Contents lists available at Science-Gate

International Journal of Advanced and Applied Sciences

Journal homepage: http://www.science-gate.com/IJAAS.html

Cancelable and hybrid biometric cryptosystems: current directions and open research issues

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, UPM Serdang, Selangor, Malaysia*
[2]*Department of Computer Science, University of Jos, Jos, Nigeria*

ARTICLE INFO

Article history:
Received 28 April 2017
Received in revised form
20 September 2017
Accepted 21 September 2017

Keywords:
Biometrics
Biometric cryptosystem
Privacy
Security

ABSTRACT

Cancelable and hybrid biometric cryptosystems are two techniques used to offer protection against the security and privacy challenges faced by users of biometric authentication systems. The main objective of this paper is to present a critical review of current and emerging trends as well as open research issues in cancellable and hybrid biometric systems. The study examines cancelable biometrics under two main categories, namely non-invertible transformation and biometric salting. It also explores hybrid cryptosystems as means of providing improved template security and user privacy. The review focusses on the modes of operation, performance accuracy, security and privacy of various types of cancellable and hybrid biometric cryptosystems. It also provides a more comprehensive survey of latest research works in cancellable and hybrid biometric cryptosystems than existing review papers in these fields. The paper will provide readers with up-to-date information on current directions and open research issues in cancelable and hybrid biometric cryptosystems.

1. Introduction

Biometric recognition systems use suitable sensors to acquire biometric images from the clients. The images obtained from clients during enrolment are not stored as pictures in the databases. Rather, they are processed using appropriate mathematical and statistical techniques in order to obtain useful features which are used to represent the identity of clients. This process is referred to as feature extraction and the extracted feature vector denotes the reference template. The extracted features comprise of a set of value which are grouped together in what is known as a feature vector. The values which make up a feature vector can be in different formats such as binary, real and point sets. The verification process involves the acquisition of a probe image from clients. The same feature extraction method applied during enrolment is used to obtain a probe template which represents the test data. The test template is compared with the reference template to determine whether both of them belong to the same object. The noisy nature of biometric data introduces slight differences among multiple images belonging to the same subject. This difference is known as intra-class variation or intra-class distance. Similarity errors caused by intra-class variation make it imperative to use a threshold during the verification process. Templates obtained from different images belonging to the same user will have a higher degree of similarity than templates belonging to different users. A successful authentication requires that the dissimilarity between a reference template and a probe template be less than the assigned threshold.

Conventional biometric systems store biometric templates directly in the database. Such templates could be stolen by intruders and used to launch replay attack against the authentication system. Unprotected templates also expose legitimate users to privacy violations in the form of cross matching attacks, template sharing and function creep. A more challenging situation occurs if an intruder is able to reconstruct actual biometric images from compromised digital templates. This results in loss of identity as an intruder may impersonate the legitimate owner of the biometric during enrolment and authentication. The enormity of these challenges makes it imperative for practical biometric systems to provide adequate protection for stored templates and privacy for legitimate users.

[*] Corresponding Author.
Email Address: abayomi.jegede@ymail.com (A. Jegede)

https://doi.org/10.21833/ijaas.2017.011.010

Biometric cryptosystems or template protection schemes apply techniques from the domain of cryptography and biometrics to address the security and privacy issues related to the use of biometrics as an authentication mechanism. The deployment of biometric cryptosystems enables the authentication system to perform both verification and template protection simultaneously. 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 also make it possible to revoke, update or replace biometric data in the event of loss or data corruption.

2. Cancelable biometrics

Cancelable biometrics can be defined as "an intentional, repeatable distortion of a biometric signal based on a chosen transform" (Ratha et al., 2001). The goal of cancelable biometrics is to provide diversity and unlinkability by using different transforms for different applications involving the same set of users. This prevents collision among templates of the same subjects stored in different biometric databases. The approach also provides revocability, which allows administrators to remove a compromised template and reissue a new one based on the same biometric data. Template revocability is achieved by changing the transformation parameters used for the previous enrolment. The security of transformed templates is guaranteed since decryption does not take place during authentication. Rather, the authentication process involves a comparison between the reference and the query templates in the transformed domain. The cancelable approach can be classified as non-invertible transforms and invertible transforms or biometric salting. Both methods apply specific transformation parameters to a biometric feature vector in order to obtain its transformed version.

2.1. Non-invertible transforms

Non-invertible transforms apply a one-way and an irreversible process to generate a transformed template from a biometric data. The approach provides resistance against template reconstruction even if an impostor gains access to both the templates and the transformation parameters. Non-invertible transformation was first implemented using three techniques, namely grid morphing, block permutation and feature domain transforms (Ratha et al., 2001). Grid morphing and block permutation were used to carry out distortion of fingerprint images. These techniques provide non-invertibility by preventing matching between a transformed image and an original image. They also achieve diversity by preventing matching between multiple versions of transformed images obtained using different parameters. It is important to note that block permutation is highly vulnerable if an attacker knows the permutation key (Rathgeb et al., 2012). Feature domain transforms, namely Cartesian, radial and functional transforms (Ratha et al., 2006) obscure fingerprint minutia point sets to prevent the recovery of original (point set) data from the transformed version. Experimental results show that these approaches provide template security, renewability and revocability with minimal loss in recognition accuracy. It was observed that feature transformation increases the false rejection rate (FRR) by 5% for any given false acceptance rate (FAR). The application of cartesian, polar and surface folding transformations on fingerprint biometric data provides template security, revocability and cross-matching (Ratha et al., 2007). It also prevents cross-matching of templates in biometric databases. Security analysis shows that the key lengths for polar transformation and surface folding transform are 64 bits and 66 bits respectively. Cartesian and polar transforms suffer low recognition performance because a little change in minutiae position in the original fingerprint can lead to a significant change in minutiae position of the transformed template (Quan et al., 2008). The key lengths of polar and surface folding transforms are low and this makes them susceptible to brute force attack. Functional transforms are vulnerable to dictionary attack and attack via record multiplicity (Quan et al., 2008; Shin et al., 2009). Fingerprint templates created using non-invertible Gabor transform provide diversity, resistance to template reconstruction attack and robustness against minor transformation errors and rotation distortion (Narayanan and Subramanian, 2011). A key generated from user's handwriting (a behavioral biometric) can also be used to transform fingerprint features (Arya and Singh, 2012). The handwriting features are generated based on the direction and speed of the characters. Results from experiments shows that the approach has good recognition accuracy with FRR and FAR of 4.0% and 0% respectively. The security of the approach relies on the difficulty an attacker faces in attempting to forge the handwriting of legitimate users. An attacker can construct valid keys from compromised handwritings and use the keys to retrieve fingerprint data from transformed templates.

Non-invertible transformations have also been applied to other biometric modalities apart from fingerprint. For example three bio-convolving techniques: baseline, mixing and shifting were proposed for on-line signature (Maiorana et al., 2011). These approaches provide template renewability and security, but slightly lower recognition accuracy. Experimental results show that mixing has lower false rejection rate of (FRR), but higher false acceptance rate (FAR) shifting. The mixing approach achieves FRR of 10% and FAR 3%

while the FRR and FAR for shifting are 12% and 1.85 respectively. The security of the scheme depends on the secrecy of the transformation key. An attacker can compromise the scheme and recover original templates if he gains access to the transformation key. A technique which integrates cancelable techniques with knowledge signatures (Xu et al., 2008) have been shown to provide good recognition accuracy when applied to voiceprint features. The approach also prevents disclosure of the original voice data even if an impostor gains access to the transformation key.

