Journal of Biometrics & Biostatistics
ISSN: 2155-6180

Mamatha, J Biom Biostat 2018, 9:2
DOI: 10.4172/2155-6180.1000398

Review Article Open Access

A Review of Cancelable Biometric Authentication Methods

Mamatha R*

Information Science and Engineering, BMS College of Engineering, Bangalore, India

Abstract

Biometric analysis for identity verification is becoming a widespread reality. Such implementations necessitate large scale capture and storage of biometric data, which raises serious issues in terms of data privacy and identity theft. Unlike credit cards and passwords, which can be revoked and reissued when compromised, biometrics are permanently associated with a user and cannot be replaced. In order to prevent the theft of biometric patterns, it is desired to modify them through revocable and non-invertible transformations to produce Cancelable biometric templates. This paper provides a review of the state of the art of different methods of biometric based authentication schemes and cancelable biometric systems.

Keywords: Biometrics; Cancelable biometric templates; Random projection

Introduction

The biometric attribute possessed by every individual measure distinctive and has the potential to acknowledge. Therefore, biometrics is used for authentication or recognition for many critical applications like access control, border control, immigration, forensic and law enforcement. Biometric authentication [1,2] system provides better security compared to password or token based authentication system. However, compromise of the stored templates is a critical problem in biometric system. Biometric spoofs can be created by an adversary for stolen template which can be used to have legitimate access to systems that employ the same biometric trait of the user. While knowledge can be forgotten and tokens can be lost or stolen, biometrics do not suffer from these deficiencies and can provide the security of long passwords without sacrificing the ease of memorizing short ones.

Biometric traits can be divided into Physiological, behavioral and both physiological and behavioral modalities. Physiological modality includes Face, fingerprint, Hand geometry, Iris, Retina, Vein, Ear shape which deals with the body shape which are shown in Figure 1. In face recognition, the spatial geometry like shape, size, the structure of the face is reflected as structures to recognize a person. Facial recognition is one of the popular way of recognizing the individuals. A person is identified based on the pattern of ridges, minutiae points in case of fingerprint biometrics. Hand geometry recognition measures the physical structure of the hand including size, length, width, shape of finger, distance between fingers etc. Pigmented portion of the eye is Iris that remains same throughout the life.

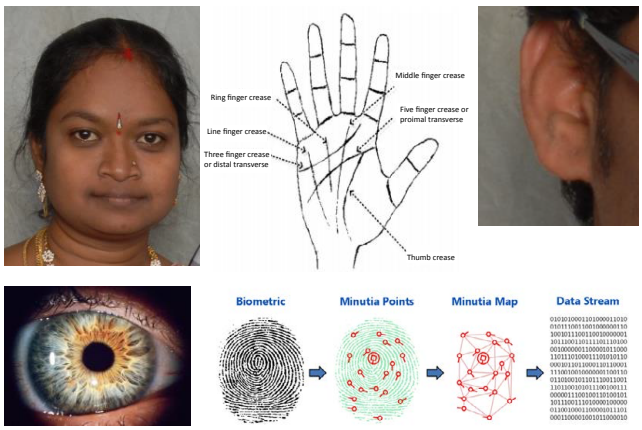

Figure 1: Physiological cancelable biometric modalities.

Human behaviour is related to behavioral modalities such as Signature and Key stroke pattern as shown in Figure 2. A unique writing style of every person identifies a person using the dynamic signature that deals with the speed, the direction of writing, pressure applied while writing, time taken to finish the signature. Keystroke dynamics practices the time taken to type particular word; time, speed and pressure while hitting the keys. Figure 3 displays Voice and brain waves

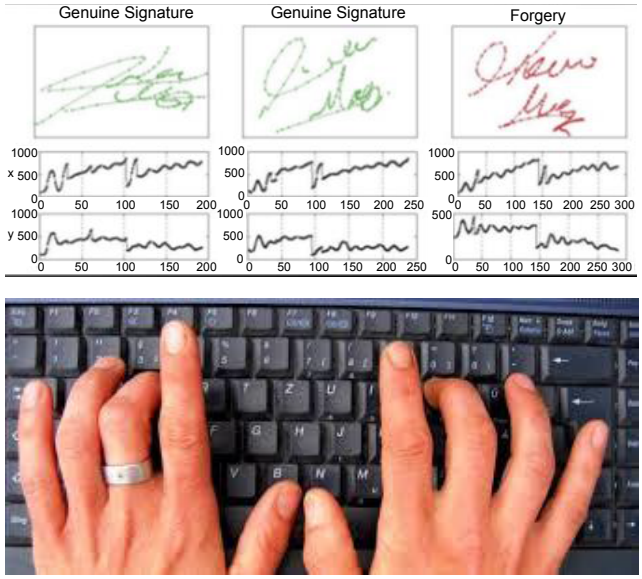

Figure 2: Behavioral cancelable biometric modalities.

