Cancelable Crypto-Biometrics for more sanctuary augmentation

Dr.Kashif Qureshi

Department Of Computer Science, tel: +966 (0)535598451,Jazan University, Jazan, Saudia
Srk1521@gmail.com

Abstract

This paper puts forth a fresh methodology for the secure storage of fingerprint template by generating Secured Feature Matrix and keys for cryptographic techniques applied for data Encryption or Decryption with the aid of cancellable biometric features. Conventional techniques depend on biometric features like face, fingerprint, hand geometry, iris, signature, keystroke, voice and the like for the extraction of key information. If a Biometric Key is missing or stolen, it is lost perpetually and possibly for every application where the biometric is utilized, since a biometric is permanently linked with a user and cannot be altered.

This paper puts forth a fresh methodology for the secure storage of fingerprint template by generating Secured Feature Matrix and keys for cryptographic techniques applied for data Encryption or Decryption with the aid of cancellable biometric features. Conventional techniques depend on biometric features like face, fingerprint, hand geometry, iris, signature, keystroke, voice and the like for the extraction of key information. If a Biometric Key is missing or stolen, it is lost perpetually and possibly for every application where the biometric is utilized, since a biometric is permanently linked with a user and cannot be altered.

Biometric Security Systems have numerous problems because of the fact that the biometric data of a person is stored in the system. These problems would arise when that data is compromised. The standard password based security systems have the ability to cancel the compromised password and reissue a new one. The biometrics cannot be canceled or changed which can be their advantage and a disadvantage in this particular situation. The concept of cancelable biometrics can improve the biometric security system so that it gains the advantages of the password based security system, by not losing the inherent superiority. This paper proposes a novel approach by utilizing cancelable biometric features for securely storing the fingerprint template by generating Secured Feature Matrix and keys for cryptographic techniques applied for data Encryption or Decryption. The conservative techniques rely on biometric features such as face, fingerprint, hand geometry, iris, signature, keystroke, voice, etc for extracting key information. If a Biometric Key is lost or stolen, it is lost forever and perhaps for every application where the biometric is used, because a biometric is enduringly linked with a user and cannot be changed. The use of cancelable biometric features enhances the robustness and reliability of the cryptography technique. There are several biometric systems invented for cryptography, but the proposed cancelable biometric cryptography technique fashions novel biometric systems to generate Cryptographic Key.

Keyword: **Biometrics, Cancelable Biometrics, Cryptography, Key generation, Irrevocable Key, Fingerprint, Minutiae Points, Security Analysis**.

1. Introduction

Biometrics (or biometric authentication)[note 1] refers to the identification of humans by their characteristics or traits. Biometrics is used in computer science as a form of identification and access control. It is also used to identify individuals in groups that are undersurveillance.

Biometric identifiers are the distinctive, measurable characteristics used to label and describe individuals. Biometric identifiers are often categorized as physiological versus behavioral characteristics. A physiological biometric would identify by one's voice, DNA, hand print or behavior. Behavioral biometrics are related to the behavior of a person, including but not limited to: typing rhythm, gait, and voice.[note 2] Some researchers have coined the term behaviometrics to describe the latter class of biometrics.

Generally Biometric Security System consists of two phases. The first phase is enrolment phase, in which the user's biometric template will be acquired. The second phase is authentication phase, in which biometric sample is taken from the user and compared to the biometric template stored in the database. If both of them match, positive authentication is achieved. But the fact is that the biometric data of every user in that system which is stored in a database opens a few potential problems.

- *Identity theft* - There is a possibility that the attacker may steal the biometric data from the database and using that data constructs an artifact can be used to impersonate the original user. The artifact can be an artificial finger, artificial eye, face mask, photography, or something else depending on the type of the biometrics in database.
- *Irrevocability* - The nature of biometric sample is

permanent. And also the user shouldn’t be able to change the template acquired. The fact that biometric templates, once issued, it cannot be reissued, changed or revoked.

- *Disclosure of personal information* - The biometric sample information of any person like genetic origin of a person or existence of some diseases like diabetes or stroke is considered personal and these shouldn’t be revealed to anyone without the person’s consent. Since forcing the user to reveal his personal information is illegal, the use of biometrics should be forbidden.
- *Possibility of use* - Biometric sample should be used only for the purpose it was given for. Any situation in which that scope is overridden is considered an invasion of privacy should be strictly forbidden.

