheme, fuzzy vault and shielding function. Two categories of key generation schemes considered are private template and quantization schemes. The paper also discusses the modes of operations, strengths and weaknesses of various kinds of key-based template protection schemes. The goal is to provide the reader with a clear understanding of the current and emerging trends in key-based biometric cryptosystems.

Keywords**:** authentication, biometric, security, privacy

1. Introduction

Biometrics is a compound word derived from 'bio', which means living or life and 'metrics', which refers to a method of measuring something or results obtained from such measurement. The term generally refers to the various technologies which use mathematical and statistical theories and methods to measure the biological characteristics of the human body. The measurable characteristics are broadly divided into two broad categories, namely: physiological characteristics and behavioural characteristics. Physiological characteristics such as fingerprints, face, iris, DNA, retina, palmprint, ear, lip, knuckle texture, skin spectroscopy, and palm bio-impedance spectroscopy are acquired directly from the bodies of the users. They are always available to the owner and are difficult to lose. Behavioural characteristics, on the other hand, describe how the owner behaves, acts or does things. These are not permanent and could suffer variations over a period of time. Examples of behavioural characteristics are keystroke dynamics, signature patterns, typing behaviour, syslometry, behavioural profiling and linguistic profiling. The taxonomy diagram in Figure 1 illustrates the categorization of biometric characteristics as well as the examples for each category. Practical applications of biometrics include border control; access control to sensitive government installations; racial classification; citizenship verification; monitoring attendance in schools and offices; cardless Automatic Teller Machines (ATMs); access to computer systems and networks; online banking; electronic trading; and payment processing systems.

Biometric systems can be classified as either unibiometric or multibiometric depending on the number of biological traits required for enrolment and authentication. Unimodal or unibiometric systems are based on a single biometric trait, for example, face, iris, fingerprint or retina. Unimodal systems are unisensor in their operation. That is, they use one sensor for image acquisition and verification. A multibiometric system may be multimodal, multi-sensor, multi-instance or multi-algorithmic. Multimodal systems use more than one physiological or traits for enrolment, verification and identification. Multi-sensor systems use different sensors to capture the images of different modalities during the enrolment and verification phases. An illustration is the use of camera and fingerprint scanner to acquire face image and fingerprint pattern respectively.

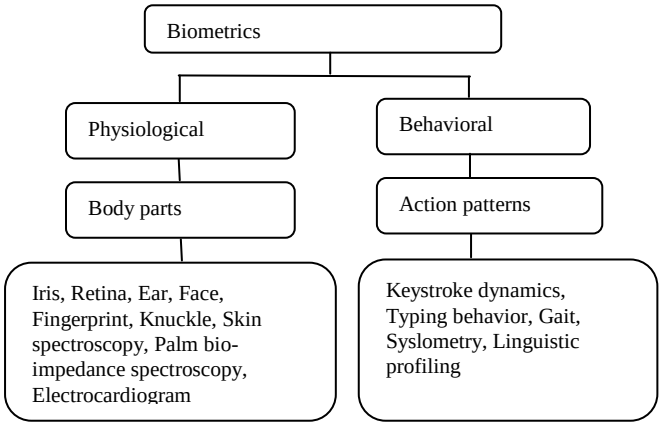

Figure 1. Taxonomy of biometrics

Multi-instance approaches combine two or more instances of the same biometric modality during enrolment and authentication. An example is the combination of multiple instances of the same fingerprint, face or iris. Multi-algorithmic (or hybrid) use a combination of two or more algorithms to carry out the enrolment and authentication processes. Multibiometric systems combine inputs from multiple sources into a single unit by a process known as fusion. Fusion can take place at the sensor level, feature level, matching score level, decisions level. Sensor or image level fusion combines raw samples of biometric data. Feature level fusion creates a composite feature vector by extracting and combining relevant and discriminant features from the original images. Feature level fusion faces challenges such as incompatibility of biometric vectors, dimensionality problems and difficulty of designing a matching algorithm for feature level matching [1]. Matching score level fusion combines the matching scores of each subsystem of the multibiometric system using techniques such as the weighted sum rule, weighted product, linear discriminant, decision tree, and the Bayesian rule. Decision level fusion uses techniques such a AND rule, OR rule and majority voting to perform fusion. Multibiometric systems face two major

challenges, namely: template security and fusion complexity [2]. Table 1 presents a comparison between unimodal and multimodal biometric systems using parameters such as cost of implementation, user convenience, performance, security, flexibility and complexity.

Table 1. Comparison between unimodal and multimodal biometric systems

Parameters	Unimodal		Multimodal	
	Low	High	Low	High
Cost	✓			✓
Convenience		✓	✓	
Recognition accuracy	✓			✓
Security	✓			✓
Flexibility	✓			✓
Complexity	✓			✓

The taxonomy diagram in Figure 2 highlights the categories, advantages and challenges of biometric systems. It also presents issues such as fusion methods, fusion complexity and template security as they relate to multibiometric systems.

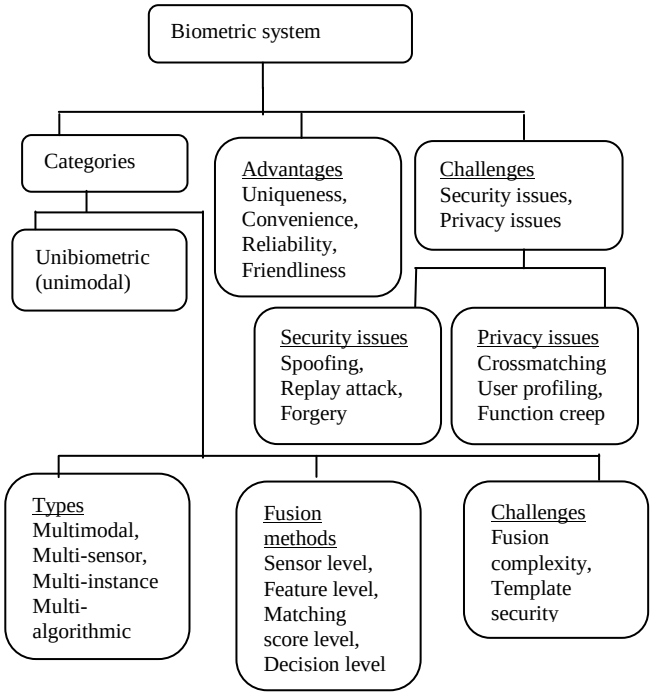

Figure 2. Taxonomy of biometric system

Biometric authentication systems use the unique and measurable biological features to verify the identity of users. Biometrics derives its strength from the uniqueness of these features and the relative difficulty with which they may be forged. Biometric authentication schemes provide a strong, secure, reliable and convenient means of access to a computer installation or physical environment. These systems verify users based on their actual identity and not what they know or possess. Although a biometric is secure in the sense that it cannot easily be copied, forged, or stolen, yet we cannot consider it to be secret. Biometric data can be disclosed without the knowledge or cooperation of the owner. For example, fingerprints can be obtained from door handles and elevator buttons. Pictures of faces, iris and retina can be captured using surveillance cameras. Attacks against stored biometric data expose the authentication system and enrolled users to numerous security and privacy threats.

The taxonomy diagram in Figure 3 illustrates the classification, purpose, basic requirements and applications of key-based biometric cryptosystems. It also shows the potential attacks that can be launched against key-based schemes.