***Corresponding author:** Mamatha R, Information Science and Engineering, BMS College of Engineering, Bangalore, India, Tel: +918026622130; E-mail: krm.ise@bmsce.ac.in

Received March 12, 2018; **Accepted** April 03, 2018; **Published** April 09, 2018

Citation: Mamatha R (2018) A Review of Cancelable Biometric Authentication Methods. J Biom Biostat 9: 398. doi: 10.4172/2155-6180.1000398

Figure 3: Both biometric physiological and behavioral cancelable modalities.

(EEG) traits which act as both physiological and behavioral. Voice recognition is a popular method for authentication which ascertains the vocal characteristic of the individual. ElectroEncephaloGraphy (EEG) is an emerging biometric trait to authenticate a person which offers high security and accuracy. This system captures the brain waves by electrodes and identifies unique brain signals stimulated by the given task.

To overcome the problem of stolen biometrics, the researchers have developed the template protection schemes. Different techniques have been aimed to expand the security of biometric templates as shown in Figure 4. The hardware based approach involves a closed recognition system, where the biometric never leaves a physically secure module such as a smart card or a hand-held device. Such a device matches the input biometric trait with the template stored in the device and releases a key in case of successful authentication. Software based solutions for template protection store a modified version of the template that reveals as little information about the original biometric trait as possible and yet can be successfully used for verification.

The software-based solutions can be classified into two main categories: template or feature transformation and biometric cryptosystem. Template transformation techniques transform the biometric template based on parameters derived from external information such as user passwords or keys [3]. Biometric cryptosystems [4,5] attempt to obtain error correcting information from biometric features which is known as helper data. The helper data does not reveal significant information about the biometric or the key. The extracted biometric features are combined with tokenized random number to create the transformed template in biohashing scheme which is an extended version of Random projection method. The biometric features are extracted using Wavelet and Fourier transformation to generate feature vector.

Cancelable biometrics [6-8] stores a transformed version of the biometric data. The transformation is one way and so knowledge of a transformed biometric does not leak information about the actual biometric data. Moreover, by using different cancellable templates, data belonging to the same user cannot be linked.

Many research works have been done in the field of canelable biometrics. Among all biometric modalities face, fingerprints and Iris are most popular for biometric authentication system. Concept of cancelable biometrics was first provided by Ratha et al. [8]. Three transformation functions provided by them are Cartesian, polar and surface folding transformation for fingerprint template [9]. Cancelable biometric template generation for multimodal biometric system (Face and Ear) is first provided by Paul et al. A pin based cancellable biometrics for fingerprint template is provided by Lacharme. Pillai et al. provided sectored random projection for cancellable iris biometrics [10].

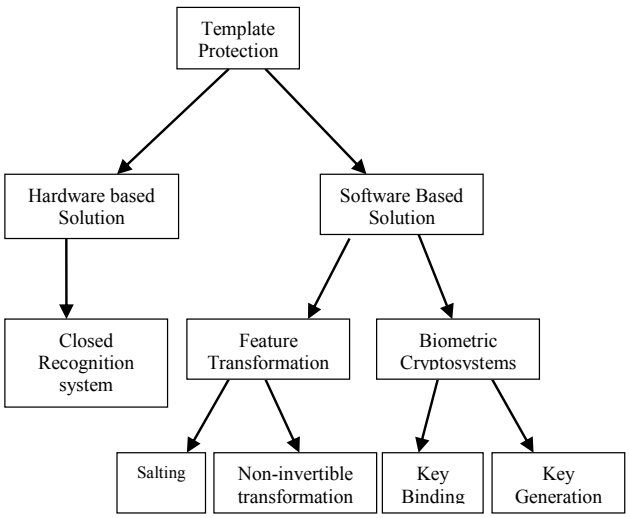

Figure 4: Different categories of template protection schemes.