Presently biometric systems use the central biometric template storage. The reason for this central storage can be seen in two different aspects. The first one is that the central template storage place avoids the extra cost and inconveniences of users. The second one is that standardization. Standards would resolve the compatibility problem over different services within the group and enable a possibility for adding a new service to the group.

The centralized storage opens many concerns for users like: Who has the right of usage? Who has the access? How can the user limit someone’s access? But there exist a number of solutions all of which relying on the hiding of biometric template in the storage. One is data encryption. The second is, more secure method called cancelable biometrics.

2. Cancelable Biometrics

Several methods for generating new exclusive biometrics have been proposed. The first fingerprint based cancelable biometric system was designed and developed by Tulyakov et al..Essentially, cancelable biometrics perform a distortion of the biometric image or features before matching. The variability in the distortion parameters provides the cancelable nature of the scheme. Some of the proposed techniques operate using their own recognition engines, such as Teoh et al. and Savvides et al. whereas other methods, such as Dabbah et al., take the advantage of the advancement of the well-established biometric research for their recognition front-end to conduct recognition. Although this increases the restrictions on the protection system, it makes the cancellable templates more accessible for available biometric technologies

Advances in Communication systems have led to enlarged quantity of digital data available in the publicly shared media. This, in turn, has led to, the need for and as a consequence, the rapid growth of cryptographic techniques. One of the elemental building blocks of computer security is cryptography. Cryptographic techniques can be deployed to encode data in such a way that it becomes incoherent to the public or third party, but not to the intended receivers of the data (Data Confidentiality).

The lack of ability of human users to memorize strong cryptographic keys has been an aspect limiting the security of systems for decades. As a result, cryptosystems commonly rely on user-generated passwords, which are simpler to remember, in order to discharge the pseudo-random keys. This is done in view of the fact that there are proofs in the history supporting the fact that one can remember only tiny passwords or keys, and even then tend to desire passwords or keys that are easily guessed by dictionary attacks or acquired using social engineering methods .

We normally write down and store keys in an insecure location, which can be shared between users, and cannot provide an assurance of non-repudiation. Additionally, the majority of people tend to use the same keys or password for a wide range of applications and as a result the infringement of one system can lead to the infringement of many others. This fact eases the job of an ultimate attacker, and hence decreasing the overall security of the data being protected. This drawback can be addressed in a large range of applications by generating strong cryptographic keys from biometric data, perhaps in conjunction with the entry of a password.

Biometrics is concerned with the quantitative data associated with unique behavioral or physiological characteristics of a person. Biometrics is also concerned with methods of validating a person’s uniqueness from one or more behavioral or physiological characteristics. Different biometric techniques are at present under research, including fingerprints, facial, palm prints, retinal and iris scans, and hand geometry, signature capture and vocal characteristics.

One of the problems with biometric techniques is that these are complex to reset. The consistency over time of biometric data is one of its greatest strengths as well as one of its greatest limitations. When a credit card number is missed, the service provider can just assign the customer a new credit card number. When the biometric features are settlement, substitute is not possible. It is obvious, one’s old fingerprint is stolen, and issue of new fingerprint for the same person is not achievable .

In order to ease this problem, we propose the use of the concept of “cancelable biometrics” for the purpose. The procedure deals with planned, repeatable distortion of a biometric signal based on a predefined transform. Distortion of biometric signal is repeated in the same method at each presentation, for enrollment and for every key generation. With this approach, each incidence of enrollment can use a different transform thus make cross matching infeasible. Moreover, if one variant of the transformed biometric data is compromised, then the transform operation can merely be changed to create a new variant for reenrollment as if, essentially, for a new person. Commonly, the transforms used for distortion are selected to be noninvertible. Thus the original (undistorted) biometrics cannot be recovered even if the transform method and the resulting transformed biometric data are known.

3. Associated Work

Our work is inspired from a number of previous works related to cancelable biometrics and the generation of cryptographic key from cancelable biometric features. A brief review of some of the works is given below:

Cancelable biometrics proffers a greater level of privacy by facilitating more that one template for the same biometric data and thus the non-link ability of user's data stored in diverse databases. The measurement of the success of a particular transformation and matching algorithm for fingerprints was described by Russell Ang et al. A key dependant geometric transform was employed on the features obtained from a fingerprint, so as to produce a key-dependent cancelable template for the fingerprint. Besides, they have also studied the performance of an authentication system that utilizes the cancelable fingerprint matching algorithm detection purposes . Experimental evaluation of the system was carried out and the results illustrated that it was possible to bring about a good performance when the matching algorithm remains unaltered.