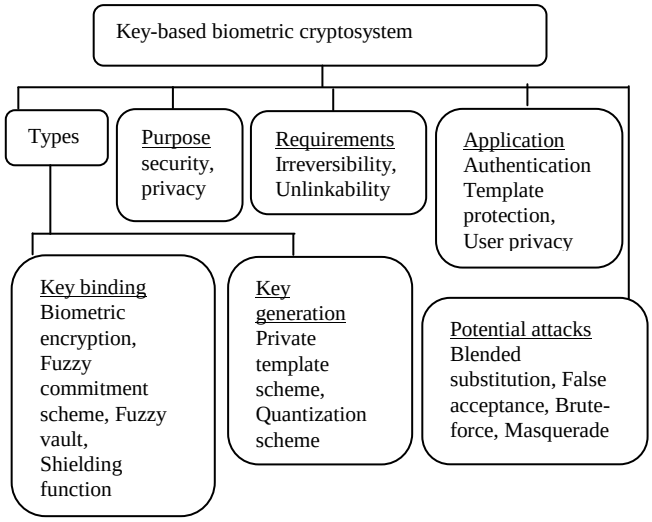

Figure 3. Taxonomy of key-based biometric cryptosystem

Biometric cryptosystems or template protection schemes are based on the integration of techniques from the domain of cryptography and biometrics. In contrast to conventional biometric recognition systems, template protection schemes do not store biometric data directly in the database. Rather, they associate secret information with a biometric data before it is stored. This makes it difficult for an intruder to obtain the original biometric data without knowing the secret information used to secure it. Template protection systems make it possible to revoke, update or replace biometric data in the event of loss or data corruption. A good template protection scheme should meet the following criteria: diversity, revocability, security and performance [3]. Template security is achieved by combining secret information with the biometric data before storage instead of storing the biometric data directly in the database. This makes it computationally hard for an attacker to obtain the original biometric data from the secure template without having knowledge of the secret information. Template protection schemes provide diversity by using different secret information and/or algorithms to create multiple versions of secure template from a single biometric data. Diversity minimizes the correlation among secure templates of the same subject which are stored in different databases. This prevents cross matching attack and guarantees user's privacy. Revocability allows biometric database administrators to replace or update templates in case of loss or compromise. This is because multiple copies of a protected template can be obtained from an instance of biometric data. It is also required that the biometric template protection scheme maintain a good balance between security and performance. In order words, the provision of template protection should not lead to a significant degradation in the recognition accuracy of a biometric system. Key-based template

protection schemes are classified as either key binding or key generation depending on the mode of operation or the method used to secure templates [4]. Table 2 presents a comparison between key binding and key generation schemes.

2. Key Binding Schemes

These schemes use 'binding' techniques to create a secure template from an input containing a secret key and biometric data. The binding process is carried out using well-known or publicly available cryptographic algorithms [4]. The secrecy of the key and the complexity of the key binding algorithm are the major factors which determine the security of the stored biometric data. This section discusses key binding schemes such as biometric encryption, fuzzy commitment scheme, fuzzy vault and shielding functions.

2.1. Biometric Encryption

Biometric encryption or bio-cryptography is a direct application of standard cryptographic algorithms to generate secure biometric templates.

Table 2. Comparison between key binding and key generation schemes

Approach	Mode of operation	Strengths	Weaknesses
Key binding	Secures a biometric data by binding it with secret key. An update of the key requires a re-enrolment in order to generate a new helper data.	i) A protected data cannot be retrieved without the knowledge of the secret key. ii) Guarantees user privacy as cryptographic keys are independent of biometric data.	An attacker who knows the secret key can recover original biometric data from protected template.
Key generation	i) Generates a key directly from extracted biometric features. ii) Derives a helper data from a biometric template and generates a key from the helper data and a given biometric sample. The store helper data is used to update a key that is suspected to have been compromised.	i) Provides security and privacy by eliminating direct storage of biometric data. ii) Difficult for attackers to reconstruct original biometric data from key string since biometric data are not retained after enrolment.	i) Key generation schemes which do not store helper data cannot provide revocable (updateable) keys. ii)Helper data based key generation schemes which use helper data are vulnerable to attack via record multiplicity

Mytec1 [5] was the first implementation of bio-cryptographic scheme. Later, Mytec2 [6] was developed to provide a more sophisticated protection for stored fingerprint template. The inability of Mytec2 to provide satisfactory security and recognition accuracy made it impossible for it to be deployed in practical scenarios [3]. A biometric encryption method based on elliptic curve cryptography has been proposed for secure biometric authentication in smart device ecosystems [7]. The approach offers a good balance between performance and security by providing a 25% latency reduction over a vanilla elliptic curve cryptography (ECC) system and a 5% lower average load. The proposed OTA protocol and biometric-aided scheme has 15% latency reduction and a 35% net reduction in latency respectively.
Elliptic curve cryptography was also used to implement biometric key agreement scheme in wireless sensor networks (WSN) [8]. This technique is suitable for low-power sensor network environments because it minimizes the computational costs between the sensor node and the GW-node. The use of ECC to provide secure session key agreement reduces the total execution time and memory requirement. It also provides security against well-known cryptographic attacks because it uses only hash function and does not require a user password. Results of security and performance analysis show that the proposed scheme provides secure, reliable and efficient WSNs. A recent proposal combined Bernoulli-logistic mapping and chaotic encryption techniques to create a secure bio-cryptographic scheme [9]. This approach is suitable for online based biometric data network encryption and information transmission. Experimental result shows that proposed technique has better correlation distribution and histogram. Security analysis demonstrates that the absolute coefficients sum (ASC) and volatility of the proposed algorithm is comparatively lower than that of logistic map. This provides high security with mixture and secrecy of the encryption scheme. Correlation analysis show that the correlation distribution of the encrypted data is fairly more uniform when combined with diffusion and mixture than that provided by logistic chaotic method. Overall, the proposed approach provides efficient performance and security. A hybrid approach to biometric encryption based on the integration of packed homomorphic encryption and ideal lattices techniques has also been proposed [10]. The protocol has shorter ciphertext and is 100 times faster than previous approaches based on homomorphic encryption. Approaches based on biometric encryption are susceptible to blended substitution attack [5], hill climbing attack [11] and nearest impostor attack [12]. Moreover, an attacker can use reconstructed secret to retrieve original biometric data from secured templates [13].

2.2. Fuzzy Commitment Scheme

A fuzzy commitment scheme [14] is a cryptographic algorithm which secures stored biometric data using cryptography and error correcting code techniques. The algorithm binds secret information with a data in order to conceal the data and prevent the owner of the data from revealing it in more than one way. Fuzzy commitment schemes have been used to secure biometric templates obtained from face, fingerprints and iris [15, 16, 17]. The approach in [15] has false rejection rate (FRR), false acceptance rate (FAR) and key length of 0.47%, 0% and 140 bits respectively. The method in [16] uses fingerprint to

generate random keys which are resistant to dictionary attack. Experimental result shows an average of 50% increase in randomness of the generated keys which provides strong resistance against brute-force attack. In [17], the proposed technique applies error correction more effectively and provides a more balanced distribution of reliability and improved recognition rates. Experimental results also reveal significant improvement in key retrieval rates. Iris fuzzy commitment schemes are reliable because their performance is not easily affected by signal degradation caused by noise and blur in iris images [18]. Image compression also has little effect on the recognition accuracy of fuzzy commitment scheme [19, 20]. Multi-factor authentication scheme based on the integration of iris-based fuzzy commitment scheme and smart card technology has been proposed [21]. The goal is to provide a simple, secure, privacy-preserving and revocable approach to template protection. However, the authors did not provide any mathematical or experimental verification of its feasibility or performance. A novel application used the fuzzy commitment for secure key management in body sensor networks (BSNs) [22]. The approach uses energy-based multihoproute-choice and biometrics synchronization mechanism (based on weak time synchronization) to provide a balance in energy used by routes and reduce the energy consumption for transmission. Experimental results show that the proposed scheme can be used to enhance the efficiency and security of BSNs. Enhanced versions of the fuzzy commitment scheme are based on dynamic use of multiple commitments [23] and the derivation of multiple commitments from a single commitment [24]. Security analysis show that these approaches provide improved security for stored biometric data because an attacker will need to compromise multiple encrypted templates and secret key before he can retrieve a secured biometric data. Other techniques aimed to achieve an adaptive approach for effective error correction [25], reliability-balancing [17] or the integration of fuzzy commitment scheme with McEliece's cipher [26]. Experimental results and security analysis reveal that these enhancements provide improved recognition and/or security of stored biometric data. A more secure version of the fuzzy commitment scheme derive a next commitment from the combination of the authenticated input and a current commitment [27]. The authors also proposed the alpha and beta smoothing methods. Experimental results show that the scheme achieves the highest rate of authentication when it uses optimal value of the beta smoothing method. An improved approach combined the fuzzy commitment scheme with biometric hashing to enhance the security stored images [28]. Biometric hashing was first applied to biometric images before securing the hashed images with the fuzzy commitment scheme. This method addresses security problem caused by poor diffusion in generic robust image hashing algorithms. Another enhanced implementation addressed the effects of uncertainty and errors in noisy channels by injecting the fuzziness property into fuzzy commitment scheme [29]. It also provides a more secure binding than the generic fuzzy commitment scheme. A modified version of the generic fuzzy commitment scheme used Gaussian technique to generate uniformly distributed data [30]. This is approach is simpler than the generic fuzzy commitment scheme as it eliminates the need for binary quantization of biometric data. In [31], the authors proposed an enhanced iris fuzzy commitment scheme which has low complexity of implementation and good recognition accuracy (FRR and FAR of 3.75% and 0% respectively). Its keys also have long dimension (400 bits) and high entropy. A comparison of key distribution schemes shows that fuzzy commitment scheme and fuzzy vault use simple processes for enrolment and authentication [32]. The application of both approaches on ECG data shows that fuzzy commitment scheme uses a more complicate process to extract ECG data and has lower FAR. It also shows that fuzzy commitment scheme and fuzzy vault have similar FARs.