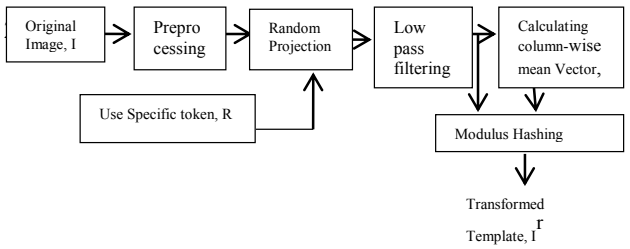

Figure 5: Block diagram of cancellable template generation.

Challenging concepts of cancelable biometrics verification

There are 4 principal criteria to be fulfilled before a cancelable biometric template can be considered useful:

Diversity: The same cancelable template cannot be employed in two different applications.

Reusability: Straightforward revocation and reissue in the occurrence of compromise.

One-way transformation: Non-invertibility of template computation to avoid recovery of secret biometric data.

Performance: The recognition performance should not be deteriorated by the formulation.

Image acquisition and feature extraction

Cancelable biometric templates are produced by projection of biometric template on random matrix in which columns are normally distributed Gaussian vectors followed by a one-way modulus hashing. One of the powerful dimensionality reduction tool is Gaussian random projection. Block diagram of the algorithm is shown in Figure 5.

In first step, columns of a raw biometric gray scale image are stored as a set of N, d-dimensional vectors $I \in R^d$. It can be represented in matrix form as I_{dXN}. The image is pre-processed from the sample followed by illumination enhancement as in step two. In third step a set of k-dimensional normally distributed random vectors are generated. Acquired biometric data image matrix I is projected on the Gaussian random matrix R in step four. In fifth step Low pass Gaussian filter is

applied to smoothen the image. The columnwise mean of the projected matrix is calculated and stored in a vector in step six. Compute modulus separately for each j^{th} column of the projected template using vector M in step seven. In the last step, approximate the fractional values of the elements of I^T towards positive infinity.

DWT and DFT methods can be used to extract features from the EEG signals. The signal is broken down into its constituent sinusoids of different frequencies using DFT. DWT [9] breaks the signal into wavelets using scaled and shifted versions of a mother wavelet. Wavelet properties of temporal localization and Fourier's frequency localization make them an ideal combination for extracting properties of EEG.

FFT is an efficient algorithm for computing the DFT of a sequence in which time domain signal of each channel was converted into the frequency domain. The standard EEG frequency bands obtained are:

Delta () – rhythmic activity between 1 and 4 Hz

Theta ( ) – rhythmic activity bet ween 4 and 8 Hz

Aplha ( ) – rhythmic activity between 8 and 12 Hz

Beta ( ) – rhythmic activity between 12 and 30 Hz

Gamma ( ) – rhythmic activity between 30 and 40 Hz.

Therefore, the FFT feature vector consisted of five features for an electrode. Process of obtaining DFT features of subject classification for the authentication process is revealed in Figure 6.

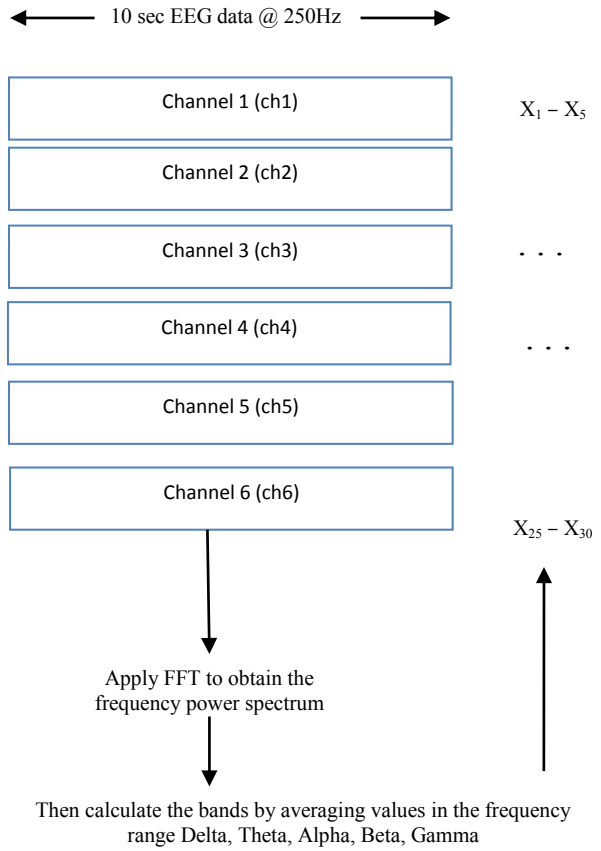

Figure 6: Process of FFT feature extraction.