Pseudo-random permutation (Grassi and Faundez-Zanuy, 2009) transforms and secures face biometric template by making it impossible for an attacker to compromise the authentication system without knowing the pseudo-random ordering of the scheme. Security analysis shows that this approach provides up to 100! different permutations. These results in large key space and less susceptibility to guessing attacks. A related study transformed real-value face template using a combination of Gaussian distribution and random scrambling (Jeong and Teoh, 2010). The template is first modified by carrying out a random replacement of some of its components using Gaussian distribution. This ensures that the transformed template retain its original mean and variance. This is followed by a random scrambling of the elements in the modified feature vector. Experimental results show that applying non-invertible transformation has minimal effects on the recognition performance of the scheme. It was also found that the EER varies with the dimension of the face template. Reproducibility tests show that it is difficult to recover original face images from transformed templates. Gray-combo and bin-combo are two techniques proposed for transformation of normalized iris image and binary iris code respectively (Zuo et al., 2008). These approaches use non-invertible and revocable transform to provide template security and protection against loss of identity. Results of security analysis show that bin-combo is more secure (560-bit key length) than gray-combo (260-bit key length). Techniques such as block re-mapping and image warping have also been used for image-level transformation of iris biometric data (Hammerle-Uhl et al., 2009). Both techniques apply repeatable and non-invertible transformations to an iris image prior to feature extraction. Experimental results show block re-mapping and image warping has equal error rate (ERR) of 1.2% and 1.3% respectively. This implies that there is no significant difference in the recognition accuracy provided by the two techniques. Other techniques proposed for image-level transformation of iris biometric data are block-remapping and texture-warping or mesh deformation (Farberbock et al., 2010). These techniques were applied to rectangular and polar iris images. The transformation process was successful for only polar iris images. The transformation of rectangular iris images failed due to segmentation errors in transformed iris image. Results from experiments show that block re-mapping has lower recognition accuracy (EER=3.1%) than texture warping is (EER=2.0%). In addition to bin-combo, user-specific permutation was proposed for binary iris code in order to achieve template security and revocability without loss in recognition performance (Rathgeb and Uhl, 2010). Performance evaluation shows that the approach provides good recognition accuracy (FRR of 3.821% and FAR of 0%) and adequate security for stored templates (a total number 38! permutations). A major limitation of the technique is the possibility of an attacker to recover the original template if he knows both the transformed template and the permutation key. Cancelable and revocable iris templates were also created using alignment-free adaptive bloom filter (Rathgeb et al., 2014). The approach supports data compression and rotation invariance. It also provides good recognition accuracy (up to 97.95% GAR and FAR of 0.01%) and high level security for stored templates. Other approaches such as Hadamard transform (Wang and Hu, 2013), spiral cube (Moujahdi et al., 2012), pulse active transform (Safie et al., 2014) and Delaunay triangle (Sandhya et al., 2016) have been used to carry out one-way transformation of biometric data. The achievements, performance and security of these and other related works are summarized in Table 1.

A recent work applied cancelable and irreversible techniques based on the modifications of SHA1 and SHA2 algorithms (Yang et al., 2015). The approach addresses pre-alignment problem and constructs new fingerprint features which are resistant to image rotation. The improved SHA1 algorithm provided improved avalanche and resistance to collision attack. The original SHA1 achieves an avalanche of 1.000000 in the 23rd round while the improved SHA1 achieves the same avalanche in the 21st round. The modified SHA2 algorithm provides local smoothness and diversity (distinctiveness). Local smoothness implies that a minor change in biometric data does not result in a large change in the value of the transformed template. Diversity allows the generation of multiple and distinct transformed templates from an instance of fingerprint data. The improved SHA1 and SHA2 provide increased efficiency in processing speeds by 8.24% and 6.29% respectively. Similarly, kernelized locality-sensitive hashing was used to create irreversible fixed length vector from fingerprint minutia (Jin and Teoh, 2015). Experimental results and security analysis based on FVC 2002 database show that the approach provides good recognition accuracy (EER of 4.35%, 4.76% and 11.49% for FVC DB1, DB2 and DB2 respectively).

Some studies analyzed the security of non-invertible schemes in order to uncover potential weaknesses. One of such weaknesses is the possibility of recovering an original image from its transformed version without having any knowledge of the transformation parameters (Lee et al., 2009). Cancelable biometrics has also been found to be susceptible to record multiplicity attack (Li and Hu, 2016). Analysis also shows that knowledge of the minutiae distribution minimizes the complexity of recovering original fingerprint data from a transformed template (Nagar and Jain, 2009). The application of non-invertible Gabor transform provides irreversibility and diversity which improves the security of the system (Narayanan and Subramanian, 2011). The technique is also robust against minor translation error and rotation distortion.

Table 1: Summary of related works (non-invertible transforms)

Author	Modality	Technique	Achievements	Performance	Security
Zuo et al. (2008)	Iris image	Gray-combo	Uses non-invertible and revocable transforms to provide security and guard against loss of identity	N/A	260-bit secret length
	Binary iris code	Bin-combo	Bin-combo is a non-invertible and revocable transform that provides security and guards against loss of identity	N/A	560-bit secret length
Hammerle-Uhl et al. (2009)	Iris image	Block re-mapping and image warping	Provides protection for iris features by applying repeatable non-invertible transformation prior to feature extraction	Results of block re-mapping shows an ERR of 1.2%, while the EER of image warping is 1.3%.	N/A
Grassi and Faundez-Zanuy (2009)	Face template	Pseudo-random permutation	Secures stored template by making it impossible for an attacker to compromise the authentication system without knowing the pseudo-random ordering of the scheme	N/A	Up to 100! different permutations which translates to large key space and less susceptibility to guessing attacks
Rathgeb and Uhl (2010)	Binary iris code	User-specific permutation	Provides template security and revocability without loss in recognition performance	Achieves FRR of 3.821% and FAR of 0%.	A total number 38! permutations are possible
Farberbock et al. (2010)	Rectangular and polar iris images	Block-remapping and texture-warping or mesh deformation	The transformation process was successful for only polar iris images. The transformation of rectangular iris images failed due to segmentation errors in transformed iris image	Block re-mapping achieves EER of 3.1%, while the EER for texture warping is 2.0%	N/A
Jeong and Teoh (2010)	Real value face template	Gaussian distribution and random scrambling	Experimental results shows that applying non-invertible transformation do not degrade the recognition performance significantly	The EER varies with the dimension of the face template. maximum EER achieved is 24%	Reproducibility tests show that it is difficult to recover original face Images from transformed templates
Moujahdi et al. (2012)	Face	Spiral cube	The difficulty of computing the projection matrix enhances the security of transformed templates	The transformation techniques reduces performance by 3.34%	Large key space and robust against brute force attack
Wang and Hu (2013)	Fingerprint	Hadamard transform	Provides revocability and template security	Good recognition accuracy (EER of 3% and 9.12%)	Supports template renewability and adequate security
Rathgeb et al. (2014)	Binary iris template	Alignment-free adaptive Bloom filter	Provides template protection, data compression, computational efficient recognition and good accuracy	Achieves genuine acceptance rate of up to 97.95% GAR (or 2.05% FAR) of and false match rate of 0.01%	Provides irreversibility of templates and unlinkability of multiple transformed templates
Safie et al. (2014)	Electro Cardiogram (ECG)	Pulse active transform	Improved performance and security	Low error rates (EER of 0.1538%/0.2388%)	Prevents the recovery of original ECG signal from secured version
Jin and Teoh (2015)	Fingerprint	kernelized locality-sensitive hashing	Provides good recognition accuracy and speedy matching	EER of 4.35%, 4.76% and 11.49% for FVC DB1, DB2 and DB2 respectively	High level template security
Sandhya et al. (2016)	Fingerprint	Delaunay triangle	A technique which provides good balance between security and performance	Satisfactory performance accuracy (EER of 2.98% and 12.17%)	Large key space, resistant to guessing and brute force attack