Security and performance analysis of the fuzzy commitment scheme revealed the relationship between the recognition accuracy of a fuzzy commitment scheme and the theoretical maximum key length in a Gaussian-model biometric source [33]. Theoretical analysis showed that fusion strategies have an impact on the security and recognition performance of multibiometric fuzzy commitment schemes [34]. It also showed that score-level and decision-level fusion methods provide a linear increase in privacy which makes them unsuitable for biometric cryptosystems. A major weakness of the fuzzy commitment scheme is its susceptibility to attacks in environments that involve trusted third party [28]. A theoretical analysis of security and privacy showed that fuzzy commitment schemes with maximum key size achieve optimal performance for the memoryless totally symmetric case [35]. It also revealed that fuzzy commitment schemes provide limited security for the secret key and biometric data in the general memoryless and stationary ergodic cases. Iris-based fuzzy commitment schemes do not offer sufficient robustness against illegal retrieval of cryptographic keys, which makes them to suffer statistically significant false acceptance rates [36]. Biometric templates protected using fuzzy commitment schemes do not exhibit sufficient diversity across multiple databases, which makes them susceptible to decodability attack and cross-matching. [37, 38]. Fuzzy commitment schemes are also susceptible to hill-climbing and brute force attacks [39, 40]. Attacks via record multiplicity can also be used to decode protected biometric data [41, 42]. A suggested solution is the integration of random bit-permutation into the operation of fuzzy commitment schemes [37]. Another solution involves the use of a perceptron-based continuous function to simplify and optimize direct discrimination in order to prevent collision among templates [43]. Decodability and cross matching attacks in fuzzy commitment scheme can also be prevented by using random permutation to create a reference template from multiple instances of biometric images [44]. Pedersen (or "issue-time") commitment has been proposed as a measure to address key leakage in fuzzy commitment scheme [45]. This approach provides high template protection and user privacy as both the secret and time of issue verified during authentication. Another strategy is based on the integration of the chaotic system [46] with the generic fuzzy commitment scheme to provide improved security [47].

2.3. Fuzzy Vault

A fuzzy vault [48] is created by using an unordered set of data to 'lock' a secret key vault. The vault can only be unlocked if there is another set of data which significantly overlaps with the original data. The generic fuzzy vault is

suitable for unordered feature sets (such as fingerprints) and does not suffer performance degradation due to missing or spurious feature elements in multiple acquisitions of the same biometric data [49]. Fuzzy vault has been widely used to protect stored templates in automatic fingerprint verification systems [50, 51]. The application of the approach in [50] on FVC 2001-DB2 database provides a genuine acceptance rate (GAR) and FAR of 97% and 0.24% respectively. Experimental results based on MSU-DB1 database show a GAR and FAR of 96.9% and 0.16% respectively. The fuzzy vault in [51] uses a new chaff point generation algorithm, which is 4.84 times faster than Clancy's algorithm and 41.86 faster than Khalil-Hani's algorithm. Results of experiments conducted using FVC2002-DB1A and FVC2002-DB2A fingerprint databases show equal error rate (EER) of 2.4% and 1.9%, respectively. Fuzzy vault has also been used to secure biometrics such as palm gesture features obtained from fingerprint position and velocity [52]. Multibiometric fuzzy vaults are based on features extracted from iris and retina [2], face, iris and fingerprint data [53] and left and right irises [54]. Experimental results and security analysis show that these approaches provide good recognition accuracy as well as high level template security and user privacy. Tams et al [55] proposed a multi-instance fuzzy vault based on multiple fingerprints instead of a single fingerprint image. This approach provides recognition accuracy (GAR of 97%), template security (61 bits) and resistance against offline attacks. A multi-factor authentication scheme used the fuzzy vault to secure fingerprints in smartcard-based systems [56]. The need for improved template security and user privacy led to the integration of the fuzzy vault approach with digital signature and zero-knowledge techniques [57] as well as Double Advanced Encryption Standard Algorithm [58]. The recognition accuracy of the fuzzy vault scheme can be improved by using Geometric hashing technique to provide auto-alignment of fingerprint features in multiple-control and compartmentalized fuzzy vault [59]. The method supports automatic alignment of features and is robust against correlation attack [60]. Results from experiments and security analysis show that the approach leads to improvement in recognition accuracy and security. The method could suffer significant drawback in terms of verification accuracy and security if the hash table becomes very large. Improved recognition performance and security can be achieved in palmprint fuzzy vault by using random chaff points which are difficult to distinguish from genuine points [61]. This method addresses intra-class variations effectively leading to an increase in recognition accuracy of the palmprint fuzzy vault. An improved approach used Euclidean distance method to overcome the effects of alignment and translation of fingerprint images [62]. This approach has good recognition accuracy (GAR of ~86.03% and FAR of ~0.39%) and does not require the alignment of reference and query templates during authentication. Recent works focus on the development of new methods of alignments for fingerprint-based fuzzy vaults [63] as well as the use of circle packing [64] and squares method [65] techniques to provide fast and less complex chaff-point generation. These approaches lead to a reduction in the amount of time required for enrolment and authentication. A similar work applied a novel noise generation technique on ridge features of fingerprint to provide invariance to geometric transformations [66]. This method provides has low FAR (0%) and high security (key space and entropy of 160 bits and ~42 bits respectively).

Fuzzy vault is susceptible to attack via record multiplicity (ARM) [4], brute force attack [67] and collusion attack [68]. The generic fuzzy vault scheme is also vulnerable to intrusion attacks, liaison attacks, combination attacks and injection attacks [61]. A major drawback of the generic fingerprint fuzzy vault scheme is that the key determines the number matching minutiae thereby increasing the amount of time required for coefficient reconstruction [69]. This problem was addressed by using multivariable linear function to create a fingerprint fuzzy vault scheme in which the number of matching-minutiae determines the number of variables required for coefficient reconstruction [69]. The security of the scheme was also improved by using the Lorenz chaotic system method to increase randomness of minutiae points. The method has high accuracy because the FAR is always zero. Cubic spline interpolation [70] is another method used to address the high computational overhead of coefficient reconstruction in fingerprint fuzzy vault. This approach has good recognition accuracy as indicated by experiments conducted using the HA-BJTU palmprint database which show FAR to be always zero. Passwords can be used to increase the security of the fuzzy vault and minimize collision among stored templates [71]. The integration of password with the fuzzy vault prevents cross matching attacks by increasing the discriminability among templates of the same subject stored in different databases. This approach is not fool-proof because brute force attack can be used to compromise the security of fuzzy vault and password. A more secure approach used a key generated from user-specific password to transform the biometric template [72]. An additional layer of protection is added by using digital signature to encrypt the vault. Results from theoretical analysis and experiments show that the FAR increases as the dimension of the biometric feature increases. Higher values of FRR are observed as the ratio of number of chaff points to the length of template increases. Other modifications of the generic fuzzy vault [73, 74, 75] provide improved recognition accuracy and security.