Daubechies family of wavelets are used to create robust features for the classification as shown in Figure 5. This figure shows sequential application of filters to decompose the signal into its detail and approximate coefficients. Discrete Wavelet Transform (DWT) provides a time frequency representation of the signal and the Daubechies wavelets irregular shape and compact nature help in analysing signals with sharp edges (Figure 7).

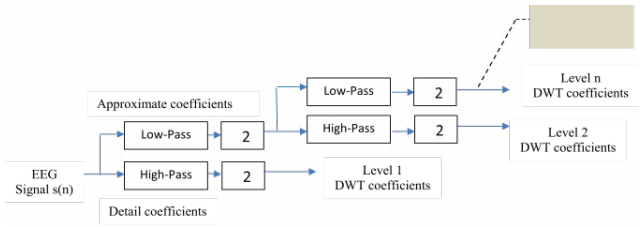

Figure 7: Decomposition structure of Discrete wavelet transform.

Multi Line Code (MLC) is a minutia descriptor constructed based on multiple lines centered at minutia itself. Suppose $Pr(x_r,y_r,\Theta_r)$ and the neighbor minutiae be $P_{(j)}(x_{(j)},y_{(j)}, \Theta_{(j)})$ for j belongs to $[1,N_{m-1}]$ and N_m is the total number of minutiae in the fingerprint. KPCA principle is employed to extract a fixed-length feature vector from originally unordered and variable-size template and introduce a specially designed kernel function. The technique of kernel substitution is a way of observing an arbitrary mapping from the data space $\{x_{(k)}\}$ $(x_{(k)} \in R_m)$ into the feature space $\{\emptyset(x_{(k)}\}(\{\emptyset_{(x(k)}\}) \in R_{m'}$ without having to compute the mapping explicitly, where N is the number of data observation and $k \in [1,N]$. Combining the kernel trick with PCA obtains a non-linear generalization of PCA called KPCA.

One of the powerful dimensionality reduction tool is Random Projection (RP). Key concept of RP [10-13] arises from Johnson and Linden Strauss Lemma (JL lemma). This lemma states that a set of p points in a high dimensional Euclidean space can be mapped down onto a k-dimensional subspace (k ≥ O (logp/epsilon square) such that the distances between the points are approximately preserved. Using matrix notation, the original data can be represented as Y_{pxN}, which can be considered as a set of N observations of dimension-p. Its projection on k-dimensional random subspace (k<<p) is denoted as $Y_{kxN}^{RP}=R_{kxp}Y_{pxN}$, where R is random k x p matrix whose columns has unit norm and Y^{RP} is the projection of Y in lower dimensional subspace.

The essential property of the projection matrix in JL lemma is that its column vectors r_i belongs to R are required to be orthogonal to each other. Number of researchers used Random Projection for Cancelable biometric system [14].

Principal Component Analysis (PCA) is one of the feature extraction methods which operate directly on image matrix. Let X_i (i=1,2,….n number of training samples) be p-by-q image matrices which are reshaped into vectors $X_i R^{PQ \times 1}$ and stacked as $T=[x_1,x_2,….x_n]$. Consider a linear projection $Y=U^TT$ which maps the pq-dimensional data set T in image space onto a d-dimensional feature space $U=[u_1,u_2,…u_d]$, where U belongs to R^{pqxd} and pq>>d. The goal behind principal components analysis is to find the best projection vectors U that maximizes the determinant of a total scatter matrix across all the image samples. The covariance matrix G_{PCA} is given by:

$$G_{PCA}=\sum_{i=1}^{n}(x_i-m)(x_i-m)^T.$$

Where G_{PCA} belongs to R^{pqxpq}, m=(1/n) $\sum_{i=1}^{n} x_i$ is a sample mean of training set and T denotes a transpose.