2.2. Biometric salting

Biometric salting allows the recovery of an original template from a transformed version if both the template and the transformation parameters are revealed to an attacker. The security of the salting technique depends largely on the secrecy of the transformation key and the complexity of the transformation algorithm. The salting technique was applied to face feature vectors in order to generate cancelable templates (Savvides et al., 2004). This approach applies minimum correlation filters in which user-specific secret PINs serve as seeds for the random basis function. The technique provides cancelability by using different convolution filters to create multiple templates from the same face image. Experimental results based on the illumination subset of the CMU pose, illumination, expressions (PIE) face dataset shows that encryption does not any effect on the recognition accuracy of the proposed approach. Ouda et al. (2010) applied biometric salting to obtain cancelable iris templates. Results of experiments based on CASIA-IrisV3-Interval database show that the approach has good recognition accuracy with FRR and FAR of 6.96% and 0% respectively. The transformation is easy to implement and does not degrade the recognition accuracy of the system. Security and privacy analysis show that the approach provides revocability, diversity and irreversibility. Transformation techniques based on user-specific random projection and error minimizations were also applied to face feature vector in order to create salted templates (Kim and Toh, 2007). Empirical results based on AR face database and BERC visual face database show that the approach provides template security, cancelability and improved recognition accuracy. Security analysis shows that the proposed method is also robust against replay attack. A recent approach applies user-specific tokenized to generate revocable binary features from phase and magnitude patterns of log-Gabor filters (Kaur and Khanna, 2017). The tokenized variables are used to perform multi-level transformations of biometric data at signal and feature levels. The use of tokenized variables provides good recognition performance and resistance against information leakage in case of correlation attacks. Experimental results show that the application of the approach on CASIA V5, CASIA NIR V5 (thermal) and ORL face databases produces equal error rates (EERs) of 1.29%, 2.03% and 0.54% respectively. The respective EERs for iris, CASIA palmprint, PolyU palmprint, CASIA MS V1 palmvein and SDUMLA-HMT fingerprint databases are 1.35%, 2%, 0.59%, 4.54% and 1.10%. The approach provides unlinkability and diversity as it is possible to generate 101 cancelable templates from an instance of biometric data. However, this scheme can be compromised if an attacker knows the user-specific tokens. A hybrid salted technique secures face; fingerprint and iris data based on the integration of slantlet and singular value decomposition transforms (Latif et al., 2017). This method provides high level template security as protected biometric image cannot be recovered without the knowledge of the transformation parameters. The approach is also robust against image processing and geometric attacks. A major weakness of the approach is that original biometric data can be obtained from a transformed template if an impostor knows the secret key.

Table 2 presents a summary of related works in biometric salting. It highlights achievements, performance and security of various salting techniques.

Table 2: Summary of related works (biometric salting)

Author	Modality	Technique	Achievements	Performance	Security
Savvides et al. (2004)	Face	Image convolution and correlation filter	Provides cancelability and good recognition performance.	The recognition accuracy is not affected by transformation or the convolution kernel.	Provides cancelability by varying the convolution kernels.
Kim and Toh (2007)	Face	Extended random projection and near optimal transformation	Efficient feature extraction, template security and improved recognition accuracy	Good recognition performance despite the transformation of biometric data.	The transformation secures original biometric data and provides resistance against replay attack.
Ouda et al. (2010)	Iris code	Tokenless cancelable scheme	Provides revocability, diversity and irreversibility without any effect on recognition performance.	Minimal impact on recognition accuracy. FRR and FAR of 6.96% and 0% respectively.	Resistant to guessing and template reconstruction attack.
Kaur and Khanna (2017)	Iris, plamprint, palmvein and fingerprint	Log-Gabor filters	Good recognition performance and resistance against information leakage in case of correlation attacks	Minimum and maximum ERRs of 0.54% and 4.54% respectively	Unlinkability and diversity -can generate 101 cancelable templates from an instance of biometric data.
Latif et al. (2017)	Face, fingerprint and iris	Salted hybrid (slantlet + singular value decomposition transforms)	High level template security as protected biometric image cannot be recovered without the knowledge of the transformation parameters.		Robust against image processing and geometric attacks.

Biometric salting is vulnerable to stolen token attack (Kong et al., 2006) and false acceptance attack (Rathgeb et al., 2012). Biohashing and other variants of the salting technique have low recognition accuracy when an attacker knows the secret tokens (Rathgeb et al., 2012). Multispace random projection (Teoh and Yuang, 2007) and Biophasor token supplements (Teoh and Ngo, 2006) provide alternative solutions to template reconstruction attack against salted biometric data. Experimental results show that multispace random projection has good recognition accuracy and prevents key leakage.