Theoretical and experimental analysis was used to identify some weaknesses in the design, properties and performance of the fuzzy vault and suitable solutions were proposed to address these limitations. In [76], the authors proposed an enhanced fuzzy vault which is resistant to brute-force and ARM attacks. This scheme has good recognition accuracy (FAR of between 0% and 0.87% and GAR of between 72.5% and 91%) and security (large key space of between 2^{112} and 2^{192}). False accept attacks in fuzzy vault was addressed by enrolling multiple fingers of the same user [77]. This approach provides high level user privacy and good recognition accuracy ($FAR < 10^{-4}$ and very low FRR). The construction of multiple vaults from an instance of biometric data is another strategy used to enhance the security of the generic fuzzy vault [78]. A successful verification requires a decoding of at least two of the vaults. Enhanced security is also provided in fuzzy vaults by storing the encryption key (lock) and the encrypted template in different servers [79]. This method provides better security and privacy as attackers will have to compromise both vaults before a protected

template can be decrypted. A novel approach known as multi-secret fuzzy vault used different secret to secure each biometric data [80]. This is an error tolerant and order tolerant technique which requires an attacker to compromise multiple secrets before he can gain access to multiple biometric data. The approach is more secure than the generic fuzzy vault which is based on a single key. The storage of minutia angles instead of the actual coordinates of the minutiae points minimizes the possibility of cross matching attack [81]. Applying this technique on multiple fingers provides resistance against angle-correlation attack. The integration of fuzzy vault with transform-based techniques [82, 83, 84, 85, 86] provides better security and privacy. The process is carried out by applying a transformation technique on biometric data before securing the transformed template with the fuzzy vault. This approach resistant to threats such as brute-force and cross matching attacks.

2.4. Shielding Function

Shielding function [87] or helper data scheme was developed to provide security for stored biometric data and guarantee the privacy of legitimate users. The approach enables the authentication system to verify a user's identity without having any knowledge of the user's biometrics. The delta-contracting and epsilon-revealing functions provide the bedrock for this scheme. The delta contracting (δ-contracting) function binds a secret with a biometric data and epsilon revealing (ε-revealing) function ensures that a protected template reveals only a small amount of information on the random secret or biometric data. The shielding function was used to protect binary templates extracted from fingerprint images using Gabor filter [88]. Results from experiment shows that this method has an EER of 4.2% and a key length of 40 bits. In a related work [89], Wavelet Fourier-Mellin Transform was used to extract features from fingerprint images before securing the acquired templates with the shielding function. This method achieved sufficient key entropy and reveals only a small amount of information about user biometrics. A previous work extracts real value vectors from preprocessed face images using Principal Component Analysis [90]. Quantization process is used to convert the real-value features into binary before binding them with a randomly generated secret. Experiment results show that the scheme has good recognition accuracy (0% FAR, FRR of 0.8529%) and security (maximum key length of 36 bits). 3D face images were used to implement a helper data scheme in order to achieve better recognition performance [91]. 3D face images generally contain a richer set of information than 2D face images. The approach provides good recognition accuracy and adequate protection for stored templates. A two-factor authentication scheme known as biometric epassport used the helper data technique to secure stored face templates [92]. Experimental results show that the approach has FAR of 0% and of 35% when applied to face images obtained from the FERET database. The application of the technique on Caltech database results in FAR and FRR of 0% and 3.5% respectively.

Shielding functions, like all other key binding approaches, are not resistant to spoofing attacks [4]. Previous implementations of the shielding function produce keys which are less than 50 bits. This falls short of the minimum requirement for biometric keys and exposes the schemes to brute force attacks [92]. They are also susceptible to attack via record multiplicity [4] and crossmatching attack [41]. Moreover, an attacker can use a reconstructed secret to obtain original biometric data from compromised helper data [13]. A comparison of different key binding techniques is presented in Table 3.

3. Key Generation Schemes

Biometric key generation schemes extract cryptographic key or hash directly from a given biometric data [93]. They are implemented either as secure sketches or fuzzy extractors. A user-specific key can be generated by combining a helper data (obtained from a given biometric template) and a given biometric sample [94]. The method used for key generation depends largely on the nature or structure of the biometric data. A helper data may be obtained from a given biometric reference data and stored in the form of an updateable key or hash value or user-specific keys may be extracted directly from a reference biometric data [95]. Most key generation schemes store helper data to allow for revocability of stolen or corrupted templates. The two major approaches used for biometric key generation are private template scheme and quantization scheme.

3.1. Private Template Schemes

Template protection schemes based on the biometric key generations have been implemented using modalities such as face [96] and fingerprints [97, 98]. The approach in [96] was deployed in multifactor authentication schemes to provide template security and user privacy for biometric data stored in chips or cards. The authors noted that security (measured in terms of entropy loss) and performance (expressed in terms of FAR and FRR) should also be taken into consideration when assessing a practical system template protection system. The study in [97] proposed a fingerprint alignment technique based on the focal point of high curvature regions. The application of the proposed system on FVC2002-DB1 and DB2 databases achieved a false non-match rate (FNMR) of 16.2% and 12.6% respectively. The false match rate (FMR) in both cases was zero.

The proposed approach in [98] generates multiple and cancellable cryptographic keys from a single fingerprint image. Experimental results and security analysis show that the method is simple and efficient. It also prevents the recovery of original biometric data from protected templates. A novel approach used scale-based parity code to generate continuous keys from free-text keystroke dynamics [99]. This is in contrast to most key generation approaches which are based on fixed form biometric input. The approach uses linear discriminant analysis (LDA) to extract the most stable and discriminant features from keystroke signals. A privacy-preserving protocol based on homomorphic encryption is used in conjunction with LDA to provide template updateability without compromising the security of stored biometric data and privacy of enrolled users. The application of this technique on biometric features of 486 users obtained using LDA revealed equal error rate of 5%. Extracting biometric features without the use of LDA showed an equal error rate of less than 7%. It is also possible to store biometric templates directly as secret keys or to first compute the hash of the templates and then store the hash values as a secret key [100, 101]. Empirical analysis shows that the

approach in [100] has an entropy of 173 bits. The large entropy ensures that the probability of collision among templates generated from different irises is about 1 in 10^{52}.

Table 3. Comparison of key binding techniques

Technique	Mode of operation	Strengths	Weaknesses
Biometric encryption	Applies standard cryptographic algorithm to generate secure biometric template.	Prevents an attacker from decrypting protected templates without the knowledge of the algorithm and cryptographic key.	(i) Possible to use reconstructed secret to retrieve original biometric data from secure template. (ii) Susceptible to blended substitution, hill-climbing and nearest impostor attacks.
Fuzzy commitment scheme	Uses cryptography and error correcting techniques to bind secret information to a biometric data.	The 'commitment' derived from the biometric data and secret key secures the biometric template. It also protects the secret key by storing only its hash value.	(i) Template security are user privacy are guaranteed once an attackers knows the protected template and secret key. (ii) Susceptible to ARM, hill climbing, brute force, decodability and crossmatching attacks.
Fuzzy vault	Uses an unordered set of biometric data to lock a secret key in a vault.	The vault cannot be decoded without a biometric data which closely overlaps with the original one.	(i) Susceptible to ARM, brute force and collusion attacks. (ii) Vulnerable to intrusion, liaison, combination and injection attacks.
Shielding function	Creates a secure template (helper data) from a random secret and biometric data.	The helper data and hash function secures biometric data and random secret respectively. Original biometric data cannot be recovered from secured template without the knowledge of the secret key.	(i) Short key length (ii) Possible to use reconstructed secret to retrieve original biometric data from compromised helper data. (iii) Susceptible to ARM, brute-force and crossmatching attacks.

The method in [101] generates similar 2048-bit templates from iris images of the same user. A limitation of these approaches is the possibility to reconstruct raw biometric data from compromised biometric hashes [102]. This challenge can be addressed by using strong hash algorithms such as MD-5 and SHA-512 to generate random keys from biometric data. The approach supports non-repudiation and is resistant to brute-force attack. This method is efficient for fingerprint key generation because it minimizes intra-class variation and does not require fingerprint alignment during authentication. A similar method compares only a fraction of the keys instead of the entire keys during authentication [103]. This method is simple, efficient, secure and less susceptible to intra-class variation.