The iris image, p € R^N, is transformed to an N dimensional Gabor vector g, where N is the number of pixels containing the iris. The iris feature vector g, is then projected onto a random subspace by a random n X N matrix Ψ, where n ≤ N. This process can be described as y=Ψg, where y is the n dimensional Random Projection vector.

Stages of verification

Two phases of biometric authentication are enrolment and verification. Enrolment involves measuring an individual's biometric data for the construction of a biometric template. Verification involves a measurement of the same data and comparison with the stored template.

Enrolment, Authentication and key generation are the three phases of cancelable Neurokey generation scheme [15] as shown in Figure 8. In enrolment phase, an individual establishes the authentic regions of the EEG features for a chosen activity using the training samples. These regions are stored as a template to authenticate later. Using classic biometric approach the system will authenticate a subject in second phase. Key generation phase accepts the EEG signals of the established mental activity and generates the feature vectors after appropriate feature selection.

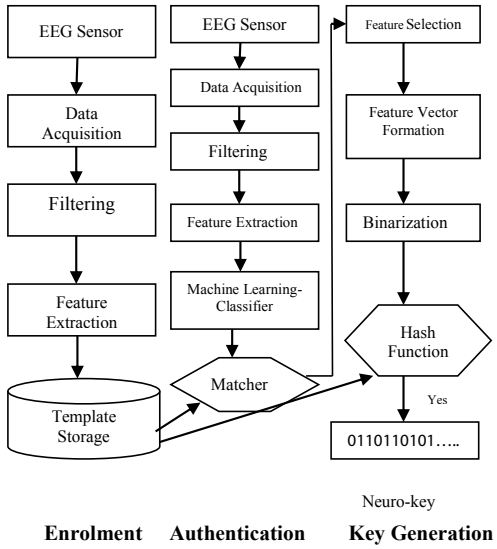

Figure 8: Flow of key generation from EEG.

Cancelable biometric verification methods

Two classification models such as Support Vector machine and Bayesian networks are used as classifiers. Principal Component Analysis (PCA) and Linear Discriminant Analysis (LDA), Vertical 2DPCA (V2DPCA) and Horizontal 2D PCA (H2DPCA), Support Vector Machine are some of the other classifiers.

Support vector machine (SVM) is used as a classifier because of its accuracy and ability to separate the classes using the concept of hyper plane separation to the data, mapping the predictors onto a new, higher-dimensional space in which they can be separated linearly. The performance metrics were compared with Bayesian network classifier. Once the classification was performed, the results were analyzed and performances were compared using the following metrics.

$$\text{Accuracy} = \frac{P+Q}{P+Q+R+S}$$

$$\text{Precision} \quad \overline{P \quad R}$$

$$\text{Recall} = \frac{P}{P+S}.$$

Where P is True Positive, Q is True Negative, R is False Positive and S is False Negative.

Horizontal 2D PCA performs PCA directly on the image matrix. H2DPCA finds most discriminative projection vectors for a linear projection. This horizontal 2DPCA works only in the horizontal (row) direction of the image matrix. As an alternative to H2DPCA, vertical 2DPCA takes a transposed face image matrix as input and then image covariance matrix is written in a form as shown in Figure 9.

Registration-Based Cancelable Biometrics

Registration-based methods need to locate singular points in fingerprint images and then translate minutiae with respect to the singular point. The image pre-alignment process can cause considerable singular point alteration and produce a non-negligible number of fake minutiae. Gaussian random projection works with existing matcher which uses a signal transformation technique.

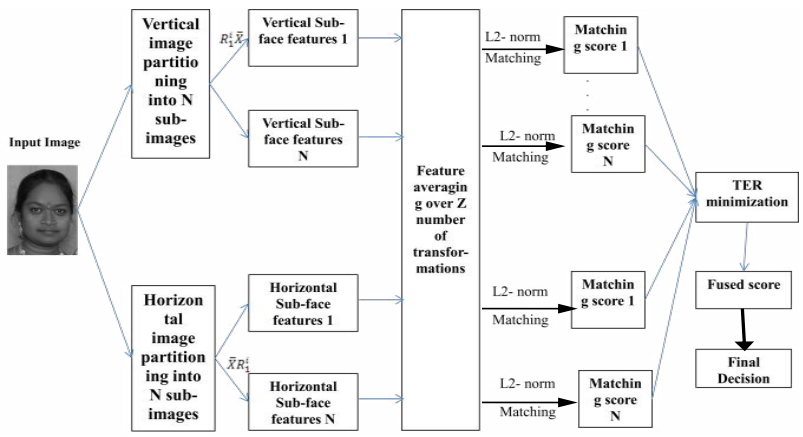

Figure 9: An overview for thepR1 and pR2 projections.