3. Hybrid biometric cryptosystems

Hybrid cryptosystems integrate two or more template protection schemes to create a single biometric cryptosystem. Hybrid techniques rely on the strengths of the component schemes to provide an integrated approach with better security and user privacy. A major drawback of hybrid schemes is that they have higher implementation costs and complexity of operation. A hybrid scheme was created by combining non-invertible transformation and secure sketch (Bringer et al., 2008). The scheme leverages on the error correcting capability of secure sketch to address low recognition accuracy of non-invertible transformation. The application of the technique to fingerprint yields FRR of 35% and FAR of 5.53%. It also improves the recognition performance without compromising the security of stored templates. Similarly, Bloom filter was also used to transform face templates before securing the transformed templates with the helper data (Butt and Damer, 2014). Bloom filters generate an irreversible template which helps to increase the security of the scheme. That is, a compromise of the helper data will not reveal original biometric templates. However, the use of bloom filters lowers the recognition performance of the scheme. It is also possible to obtain a hybrid scheme by 'coupling' a fuzzy commitment scheme with fuzzy vault (Nagar et al., 2010). This method provides good recognition performance (GAR = 95% and FAR = 0.01%) and offers a two-level protection for stored fingerprint templates. Security analysis shows that the hybrid approach increases the min-entropy (a measure of security) of the fuzzy vault from 31 bits to 47 bits. A related work (Chafia et al., 2010) first used fuzzy commitment scheme to encode the true fingerprint minutia before securing the encoded template in a fuzzy vault. Experimental results show that the scheme achieves GAR of 68.5% and FAR of 3.5%, which indicates improved performance accuracy over the baseline study. Template protection techniques such as enhanced biohash and key binding have been integrated to provide a hybrid scheme for securing face templates (Ao and Li, 2009). Performance analysis shows that the scheme has genuine acceptance rate (GAR) of 97.79% and FAR of 8.32%. The use of BCH encoding as error correction method minimizes the success of brute force attack. In summary, the method achieves improved security, but with a minimal (1-2%) reduction in accuracy. A related work (Yang et al., 2013) used bio-hashing technique to create non-invertible fingervein templates which are used as inputs for fuzzy commitment scheme and fuzzy vault. A separate evaluation of this technique on fuzzy commitment scheme and fuzzy vault reflects good recognition performance and security. However, the security and recognition accuracy becomes degraded when fuzzy commitment scheme is fused with fuzzy vault because they use different similarity measures. Face template protection was also performed using a scheme which combines three techniques, namely random projection, discriminability-preserving transform and fuzzy commitment scheme (Feng et al., 2010). Results from experiments show that scheme has EER of between 8.55% and 16.68%. It also provides cancelability, discriminability and an increase in recognition accuracy by 4 -15%. It is also resistant to masquerade, hill-climbing and brute force attacks. Other proposals for hybrid schemes are based on the integration of traditional encryption techniques. For example, RSA and simple symmetric algorithm were used to create a hybrid scheme, which has a maximum key length of 32 bits and supports biometric data of variable input sizes (Nasir and Kuppuswamy, 2013). The scheme also provides improved authentication speed (can handle up to 624 bytes per second) and security of stored templates. Similarly, a technique based on key generation and encryption was proposed to provide secure transmission of mosaic image (Dahake and Nimbhorkar, 2015). The image is encrypted (prior to transmission) by using a key generated from fingerprint data. The encrypted image cannot be decrypted without the availability of the fingerprint data. However, it is difficult to obtain the fingerprint as it is not stored directly. The original image is discarded after the generation of the biometric key.

Non-discriminability among stored templates which is a major weakness of the generic fuzzy vault was addressed by a hybrid scheme which uses password to provide an additional layer of security for fuzzy vault (Meenakshi and Padmavathi, 2010). An application of this technique to multibiometric (fused fingerprint, iris and retinal features) template shows that the use of password enhances user privacy by providing discriminability among protected templates. It also provides improved security by increasing the entropy of the vault by 18 to 30 bits. Similarly, user-specific transformation was applied on face biometric data before securing the transformed template in a fuzzy vault (Wu and Yuan, 2010). This approach achieves minimum FRR and FAR of 23% and 15.38% respectively. It also improves the security of fuzzy vault by using a key generated from user-specific password to encrypt the vault. A related work (Chen and Chen, 2010) first applied noninvertible transformation to fingerprint data and then secured the transformed templates in a fuzzy vault. In another study, one-way cryptographic hashing is used to create non-invertible templates before securing the hashed template in a fuzzy vault (Vo et al., 2014). This is similar to using random projection to obscure genuine palmprint chaff points before securing the protected points in a fuzzy vault (Liu et al., 2014). This method achieves good recognition accuracy, cancelability and security. The FAR is always 0% and a reduction in FRR leads to a decrease in the security of the scheme. A secure and effective approach based on the integration of non-invertible transformation with key generation was proposed for fingerprint template protection (Lalithamani and Soman, 2009). Non-invertible templates and keys were created by applying a one-way transformation to fingerprint minutiae before generating a unique key from the transformed template. A major shortcoming of the hybrid scheme is the complexity of its implementation and operation as well as an increase in the time required for authentication.

The relevant works in hybrid cryptosystems are summarized in Table 3. The table highlights achievements, performance and security of various hybrid techniques.

Table 3: Summary of related works (hybrid schemes)

Author	Modality	Technique	Achievements	Performance	Security
Bringer et al. (2008)	Fingerprint	Secure sketch + non-invertible transformation	Leverages on the error correcting capability of secure sketch to improve the recognition performance, while not compromising security	The scheme yields FRR of 35% and FAR of 5.53%	N/A
Ao and Li (2009)	Face	Enhance biohash + key binding	The scheme achieves improved security, but with a minimal (1-2%) reduction in accuracy	Achieves GAR of 97.79% and FAR of 8.32%	The BCH encoding method minimizes the success of brute force attack
Chafia et al. (2010)	Fingerprint	Fuzzy vault + fuzzy commitment scheme	Provides improved performance accuracy over the baseline study	Achieves GAR of 68.5% and FAR of 3.5%	
Meenakshi and Padmavathi (2010)	Fused fingerprint, iris and retinal features	Password + fuzzy vault	Uses password to provide additional layer of security and enhance user privacy.	Multimodal fuzzy vault reduces the failure to capture rate of the generic fuzzy vault	The use of password increases the entropy of the vault by 18 - 30 bits
Nagar et al. (2010)	Fingerprint minutia	Fuzzy vault + fuzzy commitment scheme	Offers a two-level protection for stored fingerprint templates	Results show GAR of 95% and FAR of 0.01%	The hybrid approach increases the min-entropy of the fuzzy vault from 31 bits to 47 bits
Feng et al. (2010)	Face	Random projection + discriminability-preserving transform + fuzzy commitment scheme	The scheme provides cancelability and discriminability. It also increases recognition accuracy by 4 -15%	Results show EER of between 8.55% and 16.68%	Resistant to masquerade, hill-climbing and brute force attacks
Wu and Yuan (2010)	Face	User-specific transformation + fuzzy vault	Improves the security of fuzzy vault by using a key generated from user-specific password to encrypt the vault	Achieves minimum FRR and FAR of 23% and 15.38% respectively	N/A
Filho et al. (2012)	Signature	Papilo's method + Bio-convolving	A method which provides robust and secure signature verification	Provides good recognition accuracy	Adequate security (key length of 128 bits)
Ghany et al. (2012)	Fingerprint	Random projection + class distribution preserving + biohash	An efficient approach which provides good recognition accuracy and security simultaneously	Minimal error rate of 0.0627%	Provides improved security for biometric templates
Zhu et al. (2012)	Voiceprint	Random projection + fuzzy vault	Provides good recognition accuracy and improved security	Low FRR (4.37%) and FAR (0.07%)	Very large key space and low probability of guessing the secret key correctly
Nasir and Kuppuswamy (2013)		RSA + simple symmetric algorithm	Provides improved authentication speed and security of stored templates	Authentication speed of 624 bytes/second	Maximum key length of 32 bits for biometric data of variable input sizes
Butt and Damer (2014)	Face	Bloom filter + helper data	Provides improved security for stored face templates	Lower recognition performance due to bloom filters transformation	A compromise of the helper data will not reveal original biometric data
Le et al. (2014)	Face	Periodic function transform + fuzzy vault	Simple implementation which is suitable for different kinds of biometrics	Have low error rate (EER of 0.25%)	Provides template revocability and security
Liu et al. (2014)	Palmprint	Random projection + fuzzy vault	Achieves good recognition accuracy, cancelability and security	The FAR is always 0%. Lowering FRR reduces security	Random projection obscures genuine chaff points and enhances template security