3.2. Quantization Schemes

Quantization schemes generate biometric keys using helper data and binarized (or quantized) biometric features. A unique feature of quantization schemes is the ability to extract the same keys from multiple acquisitions of a biometric modality even when the images are captured using different sensors. Results from experiments using a fingerprint show that up to 40% of fingers generate the same cryptographic key even when different scanners were used to capture the fingerprint images of each finger [104]. A related work generates unique and dynamic keys from fingerprints of 97.25% users [105]. Quantization schemes may be implemented as a multi-modal system; that is, a unique key may be derived from the fusion of two or more biometric modalities. [106]. Experimental results based on the combination of ECG signals obtained from MIT-BIH database and speech signals from a speech database created for testing purposes showed that the proposed approach has FAR and FRR are 1.27% and 10.62% respectively. A weakness of helper-data-based quantization scheme is the possibility of recovering original biometric images from protected templates. It is possible for an attacker to obtain face feature vectors from protected templates and then reconstruct real face [107]. A context-based approach to biometric key generation produces revocable and long dimensional (70-bit, 140-bit and 280-bit) biometric keys from iris images [108]. This method also has good recognition accuracy with GAR of 84.26%, 95.52% and 94.68% for the respective key lengths. Biometric keys have also been generated from hand bone images and heart vascular visualizations [109]. This technique extracts and models linguistic features from these images as graph grammars. Security analysis shows that this method generates strong, random and revocable biometric keys. The application of semi-supervised data clustering on signature (a behavioral biometric) produced consistent and discriminative keys [110]. The generated keys are also resistant to brute force attack because they have long dimension keys and high entropy. Quantization schemes which use helper data are vulnerable to attack via record multiplicity [4]. This exposes the secure sketch strategy to security and privacy flaws when an impostor gains access to multiple versions of protected templates which are generated from the same biometric data [111]. Hence, there is need for a trade-off between minimizing the amount of useful information available to an attacker when systems are compromised and the prevention of attacks against systems that are assumed to be secure [112]. Table 4 presents a comparison of the two common key generation techniques.

4. Future Research Directions

Biometric authentication systems verify the identity of users by acquiring digital versions of biometric traits and comparing them with the reference templates stored in the

database. A successful authentication occurs when there is a match between a probe template and a reference template. The system does not have any idea whether the probe biometric image is acquired from a live subject or an artificial representation of his identity. Fake representations of identity can be carried out using stolen photographs or video streams which contain the face and eye images of legitimate users. An impostor can also use 3D artifacts such as face moulds, fingerprint moulds and fake eyeballs to fool the authentication system. Susceptibility to spoofing attack will enable an impostor to impersonate legitimate users and gain unauthorized access to the resources protected by the biometric system. Spoofed biometric representations can also be used to carry out authorized enrolment which undermines the integrity of the authentication system. The inability of a biometric system to detect fake representations may allow for repudiation. Repudiation makes it possible for an individual to deny transactions he actually performed, claiming that they are the results of attacks.

Table 4. Comparison key generation techniques

Technique	Mode of operation	Strengths	Weaknesses
Private template schemes	Extract user specific keys directly from reference biometric data.	Provides template security and user privacy as biometric data is not in the authentication system. The use of strong hash algorithms to generate random keys from biometric data provides non-repudiation and resistance to brute-force attack.	(i) Short keys - susceptible to exhaustive search or brute force attack. (ii) Keys are not updateable in case of compromise.
Quantization schemes	Generates biometric keys using helper data and quantized biometric features.	(i) Can extract the same keys from multiple instances of a biometric data. (ii) Provides security and privacy because it does not store user-specific information such as biometric data.	Vulnerable to attack via record multiplicity.

Future research efforts should consider the provision of anti-spoofing (or liveness detection) capabilities [113, 114] in biometric key-based cryptosystems. Integrating liveness detection in a biometric authentication system will prevent spoofing attack and repudiation. It will also enhance the security and integrity of the authentication system. The integration of device authentication in biometric cryptosystems will enhance the security of the authentication scheme and provide improved resistance against spoofing attacks. This is because such enhanced schemes will verify the identity of the users and the device (personal computer or mobile device) before access is granted. Thus, an impostor who gains access to only spoofed biometric data will also require the authenticity of his device to be verified.

Session hijacking allows impostors to gain access to the system by tricking or coercing authorized users. It is also possible for an unscrupulous user may also hand over his working session to an intruder. This makes it is imperative for biometric cryptosystems to provide mechanisms for repeated verification of a user's identity during an entire working session. Continuous authentication techniques [115, 116, 117, 118] will prevent session hijacking and improve the security of the biometric authentication system.

Most key binding schemes tend to have shorter key lengths, small key space and low key entropies. This makes them susceptible to attack via record multiplicity and brute-force attack. Such schemes do not provide the level of security and privacy capabilities required for practical applications. The integration of key-based techniques with cancelable biometrics [119] will satisfy the security and privacy requirements for real world applications.

Future research efforts should also consider the deployment of biometric cryptosystems for the protection of sensitive biometric data in Internet of Things (IoT) [120] systems and wireless body sensor networks [121]. This will provide adequate privacy for human components in these systems.

5. Conclusions

This paper discussed the benefits as well as the security and privacy risks associated with the use of biometrics as an authentication mechanism. It examined key-based biometric cryptosystems under two major categories, namely: key binding schemes and key generation schemes. The discussion focused on key binding techniques such as biometric encryption, fuzzy commitment scheme, fuzzy vault and shielding function. The two categories of key generation techniques discussed are private template schemes and quantization schemes. The paper highlighted the modes of operation, strengths and limitations of the various techniques. It also presented an up to date review of previous works in biometric key binding and key generation domains. This paper will provide current and intending researchers with an up to date knowledge of previous research works, current directions and open research issues in key-based biometric cryptosystems.

Acknowledgements

This material is based upon work supported by the Ministry of Higher Education Malaysia under Grant No. FRGS 08-01-15-1721FR.

References

[1] D. Karmakar and C.A. Murphy, "Generation of new points for training set and feature-level fusion in multimodal biometric identification," Springer Machine Vision and Applications, Vol. 25, No. 2, pp. 477-487, 2013.

[2] M.K. Geetika, "Multimodal-based fuzzy vault using iris, retina and fingervein," Fourth International Conference on Computing, Communications and Networking Technologies," Tiruchengode, India, pp. 1-5, 2013.

[3] D. Maltoni, D. Maio, A.K. Jain and S. Prabhakar, Handbook of fingerprint recognition, Berlin, Germany: Springer, 2005.

[4] C. Rathgeb, A. Uhl and P. Wild, Iris-biometrics: from segmentation to template security. S. Jajodia (ed.), Advances in Information Security, Springer, 2013.

[5] C. Soutar, G.J. Tomko and G.J. Schmidt, Fingerprint controlled public key cryptography system, US Patent 5541994, 1996.

[6] C. Soutar, D. Roberge, A. Stoianov, R. Gilroy and B.V. Kumar, "Biomteric encryption - enrolment and verification procedures," Proceedings of SPIE, Vol. 3386, pp. 24-35, 1998.

[7] M. Salas, "A secure framework for OTA smart device ecosystems using ECC and biometrics," Springer Communications in Computer and Information Science, Vol. 381, pp 204-381, 2013.

[8] E-J. Yoon, and K-E. Yoo, "A biometric based authenticated key agreement scheme using ECC for wireless sensor networks," International Conference on Management and Service Science, Gyeongju, Korea, pp. 699-705, 2014.

[9] C.Z. Liew, R. Shaw, L. Li, and Y. Yang, "Survey on biometric data security and chaotic encryption strategy with bernoulli mapping," 2014 International Conference on Medical Biometrics, Shenzhen, China, pp. 174-180, 2014.

[10] M. Yasuda, T. Shimoyama and J. Kogure, "Packed homomorphic encryption based on ideal lattices and its applications in biometrics," Springer Lecture Notes in Computer Science, Vol. 8128, pp. 55-74, 2013.

[11] A. Adler, "Vulnerabilities in biometric encryption systems," Springer Lecture Notes in Computer Science, vol. 3546, pp. 211-228, 2005.

[12] A. Stoianov, T. Kevenaar and M.V.D. Veen, "Security issues of biometric encryption," Toronto International Conference on Science and Technology for Humanity, Toronto, Canada, pp. 34–39, Sep. 2009.

[13] X. Boyen, "Reusable cryptographic fuzzy extractors," 11th ACM Conference on Computer and Communications Security, Washington, DC, USA, pp. 82-91, 2004.

[14] A. Juels and M. Wattenberg, "A fuzzy commitment scheme," 6th ACM Conference on Computer Communications and Security, Singapore, pp. 28-36, 1999.

[15] F. Hao, R. Anderson and J. Daugman, "Combining cryptography with biometrics effectively," IEEE Transactions on Computers, Vol. 55, No. 9, pp. 1081-1088, 2006.