Neurokey

Brainwaves (EEG) can be used for providing authentication as in by Garima et al. [15]. Exploiting the brain as a biometric physical unclonable function, a unique key is generated from a user's EEG signal. The approach of cancelable biometrics was implemented by altering user's thoughts. The experiment carried on the Dataset1 and Dataset2 of Neurodynamics Laboratory at the state University of New York Health Centre at Brooklyn, USA shows that Accuracy is 96.2 in Support Vector Machine and 98.45 in Bayesian Network. In case of compromise of biometric, the neurokey can be changed by performing a different cognitive task. As an enhancement, hybrid algorithms for feature mapping to binary code words can be done.

Gaussian random projection

Projection of biometric template on random matrix followed by one-way modulus hashing produces cancelable biometric templates [16]. Random matrix columns are normally distributed vectors which have zero mean and unit variance. One of the powerful dimensional reduction tool is Random Projection which states that a set of d points in a high Euclidian space can be mapped down onto a k-dimensional subspace such that the distances between the points are approximately preserved. The performance evaluated on three standard facial databases, ORL, Indian face database and Extended Yale Face Database 8 expresses the EER of 0.00%, 0.03% and 0.12% [17].

Embedded authentication based on fingerprint and chaotic encryption

Escobar et al. [18] suggested a fingerprint template protection based on chaotic encryption. The scheme uses an embedded authentication system based on a 32-bit microcontroller. A new authorized user can register in the embedded system with a fingerprint. 32-bit microcontroller M52259 of Freescale, fingerprint reader module Futronic FS83 and human interface were used in the authentication system. Infrared LED technology is used in fingerprint scanning. Encryption algorithm based on Murillo-Escobar et al. was used. Based on fingerprint module Furtonic FS83 specifications, the authentication system has the fingerprint recognition accuracy of FAR 10^6 and FRR 10^2. As an enhancement, security and performance capabilities in an embedded expert system can be increased. Other real-time monitoring schemes such as thermal sensing, heart rate sensing, pulse rate sensing could be implemented to determine if an authorized live person is using the system or not [19-21].

Extraction of partial face features for cancelable identity verification

Seok et al. [21] use partial face image matrix to extract localized random features for cancellable identity verification. Partial face image features extracted on two directional projection i.e., on horizontal and vertical facial features. Cancelable face template was generated by taking an average of each directional features over n number of features. Extensive experiments conducted on AR, BERC, AT and T, Sheffield and FERET database shows that Sheffield database outperforms.

Alignment-Free Cancelable Biometrics

Accurate detection of singular points in Registration- based methods is hard to achieve due to noisy and rotated fingerprint images. Also matching error may occur due to registration error. It is hard to define the core point in arch and tented-arch fingerprint patterns. To overcome these issues, numerous alignment free methods have been devised in the literature. No image registration is required in registration-free methods. Rotation and shift invariant relationship between minutiae points is exploited to generate fingerprint templates.

Kernel PCA enabled bit-string representation

Wong et al. [22] developed minutiae descriptor called Multi Line Code (MLC) which is used for fixed-length binary cancelable fingerprint template generation. An unordered and variable-size MLC template is transformed using kernel principal components analysis (KPCA) into an ordered and fixed-length bit-string. Some FVC datasets such as FVC2002DB1, FVC2002DB2, FVC2004DB1, FVC2004DB2 were used for the experiment and 1.61% was the obtained equal-error rate (EER) for the final bit string. Masquerade attack was possible in case of compromise of certain information required for KPCA.

A blind system identification approach

Wang et al. [23] extend a blind system identification approach to the development of alignment free cancelable fingerprint templates. The algorithm considers the frequency samples of binary string as input which is derived from quantized pair-minutiae vectors. Frequency samples of binary string are protected in their method instead of protecting the binary string directly. As long as the binary string is safe, the original fingerprint data will not be at risk. Evaluation of this method carried over FVC2002 DB1, DB2 and DB3 shows that EER rate for the stolen-key scenario is 4%, 3% and 8.5% only when compared to other state-of-the-are alignment-free cancelable biometrics.