Nguyen et al. (2016)	Fingerprint	Linear projection + fuzzy vault	Provides improved security and good recognition performance	High recognition accuracy (GAR of 92% and FAR of 7%)	Resistant to blend substitution attack and provides high entropy
Dahake and Nimbhorkar (2015)	Fingerprint	Key generation encryption	A scheme which provides secure transmission of mosaic image by encrypting it with a key generated from fingerprint data	N/A	It is difficult to obtain the fingerprint as it is not stored directly. The original image is discarded after a key is generated from it
Khandelwal and Gupta (2015)	Fingerprint	Fuzzy vault + biometric salting	Good recognition accuracy and improved security.	Good recognition accuracy with FRR and FAR of 0.2% and 0.003% respectively.	An attacker who knows the transformation (salting) key and the lock can recover fingerprint data from secured templates.
Wu et al. (2016)	Fingerprint	Fuzzy vault + high-dimensional space projection	High security and user privacy as the system does not store any information about a user's biometric data	N/A	Resistant to against brute-force and cross-matching attacks.
Sree and Radha (2016)	Multibiometric face and fingerprint	Fuzzy vault + cancelable biometrics	Good recognition accuracy and improved security.	Good recognition accuracy with GAR and FAR of 98.1% and 2% respectively.	Improved security and user privavy.
Sandhya and Prasad (2016)	Fingerprint	Nearest neighbor feature set (NNFS) + Delaunay triangle feature set (DTFS)	Good recognition accuracy and high level security.	EER of 0%, 0.059% and 3.93% for FVC 2002 DB1, FVC 2002 DB2 and FVC 2002 DB3 respectively.	Resistant to template reconstruction, guessing and hill climbing attacks.

Non-discriminability among stored templates which is a major weakness of the generic fuzzy vault was addressed by a hybrid scheme which uses password to provide an additional layer of security for fuzzy vault (Meenakshi and Padmavathi, 2010). An application of this technique to multibiometric (fused fingerprint, iris and retinal features) template shows that the use of password enhances user privacy by providing discriminability among protected templates. It also provides improved security by increasing the entropy of the vault by 18 to 30 bits. Similarly, user-specific transformation was applied on face biometric data before securing the transformed template in a fuzzy vault (Wu and Yuan, 2010). This approach achieves minimum FRR and FAR of 23% and 15.38% respectively. It also improves the security of fuzzy vault by using a key generated from user-specific password to encrypt the vault. A related work (Chen and Chen 2010) first applied noninvertible transformation to fingerprint data and then secured the transformed templates in a fuzzy vault. In another study, one-way cryptographic hashing is used to create non-invertible templates before securing the hashed template in a fuzzy vault (Vo et al., 2014). This is similar to using random projection to obscure genuine palmprint chaff points before securing the protected points in a fuzzy vault (Liu et al., 2014). This method achieves good recognition accuracy, cancelability and security. The FAR is always 0% and a reduction in FRR leads to a decrease in the security of the scheme. A secure and effective approach based on the integration of non-invertible transformation with key generation was proposed for fingerprint template protection (Lalithamani and Soman, 2009). Non-invertible templates and keys were created by applying a one-way transformation to fingerprint minutiae before generating a unique key from the transformed template. A major shortcoming of the hybrid scheme is the complexity of its implementation and operation as well as an increase in the time required for authentication.

A recent hybrid technique for fingerprint template protection is based on the integration of key generation and key binding techniques (Wu et al., 2016). The approach uses high-dimensional space projection to generate unique keys from fingerprint images. The generated keys are then encrypted with the fuzzy vault. The approach provides improved template security and user privacy as the authentication system does not store any information about a user's biometric characteristics. It also provides resistance against brute-force and cross-matching attacks. A different strategy combined fuzzy vault (key binding) and periodic transformation (cancelable method) techniques to provide improved template security and user privacy (Dang et al., 2016). Periodic transformation is a simple technique which can be applied to different biometric modalities. Results of security analysis show that the proposed hybrid scheme is resistant to brute force attacks. A related work (Sree and Radha, 2016) used a hybrid scheme based on the integration of fuzzy vault and cancelable biometrics to secure multibiometric (face and fingerprint) data. This approach first transforms biometric images prior to feature extraction. Extracted face and fingerprint feature data are combined using feature level fusion before securing the fused biometric data with fuzzy vault. Experimental results show that the approach has good recognition accuracy with GAR and FAR of 98.1% and 2% respectively. Similarly, Li and Hu (2016) applied pair-polar transformation to fingerprint minutiae structures before encoding the transformed data with the fuzzy vault. Pair-polar transformation allows the use of different transformation secrets for different applications. This method provides template discriminability, revocability and diversity. The approach also uses large number of chaff points to increase the complexity of recovering original biometric data from protected templates. Fuzzy vault has also been combined with biometric salting to create a computationally efficient hybrid scheme for securing fingerprint data (Khandelwal and Gupta, 2015). The approach has good recognition accuracy with FRR and FAR of 0.2% and 0.003% respectively. A limitation of this approach is that an attacker who knows the transformation (salting) key and the lock can recover fingerprint data from secured templates. Two different cancelable techniques were also used to create a hybrid approach for fingerprint template protection based on weighted sum rule and *T*-operators (Sandhya and Prasad, 2016). This method uses nearest neighbor feature set (NNFS) and Delaunay triangle feature set (DTFS) to obtain matching scores from reference and probe fingerprint data. Authentication is performed using *T*-operators (*T*-norms and *T*-conorms) to combine the matching scores of reference and probe fingerprint data. Experimental results show that the approach has good recognition accuracy with EER of 0%, 0.059% and 3.93% for FVC 2002 DB1, FVC 2002 DB2 and FVC 2002 DB3 respectively. Security analysis shows that the approach is resistant to template reconstruction, guessing and hill climbing attacks.

4. Open issues and challenges

Applying cancelable techniques results in high template security but with a corresponding reduction in recognition accuracy (Feng et al., 2010). This is because the transformation alters the composition of image pixels or feature vectors in the original biometric data. This makes it difficult for matching to be carried out in the transformation domain. One-way transformation techniques such as gray-combo and bin-combo (Zuo et al., 2008), pseudorandom permutation (Grassi and Faundez-Zanuy, 2009), spiral cube (Moujahdi et al., 2012), Hadamard transform (Wang and Hu, 2013), pulse active transform (Safie et al., 2014), alignment-free adaptive bloom filter (Rathgeb et al., 2014) and Delaunay triangle (Sandhya et al., 2016) depend on the complexity of the algorithms, while user-specific secret permutation (Rathgeb and Uhl, 2010) relies on the secrecy of the permutation key. Although gray combo and bin-combo have long key lengths (260 bit and 560 bits respectively) and large key space, both approaches are susceptible to exhaustive search attack. The entire key space can be searched and the original iris image or iris code recovered from transformed image or transformed template respectively. Pseudorandom permutation can be compromised if an impostor understands the pseudo-random ordering of the scheme. Its large key space of 100! can be searched using exhaustive search and this leads to the recovery of secret permutation keys. Transformed templates are derived from original biometric data using projection matrix (in the case of Spiral cube) and Hadamard matrix (in the case of Hadamard transform). The inverse of both matrices can be computed and thus an attacker who knows the transformation matrix can recover original biometric data from a transformed template. Alignment-free adaptive bloom filter transforms biometric data by mapping it from a high dimensional subspace to a low dimensional subspace. A major limitation of this approach is the loss of information in the original biometric data. Pulse active transform is only suitable for biometric data in continuous form such as ECG and signature and not suitable for binary biometric data such as iris code. Delaunay triangle uses a set of complex processes and a user-specific key to secure biometric data. An attacker can use reverse engineering to recover original biometric data from a protected template if he knows the user-specific key. User-specific permutation and random scrambling can be easily compromised once an attacker obtains the secret key used to transform the template. A previous work based on pseudo-random permutation (Grassi and Faundez-Zanuy, 2009) analyzed the security of the proposed technique without providing information on the recognition accuracy. On the other hand, approaches such as block remapping and image warping (Hammerle-Uhl et al., 2009; Farberbock et al., 2010), random scrambling (Jeong and Teoh, 2010), Hadamard transform (Wang and Hu, 2013), pulse active transform (Safie et al., 2014) and alignment-free adaptive bloom filter (Rathgeb et al., 2014) provide information on recognition accuracy but not on security.