[16] S.S.S. Priya and P. Kathigaikumar, "Mixed random 128 bit key using fingerprint features and binding key for AES algorithm," 2014 International Conference on Contemporary Computing and Informatics, Mysore, India, pp. 1226-1230, 2014.

[17] C. Rathgeb, A. Uhl and P. Wild, "Reliability-balanced feature level fusion for fuzzy commitment scheme," 2011 International Joint Conference on Biometrics, Washington, DC, USA, pp. 1-7, 2011.

[18] C. Rathgeb and A. Uhl, "Iris-biometric fuzzy commitment schemes under signal degradation," Springer Lecture Notes in Computer Science, Vol. 7340, pp. 217-225, 2012.

[19] C. Rathgeb, A. Uhl and P. Wild, "Iris-biometric fuzzy commitment schemes under image compression," Springer Lecture Notes in Computer Science, vol. 8259, pp. 374-381, 2013.

[20] K. Iida and H. Kiya, "Secure and robust identification based on fuzzy commitment scheme for JPEG image," 2016 IEEE International Symposium on Broadband Multimedia Systems and Broadcasting, pp. 1-5, Nara, Japan, 2016.

[21] A.A. Al-Saggaf, L. Ghouti and H.S. Acharya, "Biometric cryptosystem with renewable templates**,"** National Workshop on Information Assurance Research, Riyadh, Saudi Arabia, pp. 1-5, 2012.

[22] H. Zhao, J. Qin and J. Hu, "An energy efficient key management scheme for body sensor networks," IEEE Transactions on Parallel and Distributed Systems, Vol. 24, No. 11, 2202-2210, 2013.

[23] S. Choto and N. Premasathian, "A dynamic fuzzy commitment scheme using ARRSES forecasting," 7th International Conference for Internet Technology and Secured Transactions, London, UK, pp. 616-619, 2012.

[24] N. Premasathian, "A multiple fuzzy commitment scheme," 2013 International Conference on Computer Applications Technology, pp. 1-4, Munich, Germany, 2013.

[25] C. Rathgeb and A. Uhl, "Secure iris recognition based on local intensity variations," Springer Lecture Notes in Computer Science vol. 6112, pp. 266-275, 2010.

[26] D.B. Ojia and A. Sharma, "A fuzzy commitment scheme with Mceliece's cipher," Survey in Mathematics and Its Applications," Vol. 5, pp. 73-82, 2010.

[27] S. Choto and N. Premasathian, "A dynamic fuzzy commitment scheme using multiple commitments," 2012 Symposium on Communications and Information Technologies, Gold Coast, Australia, pp. 308-312, 2012.

[28] Z. Liu, Q. Li and X. Niu, "Improve the security of image robust hash using fuzzy commitment scheme," Springer Neural Computing and Applications, Vol. 23, No. 1, pp. 67-72, 2013.

[29] A. Al-Saggaf, "Crisp commitment scheme based on noisy channels," 2011 Saudi International Electronics, Communications and Photonics Conference, Riyadh, Saudi Arabia, pp. 1-4, 2011.

[30] A.J. Han Vinck, A. Jivanyan and J. Winzen, "Gaussian fuzzy commitment," 2014 International Symposium on Information Theory and its Applications, Melbourne, Australia, pp. 571-574, 2014.

[31] S. Adamovic, M. Milosavljevic, M. Veinovic, M. Saraic and A. Jevremovic, "Fuzzy commitment scheme for generation of cryptographic keys based on iris biometrics," IET Biometrics, Vol. 6, No. 2, pp. 89-96, 2017.

[32] G. Zheng, G. Fang, M.A. Orgun and R. Shankaran, "A comparison of key distribution schemes using fuzzy commitment and fuzzy vault within wireless body area networks," 2015 IEEE International Symposium on Personal, Indoor and Mobile Radio Communications - Services, Applications and Business, Hong Kong, pp. 2120-2125, 2015.

[33] E.J.C. Kelkboom, J. Breebaart, I. Buhan and R.N.J. Veldhuis, "Maximum key size and classification performance of fuzzy commitment for Gaussian modelled biometric sources," IEEE Transactions on Information Forensics and Security, Vol 7, No. 4, pp. 1225-1241, 2012.

[34] J. Merkle, T. Kavenaar, and U. Korte, "Multi-modal and multi-instance fusion for biometric cryptosystems," 2012 International Conference of the Biometrics Special Interest Group, Darmstadt, Germany, pp. 1-6, 2012.

[35] T. Ignateko and F.M.J. Willems, "Information leakage in fuzzy commitment schemes," IEEE Transactions on Information Security and Forensics, vol. 5, iss. 2, pp. 337-348. Jun. 2010.

[36] C. Rathgeb and A. Uhl, "Statistical attack against iris-biometric fuzzy commitment schemes," IEEE Conference on Computer Vision and Pattern Recognition Workshops, Colorado Springs, USA, pp. 23-30, 2011.

[37] E.J.C. Kelkboom, J. Breebaart, T.A.M. Kavenaar, I. Buhan and R.N.J. Veldhuis, "Preventing decodability attack based on cross-matching in a fuzzy commitment scheme," IEEE Transactions on Information Security and Forensics, Vol. 6, No. 1, pp. 107-121, 2011.

[38] C. Rathgeb and A. Uhl, "Statistical attack against fuzzy commitment Schemes," IET Biometrics, Vol. 1, No. 2, pp. 94-104, 2012.

[39] X. Zhou, A. Kuijper, R. Veldhuis and C. Busch, "Quantifying privacy and security of biometric fuzzy commitment," 2011 International Joint Conference on Biometrics, Washington, DC, USA, pp. 1-8, 2011.

[40] X. Zhou and C. Busch, "Measuring privacy and security of iris fuzzy commitment," 2012 International Carnahan Conference on Security Technology, Boston, Massachusetts, USA, pp. 168-173, 2012.

[41] I. Buhan, J. Guajardo and E. Kelkeboom, "Efficient strategy to play the indistinguashability game for fuzzy sketches," 2010 International Workshop on Information Forensics and Security, Seattle, WA, USA, pp. 1-6, 2010.

[42] K. Simoens, P. Tuyls and B. Preneel, "Privacy weaknesses in biometric sketches," 30th IEEE Symposium on Security and Privacy, California, USA, pp. 188-203, 2009..

[43] Y.C. Feng and P.C. Yuen, "Binary discriminant analysis for generating binary face template, IEEE Transactions on Information Forensics and Security, Vol. 7, No. 2, pp. 613-624, 2012.

[44] M. Favre, S. Picard, J. Bringer and H. Chabanne, "Balancing is the key: performing finger vein template protection using fuzzy commitment," 2015 International Conference on Information Systems Security and Privacy, Kolkata, India, pp. 1-8, 2015.

[45] D. Bissessar, C. Adams and D. Liu, "Using biometric key commitments to prevent unauthorized lending of cryptographic credentials," 2014 Twelfth Annual International Conference on

Privacy, Security and Trust, Toronto, ON, Canada, pp. 75-83, 2014.

[46] G. Chen, "Constructing a simple chaotic system with an arbitrary number of equilibrium points or an arbitrary number of scrolls," Springer Advances in Intelligent Systems and Computing, Vol. 210, pp. 1-6, 2013.

[47] N. Wang, Q. Li and A.A.A. El-Latif, "A novel protection scheme for multibiometrics based on fuzzy commitment and chaotic system," Springer Signal, Image and Video Processing, Vol. 9, No. 1, pp. 99-109, 2015.

[48] A. Juels and M. Sudan, "A fuzzy vault scheme," IBM Design Codes and Cryptography," Vol. 38, No. 2, pp. 237-257. 2006.

[49] V. Krivokuca, W. Abdulla and Swain, "A disection of fingerprint fuzzy vault schemes," 27th Conference on Image and Vision Computing, Dunedin, New Zealand, pp. 256-261, 2012.

[50] K. Nandakumar, A.K. Jain and S. Pankanti, "Fingerprint-based fuzzy vault: implementation and performance," IEEE Transactions on Information Forensics and Security, Vol. 2, No. 4, pp. 744-757, 2007.