Sectored random projections

Cancelable Iris Biometric system first quotes the iris pattern of the user, Gabor features are figured later, a different Random Projection is applied for each application afterwards and finally the new pattern is transferred to the application database [24]. N dimensional feature vectors are embedded in a lower dimension n in random projection. The user's iris pattern cannot be generated in case of compromise because of dimensionality reduction caused by projection. Experiments carried on MMU dataset shows that recognition rate of 97.7% are higher than salting methods. The algorithm is robust for degradations due to eyelids and eyelashes.

Curtailed circular convolution

Process of registering fingerprint images with respect to core and delta points is relinquished by constructing transformed templates based on pair-minutiae vectors as in Wang and Hu [25]. Core transformation in the design of cancelable templates uses a fundamental transform analysis of Linear Time-invariant systems. A binary string is generated by quantizing and bin-indexing pair-minutiae vectors. The scheme has strong security when both transformed template and parameter key are compromised. Experiment carried on FVC 2002 database has EER of 2% compared to other existing alignment-free cancellable fingerprint templates [26-32]. Summary of the above methods is given in Table 1.

	Accuracy	EER	FAR	FRR
Neurokey	96.2%	-	-	-
Gaussian Random Projection	-	0.03%	-	-
Chaotic encryption	-	-	10^6	10^2
Blind system	-	4%	-	
Sectored random projection	97.7%	-	-	-
Curtailed circular convolution	-	2%	-	-

Table 1: Summary.

Conclusion

The transformation management in cancelable biometrics is equivalent to key management in information security. The original biometrics signal is not required to be retained as both enrolment and authentication is carried out using the transformed biometrics in cancelable biometrics. In this survey, we have discussed about popular and emerging biometric traits which can be used for user authentication. In this paper, we have reviewed most of the traditional biometric systems which leads us to the potential cancelable biometric based system. We have also reviewed some of the state-of-the art literatures of cancelable biometrics. This article can be used as basic information provider about traditional and cancellable biometrics, which we hope will help researchers to get encouraged to further research and build a practical cancellable biometric based authentication system. Cancelable biometrics is inspired by the approach which handles biometric variability.