Hybrid schemes derive their security and privacy-preserving capabilities from the constituent template protection schemes. A successful compromise of the security of the component schemes will lead to a violation of the security of stored biometric data and privacy of legitimate users. For example, hybrid schemes based on password or PIN and fuzzy vault (Meenakshi and Padmavathi, 2010; Wu and Yuan, 2010) can be compromised if an attacker knows the secret used to lock the vault and the user password. Hybrid schemes created by integrating of fuzzy commitment scheme and fuzzy vault (Chafia et al., 2010; Nagar et al., 2010) also have their limitations. This is because both the inner fuzzy commitment scheme and the outer fuzzy vault can be compromised once an attacker obtains the random secret and the 'lock' respectively. An improved approach based on random projection, class distribution preservation and biohashing (Ghany et al., 2012) provides better template security and user privacy. However, random projection results in loss of information in the original data (Lin and Gunopulos, 2003). Biohash is susceptible to false acceptance if an impostor compromises the hash key or the pseudorandom numbers used to secure the biometric data of a legitimate user (Lumini and Nani, 2007). The use of random projection and fuzzy vault (Zhu et al., 2012; Liu et al., 2014) to create hybrid schemes has security limitations. This is because the outer vault can be unlocked by an attacker who knows the secret key.

The inverse of the projection matrix can be computed and the original template recovered from the transformed version. Similar limitations are found in approaches based on linear projection and fuzzy vault (Nguyen et al., 2016) as well as random orthonormal projection and fuzzy commitment scheme (Nguyen et al., 2015). Integrating periodic function transform and fuzzy vault provides improved security and user privacy. However, the inner functional transform is susceptible to dictionary attack (Shin et al., 2009) and the outer fuzzy vault can be cracked if an attacker knows the secret key. The integration of fuzzy commitment scheme and chaotic system (Wang et al., 2015) has some limitations despite the improvements in template security and user privacy. This is because chaotic scheme is susceptible to known plaintext attack (Li, 2016) and fuzzy vault can be compromised if an attacker knows the random secret and the only in the security and privacy of a hybrid scheme.

Some previous hybrid techniques (Bringer et al., 2008; Ao and Li, 2009; Chafia et al., 2010; Wu and Yuan, 2010; Feng et al., 2010; Ghany et al., 2012; Liu et al., 2014; Wang et al., 2015) provide information on recognition accuracy but not on security. Other approaches (Meenakshi and Padmavathi, 2010; Filho et al., 2012; Nasir and Kuppuswamy, 2013; Le et al., 2014) analyze the security of the proposed techniques without providing detailed information on the recognition accuracy. Three other works (Butt and Damer, 2014; Nguyen et al., 2015; Dahake and Nimbhorkar, 2015) do not provide information on the recognition accuracy and security of the proposed techniques. This makes it difficult to access the suitability of the proposed approaches for practical situations.

Researches in biometric cryptosystem have focused mainly on template protection and user privacy. The studies have not addressed other important issues such as spoofing. An impostor who obtains fake version of the biometrics of a genuine user can evade the authentication mechanism and gain unauthorized access to the system. We suggest that researchers devote attention to the integration of anti-spoofing methods in existing and future biometric cryptosystems. This will add an extra layer of security and prevent impostors from using fake versions of biometrics to fool the authentication system.

An authorized user who gains legitimate access to the system could intentionally hand over his session to an intruder or may be tricked or coerced to do so. It is important that biometric cryptosystems have means of verifying the identity of a user during an entire working session. This is known as continuous authentication (Brocardo et al., 2014). Existing and future implementations of biometric cryptosystems can use this technique to prevent impostors from hijacking the sessions of genuine users and discourage unscrupulous users from handing over their session to illegitimate persons.

Biometric cryptosystems generally have shorter key lengths than conventional cryptographic algorithms such as RSA, AES and Triple DES. This makes many implementations of biometric cryptosystem susceptible to brute-force attack. Research efforts should focus on developing biometric cryptosystems with long key lengths and high entropies that can provide the level of security required for real world environments.

5. Conclusion

This paper explored the current directions and open research issues in cancellable and hybrid biometric cryptosystems. It discussed the benefits and challenges of using biometrics as a means of authentication. It also presented biometric cryptosystems as a suitable solution to the numerous security and privacy challenges faced by the users of biometric authentication systems. The study examined cancellable biometric cryptosystems under two major categories, namely: non-invertible transformation and biometric salting. The article also explored hybrid cryptosystems as a means of providing improved template security and user privacy. Also discussed are discussed the mode of operation, strengths and weaknesses of cancellable and hybrid biometric cryptosystems as well as an up-to-date review of previous research works in these fields. Finally, we present the open research issues in biometric cryptosystems. This paper will provide the reader with an understanding of cancelable and hybrid biometric cryptosystems. It will make the reader familiar with previous research works as well as future directions and open research issues in cancelable and hybrid biometric cryptosystems.

Acknowledgment

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

References

Ao M and Li SZ (2009). Near infrared face based biometric key binding. In the International Conference on Biometrics, Springer, Alghero, Italy: 376-385. https://doi.org/10.1007/978-3-642-01793-3_39

Arya KV and Singh S (2012). Generating cancelable fingerprint using drawing code. In the International Conference on Soft Computing for Problem Solving, Springer, India, 189-195. https://doi.org/10.1007/978-81-322-0491-6_18

Bringer J, Chabanne H, and Kindarji B (2008). The best of both worlds: applying secure sketches to cancelable biometrics. Science of Computer Programming, 74(1): 43-51.

Brocardo ML, Traore I, and Woungang I (2014). Toward a framework for continuous authentication using stylometry. In the IEEE 28th International Conference on Advanced Information Networking and Applications, IEEE, Victoria, BC, Canada: 106-115. https://doi.org/10.1109/AINA.2014.18

Butt M and Damer N (2014). Helper data scheme for 2D cancelable face recognition using bloom filters. In the International Conference on Systems, Signals and Image Processing, IEEE, Dubrovnik, Croatia: 271-274.