[51] T.H. Nguyen, Y. Wang, T.N. Nguyen and R. Li, "A fingerprint fuzzy vault scheme using a fast chaff point generation algorithm," 2013 IEEE International Conference on Signal Processing, Communication and Computing, Solan, India, pp. 1-6, 2013.

[52] M. Piekarcyzk and M.R. Ogiela, "Usability of fuzzy vault scheme applied to predetermined palm-based gestures as a secure behavioral lock," 2015 10th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing, Krakow, Poland, pp. 363-367, 2015.

[53] A. Razaque, P.S. Sreeramoju, F.H. Amsaad, C.K. Nerella, M. Abdulgader and H. Saranu, "Multi-biometric system using fuzzy vault," 2016 IEEE International Conference on Electro Information Technology, Grand Forks, ND, USA, pp. 122-126, 2016.

[54] C. Rathgeb, B. Tams, J. Wagner1 and C. Busch, "Unlinkable improved multi-biometric iris fuzzy vault," EURASIP Journal on Information Security, Vol. 2016, No. 26, 2016.

[55] B. Tams, "Unlinkable minutia-based fuzzy vault for multiple fingerprints," IET Biometrics, Vol. 5, No. 3, pp. 170-180, 2016..

[56] D. Moon, Y. Chung, C. Seo, S.Y. Kim and J.N. Kim, "A practical implementation of fuzzy fingerprint vault for smart cards," Springer Journal of Intelligent Manufacturing, Vol. 25, No. 2, pp. 293-302, 2014.

[57] D. Schwab and L. Yang, "Entity authentication in a mobile-cloud environment," Eighth Annual Cyber Security and Information Intelligence Research Workshop, Oak Ridge, TN, USA, 2013.

[58] S. Sowkaritha and N. Radha, "Secure iris and fingerprint templates using fuzzy vault and symmetric algorithm," 7th International Conference on Intelligence and Control, Madras, India, pp. 189-193, 2013.

[59] E. Fang, C. Han and J. Liu, "Auto-aligned sharing fuzzy fingerprint vault," IEEE China Communications, Vol. 10, No. 10, pp. 145-154, 2013.

[60] K.Y. Moon, D. Moon, J.H. Lee and H.S. Cho, "Biometrics information protection using fuzzy vault scheme," 8th International Conference on Signal Image Technology and Internet Based Systems, Naples, Italy, pp. 124-128, 2012.

[61] H. Liu, D. Sun, K. Xiong and Z. Qui, "3D fuzzy vault based palmprint," 2010 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, Huangshan, China, pp. 230-234, 2010.

[62] D.H. Sharath Yadav, M.V. Karki and S.M. Sarala, "Fuzzy vault for fingerprint template security with error correcting codes," 2016 IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology, Bangalore, India, pp. 156-160, 2016.

[63] P. Sood and M. Kaur, "Methods of automatic alignment of fingerprints in fuzzy vault: a review," 2014 Recent Advances in Egineering and Computational Sciences, Chandigarh, India, pp. 1-4, 2014.

[64] A.I. Arrahmah, Y.S. Gondokaryono and K-H. Rhee, "Fast non-random chaff point generation for fuzzy vault biometric cryptosystems," 2016 IEEE 6th International Conference on Systems Engineering and Technology, Bandung, Indonesia, pp. 199-204, 2016.

[65] H.N. Dellys, Noussaiba Benadjimi, M.R. Boubakeur, L. Sliman and F. Ali, "Fuzzy vault chaff point generation by squares method," 2015 7th International Conference of Soft Computing and Pattern Recognition, Fukuoka, Japan, pp. 357-362, 2015.

[66] T.H. Nguyen, Y. Wang, Y. Ha and R. Li, "Performance and security-enhanced fuzzy vault schem based on ridge features of distorted fingerprints," IET Biometrics, Vol. 4, No. 1, pp. 29-39, 2014.

[67] P. Mihailescu, The fuzzy vault for fingerprint is vulnerable to brute force attack, Report arXiv:0708.2974vs [cs.CV], Cornell University, 2007.

[68] H.T. Poon and A. Miri, "A collusion attack on fuzzy vault scheme," International Journal on Information Security, Vol. 1, No. 1, pp. 27-34, 2009.

[69] H.W. Liu and Y. Wang, "A new fuzzy fingerprint vault using multivariable linear function based on lorenz chaotic system," 2012 International Conference on Computer Science and Automation Engineering, TBD Zhangjiajie, China, Vol. 1, pp. 531-534, 2012

[70] H. Liu, D. Sun, K. Xiong and Z. Qui, "A new fingerprint vault method using cubic spine interpolation," 2010 International Conference on Artificial Intelligence and computational Intelligence, Sanya, China, vol.1, pp.103-106, 2010.

[71] V.S. Meenakshi and G. Padmavathi, "Security analysis of hardened retina based fuzzy vault," 2009 International Conference on Advances in Recent Technologies in Communications and Computing, Kerala, India, pp. 926-930, 2009.

[72] L. Wu and S. Yuan, "A face based fuzzy vault scheme for secure online authentication," 2010 Second International Symposium on Data, Privacy and E-Commerce, Buffalo, New York, USA, pp. 45-49, 2010.

[73] V.E. Brindha, "Biometric template security using fuzzy vault," 2011 IEEE 15th International Symposium on Consumer Electronics, Singapore, pp. 384-387, 2011.

[74] M. Fouad, A.E. Sadik, J. Zhao and E. Petriu, "A fuzzy vault implementation for securing revocable iris templates," 2011 IEEE International Systems Conference, Montreal, QC, Canada, pp. 491-494, 2011.

[75] H. Liu, D. Sun, K. Xiong and Z. Qui, "Is fuzzy vault scheme very effective for key binding in biometric cryptosystems?," 2011 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, Nanjing, China, pp. 279-284, 2011.

[76] B. Tams, P. Mihailescu and A. Munk, "Security considerations in minutiae based fuzzy vaults," IEEE Transactions on Information Forensic and Security, Vol. 10, No. 5, pp. 985-998, 2015.

[77] J. Bringer, M. Favre, C. Pelle and H.D. Saxce, "Fuzzy vault and template-level fusion applied to a fingerprint representation," 2014 International Conference of the Biometrics Special Interest Group, Darmstadt, Germany, pp. 1-4, 2014.

[78] A.A. Nasir and M. Fathy, "Alignment-free fingerprint cryptosystem based on multiple fuzzy vaults," 2015 The International Symposium on Artificial Intelligence and Signal Processing, Mashhad, Iran, pp. 251-255, 2015.

[79] J. Hartloff, M. Morse, B. Zhang, T. Effland, J. Cordaro, J. Schuller, S. Tulyakov, A. Rudra and V. Govindaraju " A multiple server scheme for fingerprint fuzzy vaults," 2015 IEEE Conference on Computer Vision and Pattern Recognition Workshops, Boston, MA, USA, pp. 119-127, 2015.

[80] K Koptyra and M.R. Ogiela, Fuzzy vault schemes in multi-secret digital steganography," 2015 10th International Conference on Broadband and Wireless Computing, Communication and Applications, Krakow, Poland, pp. 183-186, 2015.

[81] M. Neu, U. Korte and M. Ullman, "Improvement of fuzzy vault for multiple fingerprints with angles," 2016 International Conference of the Biometrics Special Interest Group, Darmstadt, Germany, pp. 1-8, 2016.

[82] T.K. Dang, Q.C. Truong, T.T.B. Le and H. Truong "Cancellable fuzzy vault with periodic transformation for biometric template protection," IET Biometrics, Vol. 5, No. 3, pp. 229-235, 2016.

[83] B. Deepika, S. Sofat and M. Kaur, "Fingerprint fuzzy vault using Hadamard transformation," 2015 International Conference on Advances in Computing, Communications and Informatics, Kochi, India, pp. 1830-1834, 2015.

[84] C. Li and J. Hu, "A security-enhanced alignment-free fuzzy vault-based cryprosystem using pair-polar minutae structures," IEEE Transactions on Information Forensic and Security, Vol. 11, No. 3, pp. 543-555, 2016.

[85] S.R.S. Sree and N. Radha, "Cancellable multimodal biometric authentication system with fuzzy vault," 2016 International Conference on Computer Communication and Informatics, Coimbatore, Tamilnadu, India, pp. 1-6, 2016.