References

1. Jain AK (2004) An introduction to biometric recognition. IEEE Transactions on Circuits and Systems for Video Technology 14: 4-20.
2. Jain AK (2006) Biometrics: A tool for information Security. IEEE Transactions on Information Forensics and Security, pp: 125-143.
3. Teoh A, Goh A, Ngo D (2006) Random multispace quantization as an analytic mechanism for biohashing of biometric and random identity inputs. IEEE Transactions on Pattern Analysis and Machine Intelligence 28: 1892-1901.
4. Uludag U, Pankanti S, Prabhakar S, Jain A (2004) Biometric cryptosystems: issues and challenges. Proceedings of the IEEE 92: 948-960.
5. Lalithamani N, Soman KP (2009) An Efficient Approach for Non-Invertible Cryptographic Key Generation from Cancelable Fingerprint Biometrics. International Conference on Advances in Recent Technologies in Communication and Computing, pp: 47-52.
6. Ratha N, Chikkerur S, Connell J, Bolle R (2007) Generating cancelable fingerprint templates. IEEE Trans Pattern Anal Mach Intell 29: 561-572.
7. Bolle RM, Connel JH, Ratha NK (2002) Biometrics perils and patches. Pattern Recognit 35: 2727-2738.
8. Ratha N, Connell J, Bolle R (2001) Enhancing security and privacy in biometrics-based authentication systems. IBM Syst J 40: 614-634.
9. Hammerle-Uhl J, Pschernig E, Andreas U (2013) Cancelable iris-templates using key-dependent wavelet transforms. International Conference on Biometrics (ICB), pp: 1-8.
10. Pillai JK, Patel VM, Chellappa R, Ratha NK (2010) Sectored random projections for cancelable iris biometrics. Sectored random projections for cancelable iris biometrics. Proc IEEE Int Conf Acoust Speech Signal Process, pp: 1838-1841.
11. Pillai JK, Patel VM, Chellappa R, Ratha NK (2011) Secure and robust iris recognition using random projections and sparse representations. IEEE Trans Pattern Anal Mach Intell 30: 1877-1893.
12. Punithavathi P, Geetha S (2016) Dynamic sectored random projection for cancelable iris template. International Conference on Advances in Computing, Communications and Informatics (ICACCI), pp: 711-715.
13. Patel VM, Chellappa R, Tistarelli M (2010) Sparse representations and Random Projections for robust and cancellable biometrics. 11th International Conference on Control Automation Robotics & Vision (ICARCV), pp: 1-6.
14. Jin Z, Lai YL, Hwang JY, Kim S, Teoh ABJ (2017) Ranking Based Locality Sensitivie Hashing Enabled Cancelable Biometrics:Index of Max Hashing. IEEE Transactions on Information Forensics and Security 13: 393-407.
15. Bajwa G, Dantu R (2016) Neurokey: Towards a new paradigm of cancelable biometrics-based key generation using electroencephalograms. Computers and Security 62: 95-113.
16. Kaur H, Khanna P (2015) Gaussian Random Projection based non-invertible cancelable biometric templates. Procedia Computer Science 54: 661-670.
17. Nazari S, Moin MS, Kanan HR (2014) Cancelable face using Chaos permutation. 7th International Symposium on Telecommunications (IST), pp: 925-928.
18. Escobar MAM, Cruz-Hernandez C, Abundiz-Perez F (2015) A robust embedded biometric authentication system based on fingerprint and chaotic encryption. Expert systems with Applications 42: 8198-8211.
19. Xu D, Wang X (2010) A Scheme for cancelable fingerprint fuzzy vault based on chaotic sequence. 2010 International Conference on Mechatronics and Automation (ICMA), pp: 329-332.
20. Supriya VG, Manjunatha R (2017) Logistic Map for Cancelable biometrics. IOP Conference Series: Materials Science and Engineering 225: 1.
21. Seok B, Toh BA, Choi K, Teoh ABJ (2012) Extraction and fusion partial face features for cancelable identity verification. Pattern Recognit 45: 3288-3303.
22. Wong WJ, Teoh ABJ, Kho YH, Wong MLD (2016) Kernel PCA enabled bit-string representation for Minutiae-based cancelable fingerprint template. Pattern Recognit 51: 197-208.
23. Wang S, Hu J (2016) A blind system identification approach to cancelable fingerprint templates. Pattern Recognit 54: 14-22.
24. Pillai JK, Patel VM, Chellappa R, Ratha NK (2009) Sectored Random Projections for Cancelable Iris Biometrics. Proc IEEE Int Conf Acoust Speech Signal Process.
25. Wang S, Hu J (2014) Design of alignment-free cancelable fingerprint templates via curtailed circular convolution. Pattern Recognit 47: 1321-1329.
26. Paul PP, Gavrilova M (2014) Multimodal Biometrics using Cancelable Feature Fusion. International Conference on Cyberworlds (CW), pp: 279-284.
27. Mraki Y, Furukawa M, Fujiyoshi M, Tonomura Y, Kiya H (2014) A compressible template protection scheme for face recognition based on sparse representation. 22nd Eur Signal Process Conf, pp: 1647-1651.
28. Wong WJ, Wong MLD, Teoh ABJ (2014) A security- and privacy-driven hybrid biometric template protection technique. 2014 International Conference on Electronics, Information and Communications (ICEIC), pp: 1-5.
29. Paul PP, Gavrilova M (2014) Rank Level fusion of multimodal cancelable biometrics. 14 IEEE 13th International Conference on Cognitive Informatics and Cognitive Computing (ICCI*CC), pp: 80-87.
30. Paul PP, Gavrilova M, Klimenko S (2013) Situation Awareness through Multimodal Biometric Template Security in Real Time Environments. International Conference on Cyberworlds, pp: 82-88.
31. Paul PP, Gavrilova M (2013) Novel multimodal template generation algorithm. 12th International Conference on Conginitive Informatics and Cognitive Computing (ICCI*CC), pp: 76-82.
32. Chen X, Zheng L, Liu Z, Zhang J (2014) Privacy-preserving biometrics using matrix random low-rank approximation approach. 2014 International Symposium on Biometrics and Security Technologies (ISBAST), pp: 6-12.