Chafia F, Salim C, and Farid B (2010). A biometric crypto-system for authentication. In the International Conference on Machine and Web Intelligence, IEEE, Algiers: 434-438. https://doi.org/10.1109/ICMWI.2010.5648101

Chen H and Chen H (2010). A hybrid scheme for securing fingerprint templates. International Journal of Information Security, 9(5): 353-361.

Dahake P and Nimbhorkar S (2015). Hybrid cryptosystem for maintaining image integrity using biometric fingerprint. In the International Conference on Pervasive Computing, IEEE, Pune, India: 1-5. https://doi.org/10.1109/PERVASIVE.2015.7087177

Dang TK, Truong QC, Le TTB, and Truong H (2016). Cancellable fuzzy vault with periodic transformation for biometric template protection. IET Biometrics, 5(3): 229-235.

Farberbock P, Hämmerle-Uhl J, Kaaser D, Pschernig E, and Uhl A (2010). Transforming rectangular and polar iris images to enable cancelable biometrics. In: Campilho A and Kamel M (Eds.), Image analysis and recognition: 276-286. Springer-Verlag, Berlin Heidelberg, Germany.

Feng YC, Yuen PC, and Jain AK (2010). A hybrid approach for generating secure and discriminating face template. IEEE Transactions on Information Forensics and Security, 5(1): 103-117.

Filho OIDL, Bedregal BR, and Canuto AM (2012). An investigation of ensemble systems applied to encrypted and cancellable biometric data. In the International Conference on Artificial Neural Networks, Springer, Lausanne, Switzerland: 180-188. https://doi.org/10.1007/978-3-642-33266-1_23

Ghany KKA, Hefny HA, Hassanien AE, and Ghali NI (2012). A hybrid approach for biometric template security. In the 2012 International Conference on Advances in Social Networks Analysis and Mining, IEEE Computer Society, Washington, DC, USA: 941-942. https://doi.org/10.1109/ASONAM.2012.167

Grassi M and Faundez-Zanuy M (2009). Protecting DCT templates for a face verification system by means of pseudo-random permutations. In: Cabestany J, Sandoval F, Prieto A, and Corchado-Rodríguez JM (Eds.), Bio-inspired systems: computational and ambient intelligence: 1216-1223. Springer-Verlag, Berlin Heidelberg, Germany.

Hammerle-Uhl J, Pschernig E, and Uhl A (2009). Cancelable iris biometrics using block re-mapping and image warping. In the 12th International Conference on Information Security, Springer, Pisa, Italy, 9: 135-142.

Jeong M and Teoh ABJ (2010). Cancellable face biometrics system by combining independent component analysis coefficients. In the International Workshop on Computational Forensics, Springer, Tokyo, Japan: 78-87. https://doi.org/10.1007/978-3-642-19376-7_7

Jin Z and Teoh ABJ (2015). Construct a new fixed-length binary fingerprint representation using kernelized local-sensitive hashing. In the 10th IEEE Conference on Industrial Electronics and Applications, IEEE, Auckland, New Zealand: 296-301. https://doi.org/10.1109/ICIEA.2015.7334128

Kaur H and Khanna P (2017). Cancelable features using log-Gabor filters for biometric authentication. Multimedia Tools and Applications, 76(4): 4673–4694.

Khandelwal S and Gupta PC (2015). Implementation of secure biometric fuzzy vault using personal image identification. In the Emerging ICT for Bridging the Future-Proceedings of the 49th Annual Convention of the Computer Society of India, Springer, 1: 311-319. https://doi.org/10.1007/978-3-319-13728-5_35

Kim Y and Toh KA (2007). A method to enhance face biometric security. In the First IEEE International Conference on Biometrics: Theory, Applications, and Systems, IEEE, Crystal City, VA, USA: 1-6. https://doi.org/10.1109/BTAS.2007.4401913

Kong A, Cheunga KH, Zhang D, Kamel M, and You J (2006). An analysis of biohashing and its variants. Pattern Recognition, 39(7): 1359-1368.

Lalithamani N and Soman KP (2009). An efficient approach for non-invertible cryptographic key generation from cancelable fingerprint biometrics. In the International Conference on Advances in Recent Technologies in Communication and Computing, IEEE, Kottayam, Kerala, India: 47-52. https://doi.org/10.1109/ARTCom.2009.193

Latif EB, Wilbowo S, Wasimi S and Tareef A (2017). A hybrid encryption/hiding method for secure transmission of biometric data in multimodal authentication system. Multimedia Tools and Applications: 1-19. Springer Science+Business Media, New York, USA. https://doi.org/10.1007/s11042-016-4280-7

Le TTB, Dang TK, Truong QC, and Nguyen TAT (2014). Protecting biometric features by periodic function-based transformation and fuzzy vault. In: Hameurlain A., Küng J., Wagner R, Dang T, and Thoai N (Eds.), Transactions on Large-Scale Data- and Knowledge-Centered Systems XVI. Lecture Notes in Computer Science, 8960. Springer, Berlin, Heidelberg, Germany. https://doi.org/10.1007/978-3-662-45947-8_5

Lee Y, Chung Y, and Moon K (2009). Inverse operation and preimage attack on biohashing. In the IEEE Workshop on Computational Intelligence in Biometrics: Theory, Algorithms, and Applications, IEEE, Nashville, USA: 92-97. https://doi.org/10.1109/CIB.2009.4925692

Li C and Hu J (2016). A security-enhanced alignment-free fuzzy vault-based cryptosystem using pair-polar minutiae structures. IEEE Transactions on Information Forensic and Security, 11(3): 543-555.

Li CT (2016). A secure chaotic maps-based privacy-protection scheme for multi-server environments. Security and Communication Networks, 9(14): 2276–2290.

Lin J and Gunopulos D (2003) Dimensionality reduction by random projection and latent semantic indexing. In the Text Mining Workshop at the 3rd SIAM International Conference on Data Mining, SIAM: 1-10.

Liu H, Sun D, Xiong K, and Qiu Z (2014). A hybrid approach to protect palmprint templates. The Scientific World Journal, 2014: Article ID 686754, 9 pages. https://doi.org/10.1155/2014/686754

Lumini A and Nanni L (2007). An improved biohashing for human authentication. Pattern Recognition, 40(3): 1057-1065.

Maiorana E, Campisi P, and Neri A (2011). Bioconvolving: Cancelable templates for a multi-biometrics signature recognition system. In the IEEE International Systems Conference, IEEE, Montreal, QC, Canada: 495-500. https://doi.org/10.1109/SYSCON.2011.5929064

Meenakshi VS and Padmavathi G (2010). Security analysis of hardened multimodal biometric fuzzy vault with combined feature points extracted from fingerprint, iris and retina for high security applications. Procedia Computer Science, 2: 195-206.

Moujahdi C, Ghouzali S, Mikram M, Rziza M, and Bebis G (2012). Spiral cube for biometric template protection. In the International Conference on Image and Signal Processing, Springer, Trois-Rivières, QC, Canada: 235-244. https://doi.org/10.1007/978-3-642-31254-0_27

Nagar A and Jain AK (2009). On the security of non-invertible fingerprint template transforms. In the First IEEE International Workshop on Information Forensics and Security, IEEE, London, UK: 81-85. https://doi.org/10.1109/WIFS.2009.5386477

Nagar A, Nandakumar K, and Jain AK (2010). A hybrid biometric cryptosystem for securing fingerprint minutiae templates. Pattern Recognition Letters, 31(8): 733-741.