[86] Z. Wu, B. Liang, L. You, Z. Jian and J. Li, "High-dimensional space projection-based biometric encryption for fingerprint with fuzzy minuatia," Springer Soft Computing, Vol. 20, No. 12, pp. 4907-4918, 2016.

[87] J.P. Linnartz and P. Tuyls, "New shielding functions to enhance privacy and prevent misuse of biometric templates," Springer Lecture Notes in Computer Science, vol. 2688, pp. 393-402, 2003.

[88] P. Tuyls, A.H.M. Akkermans, T.A.M. Kavenaar, G.J. Schrijen, A.M. Bazen and R.J.N. Veldhuis, "Practical biometric authentication with template protection," Lecture Notes in Computer Science, vol. 3546, pp. 436-446, 2005.

[89] L. Huixian, W. Man, P. Liaojun and Z. Weidong, "Key binding based on biometric shielding functions," 2009 5th International Conference on Information Assurance and Security, Xi'an, China, vol. 1, pp. 19-22, 2009.

[90] H. Lu, K. Martin, F. Bui, K.N. Plataniotis and D. Hatzinakos, "Face recognition with biometric encryption for privacy enhancing self exclusion," 16th International Conference on Digital and Signal Processing, Santorini, Greece, pp. 1-8, 2009.

[91] E.J.C. Kelkeboom, B. Gokberk, T.A.M. Kevenaar and A.H.M. Akkermans, "3D face" : biometric template protection for 3D face recognition," Springer Lecture Notes in Computer Science, vol. 4642, pp. 566-573, 2007.

[92] M.V.D. Veen, T. Kavenaar, G.J. Schrijen, T.A.H. Akkermans F. Zuo, "Face biometrics with renewable templates," Proceedings of SPIE, Vol. 6072, pp. 1-12, 2006.

[93] Y. Dodis, R. Ostrovsky, L. Reyzin and A. Smith, "Fuzzy extractors: how to generate strong keys from biometrics and other noisy data," SIAM Journal on Computing, Vol. 38, No. 1, pp. 97-139, 2008.

[94] A.K. Jain, K. Nandakumar and A. Nagar, "Biometric template security," EURASIP Journal of Advances in Signal Processing, Special Issue on Biometrics, 2008.

[95] A. Boddo, Method for Producing a Digital Signature with the Aid of a Biometric Feature, German patent DE 42 43 908 AI, 1994.

[96] Y. Sutcu, Q. Li, and N. Memon, "Protecting biometric templates with sketch: theory and practice," IEEE Transactions on Information Forensics and Security, Vol. 2, No. 3, Part 2, pp. 1825-1840, 2007.

[97] K. Nandakumar, "A fingerprint cryptosystem based on minutiae phase spectrum," 2010 IEEE International Workshop on Information Forensics and Security, Seattle, WA, USA, pp. 1-6, 2010.

[98] A.S. Andallib and M. Abdulla-Al-Shami, "A novel key generation scheme for biometric cryptosystem using fingerprint minutae," 2013 International Conference on Informatics, Electronics and Vision, Dhaka, Bangladesh, pp. 1-6, 2013.

[99] J. Sadenka, K.S. Balagani, V. Phoha and P. Gasti, "Privacy-preserving population-enhanced biometric key generation from free-text keystroke dynamics," IEEE International Joint Conference on Biometrics, Clearwater, FL, USA, pp. 1-8, 2014.

[100] G. Davida, Y. Frankel, and B. Matt, "On enabling secure applications through offline biometric identification," IEEE Symposium on Security and Privacy, Oakland, California, USA, pp. 148-157, 1998.

[101] G. Davida, Y. Frankel and B. Matt, "On the relation of error correction and cryptography to an off-line biometric identification scheme," Proceedings of Workshop on Coding and Cryptography, Paris, France, pp. 129-138, 1999.

[102] K. Kummel and C. Vielhauer, "Reverse-engineer methods on a biometric hash algorithm for dynamic handwriting," 12th ACM Workshop on Multimedia and Security, Rome, Italy, pp. 67-72, 2010.

[103] R. Ranjan and S.K. Singh, "Improved and innovative key generation algorithms for biometric crytosystems," 2013 3rd IEEE International Advance Computing Conference, Ghaziabad, UP, India, pp. 943-946, 2013.

[104] G. Ma, J. Liu and B. Ni, "Probability of a unique crypto key generation based on fingers different images with two scanners," 2011 First Asian Conference on Pattern Recognition, Beijing, China, pp. 72-76, 2011.

[105] G. Paschal and D. Samantha, "Comparative features and same cryptographic key generation using biometric fingerprints," 2016 2nd International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics, Chennai, India, pp. 691-695, 2016.

[106] H.A. Garcia-Baleon, V. Alarcon-Aquino, O. Starostenko and J.F. Ramirez-Cruz, "Bimodal biometric system for cryptographic key generation using wavelet transforms," 2009 Mexican International Conference on Computer Science, Mexico City, Mexico, pp. 185-196, 2009.

[107] A. Luong, M. Gerbush, B. Waters, and K. Grauman, "Reconstructing a fragmented face from a cryptographic identification protocol," 2013 IEEE Workshop on the Applications of Computer Vision, pp. 238-245, Cleanwater Beach, FL, USA, 2013.

[108] C. Rathgeb and A. Uhl, "Context-based key generation for iris," IET Computer Vision, Vol. 5, No. 6, pp. 389-397, Nov. 2011.

[109] M.R. Ogiela and L. Ogiela, "Image based crypto-biometric key generation," 2011 Third International Conference on Intelligent Networking and Collaborative Systems, Fukuoka, Japan, pp. 673-678, 2011.

[110] W. Sheng, S. Chen, G. Xiao, J. Mao and Y. Zheng, "A biometric key generation method based on semisupervised data clustering," IEEE Transactions on Systems, Man, and Cybernetics: Systems, Vol. 45, No. 9, pp. 1205-1217, 2015.

[111] M. Blanton and M. Aliasgari, "Analysis of reusability of secure sketches and fuzzy extractors," IEEE Transactions on Information Forensics and Security, Vol. 8, No. 9, pp. 1433-1445, 2013.

[112] W. Yang, J. Hu, and S. Wang, "A delaunay triangle-based fuzzy extractor for fingerprint authentication," 2012 IEEE International Conference on Trust, Security and Privacy in Computing and Communications, Liverpool, United Kingdom, pp. 66-70, 2012.

[113] H.K. Bashier, L.S. Hoe, P.Y. Han, L.Y. Ping and C.M. Li, "Face spoofing detection based on improved local graph structure," 2014 International Conference on Information Science and Applications. Seoul, South Korea, pp. 1-6, 2014 .

[114] J. Galbally, S. Marcel and J. Fierrez, "Image quality assessment for fake biometric detection:application to iris, fingerprint, and face recognition," IEEE Transactions on Image Processing, Vol. 23, No. 2, pp. 710-724, 2014.

[115] M.L. Brocardo, I. Traore and I. Woungang, "Towards a framework for continuous authentication using syslometry," IEEE International Conference on Advanced Information Networking and Applications, Victoria, Canada, pp. 106-115, 2014.

[116] J. Roth, X. Liu and D. Metaxas, "On continuous user authentication via typing behaviour," IEEE Transactions on Image Processing, Vol. 23, No. 10, pp. 4611-4624, 2014

[117] Z. Syed, S. Banerjee and B. Cukic, "Leveraging variations in event sequences in keystroke-dynamics authentication systems," IEEE International Conference on High Assurance Systems Engineering. Miami Beach, FL, , pp: 9-16, 2014

[118] P-W. Tsai, M.K. Khan, J-S. Pan and B-Y. Liao, "Interactive artificial bee colony support passive continuous authentication system," IEEE Systems Journal, Vol. 8, No. 2, pp. 395-405, 2014.

[119] 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.

[120] A. Ur-Rehman, S. Ur-Rehman, I.U. Khan, M. Moiz and S. Hasan, " Security and Privacy Issues in IoT," International Journal of Communication Networks and Information Security, Vol. 8, No. 3, 2016.

[121] M. El Azhari, A. Toumanari, R. Latif and N. El Moussaid, "Relay Based Thermal Aware and Mobility Support Routing Protocol for Wireless Body Sensor Networks," International Journal of Communication Networks and Information Security, Vol. 8, No. 2, 2016