Narayanan R and Subramanian K (2011). An efficient secure biometric system with non-invertible gabor-transform. International Journal of Computer Science Issues, 8(5): 170-175.

Nasir MS and Kuppuswamy P (2013). Implementation of biometric security using hybrid combination of RSA and simple symmetric key algorithm. International Journal of Innovative Research in Computer and Communication Engineering, 1(8): 1741-1748.

Nguyen MT, Truong TK, and Dang TK (2016). Enhance fuzzy vault security using nonrandom chaff point generator. Information Processing Letters, 116(1): 53-64.

Nguyen TAT, Nguyen DT, and Dang TK (2015). A multi-factor biometric based remote authentication using fuzzy commitment and non-invertible transformation. In the Information and Communication Technology - EurAsia Conference, Springer, Cham, Switzerland: 77-88. https://doi.org/10.1007/978-3-319-24315-3_8

Ouda O, Tsumura N, and Nakaguchi T (2010). Tokenless cancelable biometrics scheme for protecting iris codes. In the 20th International Conference on Pattern Recognition, IEEE, Istanbul, Turkey: 882-885. https://doi.org/10.1109/ICPR.2010.222

Quan F, Fei S, Anni C, and Feifei Z (2008). Cracking cancelable fingerprint template of Ratha. In the International Conference on Computer Science and Computational Technology, IEEE, Shanghai, China, 2: 572-575. https://doi.org/10.1109/ISCSCT.2008.226

Ratha N, Connell J, Bolle RM, and Chikkerur S (2006). Cancelable biometrics: A case study in fingerprints. In the 18th International Conference on Pattern Recognition, IEEE, Hong Kong, China, 4: 370-373. https://doi.org/10.1109/ICPR.2006.353

Ratha NK, Connell JH, and Bolle RM (2001). Enhancing security and privacy in biometrics-based authentication systems. IBM Systems Journal, 40(3): 614-634.

Ratha NK, Connell JH, Bolle RM, and Chikkerur, S (2007). Generating cancellable fingerprints templates. IEEE Transactions on Pattern Analysis and Machine Intelligence, 29(4): 561-572.

Rathgeb C and Uhl A (2010). Secure iris recognition based on local intensity variations. In: Campilho A and Kamel M (Eds.), Image analysis and recognition: 266-275. Springer-Verlag, Berlin Heidelberg, Germany.

Rathgeb C, Breitinger F, Busch C, and Baier H (2014). On the application of bloom filters to iris biometrics. IET Biometrics, 3(4): 207-218.

Rathgeb C, Uhl A, and Wild P (2012). Iris biometrics: from segmentation to template security. Springer New York, USA.

Safie SI, Nurfazira H, Azavitra Z, Soraghan JJ, and Petropoulakis L (2014). Pulse active transform (PAT): A non-invertible transformation with application to ECG biometric authentication. In the IEEE Region 10 Conference, IEEE, Kuala Lumpur, Malaysia: 667-671. https://doi.org/10.1109/TENCONSpring.2014.6863117

Sandhya M and Prasad MVNK (2016). Multi-algorithmic cancelable fingerprint template generation based on weighted sum rule and T-operators. Pattern Analysis and Applications: 1-16. https://doi.org/10.1007/s10044-016-0584-5

Sandhya M, Prasad MVNK, and Chillarige RR (2016). Generating cancellable fingerprint templates based on delaunay triangle feature set construction. IET Biometrics, 5(2): 131-139.

Savvides M, Kumar BV, and Khosla PK (2004). Cancelable biometric filters for face recognition. In the 17th International Conference on Pattern Recognition, IEEE, Cambridge, UK, 3: 922-925. https://doi.org/10.1109/ICPR.2004.1334679

Shin WK, Lee MK, Moon D, and Moon K (2009). Dictionary attack on functional-based cancelable fingerprint templates. Electronics and Telecommunications Research Institute (ETRI Journal), 31(5): 628-630.

Sree SS and Radha N (2016). Cancellable multimodal biometric user authentication system with fuzzy vault. In the International Conference on Computer Communication and Informatics, IEEE, Coimbatore, India: 1-6. https://doi.org/10.1109/ICCCI.2016.7479931

Teoh AB and Ngo DC (2006). Biophasor: Token supplemented cancellable biometrics. In the 9th International Conference on Control, Automation, Robotics and Vision, IEEE, Singapore, Singapore: 1-5. https://doi.org/10.1109/ICARCV.2006.345404

Teoh ABJ and Yuang CT (2007). Cancelable biometrics realization with multispace random projections. IEEE Transactions on System, Man and Cybernetics, Part B, 37(5): 1096-1106.

Vo TTL, Dang TK, and Küng J (2014). A hash-based index method for securing biometric fuzzy vaults. In the International Conference on Trust, Privacy and Security in Digital Business, Springer, Cham, Switzerland: 60-71. https://doi.org/10.1007/978-3-319-09770-1_6

Wang N, Li Q, El-Latif AAA, Peng J, Yan X, and Niu X (2015). A novel protection scheme for multibiometrics based on fuzzy commitment and chaotic system. Signal, Image and Video Processing, 9(1): 99-109.

Wang S and Hu J (2013). A hadamard transformed-based method for the design of cancellable fingerprint templates. In the 6th International Congress on Image and Signal Processing, IEEE, Hangzhou, China, 3: 1682-1687. https://doi.org/10.1109/CISP.2013.6743947

Wu L and Yuan S (2010). A face based fuzzy vault scheme for secure online authentication. In the Second International Conference on Data, Privacy and E-Commerce, IEEE, Buffalo, NY, USA: 45-49. https://doi.org/10.1109/ISDPE.2010.13

Wu Z, Liang B, You L, Jian Z, and Li J (2016). High-dimensional space projection-based biometric encryption for fingerprint with fuzzy minuatia. Soft Computing, 20(12): 4907-4918.

Xu W, He Q, Li Y, and Li T (2008). Cancellable voiceprint templates based on knowledge signatures. In the 2008 International Symposium on Electronic Commerce and Security, IEEE, Guangzhou, China: 412-415. https://doi.org/10.1109/ISECS.2008.100

Yang W, Hu J, and Wang S (2013). A finger-vein based cancellable bio-cryptosystem. In the International Conference on Network and System Security, Springer, Helsinki, Finland: 784-790. https://doi.org/10.1007/978-3-642-38631-2_71

Yang Y, Yu J, Zhang Q, and Meng F (2015). Improved hash functions for cancelable fingerprint encryption schemes. Wireless Personal Communications, 84(1): 643–669.

Zhu HH, He QH, and Li YX (2012). A two-step hybrid approach for voiceprint-biometric template protection. In the International Conference on Machine Learning and

Cybernetics, IEEE, Xian, China, 2: 560-565. https://doi.org/10.1109/ICMLC.2012.6358984

Zuo J, Ratha NK, and Connell JH (2008). Cancelable iris biometric. In the 19th International Conference on Pattern Recognition, IEEE, Tampa, USA: 1-4. https://doi.org/10.1109/ICPR.2008.4761886