A cancelable biometric approach called Palm Hashing was projected by Connie Tee et al. in order to address the non-revocable biometric issue. This technique hashes palm print templates with a set of pseudo-random keys to acquire a unique code known as the palm hash. It is possible to store the palm hash code in portable devices such tokens and smartcards for authentication. Moreover, Palm Hashing also provides numerous advantages over other modern day approaches including clear separation of the genuine-imposter populations and zero EER occurrences. They outlined the implementation facts besides emphasizing its capabilities in security-critical applications .

A fuzzy commitment method working on lattice mapping for cryptographic key generation from biometric data was proposed by Gang Zhen et al. . Despite providing high entropy keys as output the method as well obscures the original biometric data such that it becomes unfeasible to recover the biometric data besides the stored information in the system being open to an attacker. Results of simulation illustrated that the method's authentication accuracy was analogous to that of the renowned.

Je-Gyeong Jo et al presented a simple technique for the generation of digital signatures and cryptography communication with the aid of biometrics. It has been termed necessary to generate the signature in such a way that it becomes possible to verify the same with a cryptographic algorithm in existence like the RSA/El-Jamal without altering its own security constraint and infrastructure . It was anticipated that the mechanism will be capable of guaranteeing security on the binding of biometric information in the signature scheme on telecommunication environments

4. Proposed Methodology

Recently, crypto-biometric systems have been studied for solving the key management problem of cryptographic systems and protecting templates in biometric systems at the same time. In general, the identity theft problem is drastically exacerbated for the biometric systems, since the biometric data and the corresponding feature vectors are non-renewable. To overcome this we generate a secured feature matrix from the fingerprint template and strengthened this by AES Encryption/Decryption algorithm. Besides that, this paper discusses how keys can be generated and demonstrates the technique using fingerprint images .

A. Key generation from Fingerprint

This section confers the feature generation from fingerprint biometric data. The stages are discussed below

- Extracting minutiae points from Fingerprint
- Secured Feature Matrix generation

For extracting minutiae points from fingerprint, a three-level approach is broadly used by researchers. These levels are listed as follows

- Preprocessing
- ROI selection Separation
- Minutiae extraction

For the fingerprint image preprocessing, Histogram Equalization and Gabor Filters are used to do image enhancement. Binarization is applied on the fingerprint image .Then Morphological operations are used to extract Region of Interest [ROI]. By selecting the size and shape of the neighborhood, we can construct a morphological operation that is sensitive to specific shapes in the input image.

a) Preprocessing

Histogram equalization: This method usually increases the local contrast of many images, especially when the usable data of the image is represented by close contrast values. Through this adjustment, the intensities can be better distributed on the histogram ..

Perceptional information of the image is increased through histogram equalization which permits pixel value to expand the distribution of an image. The original histogram of a fingerprint image has the bimodal type, the histogram after the histogram equalization coverts all the range from 0 to 255 and the visualization effect is improved.

Gabor filters: The Gabor filter is applied to the fingerprint image obtained by the previous step by spatially convolving the image with the filter.

A two-dimensional Gabor filter consists of a sinusoidal plane wave of a specific orientation and frequency, modulated by a Gaussian envelope. Gabor filters are employed as they have frequency-selective and orientation selective properties. These properties permit the filter to be tuned to give maximal response to ridges at a specific orientation and frequency in the fingerprint image. So, a properly tuned Gabor filter shall be used to effectively retain the ridge structures while reducing noise. The even-symmetric Gabor filter is the real part of the Gabor function, which is yielded by a cosine wave modulated by

a) Gaussian.

b) ROI Selection

Binarization: Nearly all minutiae extraction algorithms function on binary images where there are only two levels of interest: the black pixels that denote ridges, and the white pixels that denote valleys. Binarization is the process that translates a grey level image into a binary image. This enhances the contrast between the ridges and valleys in a fingerprint image, and consequently makes it possible the extraction of minutiae.

One practical property of the Gabor filter is that it has a DC component of zero, which means the resultant filtered image has a mean pixel value of zero. Hence, straightforward binarization of the image can be achieved using a global threshold of zero. The binarization process involves analyzing the grey-level value of each pixel in the enhanced image, and, if the value is greater than the global threshold, then the pixel value is set to a binary value one; otherwise, it is set to zero. The result is a binary image holding two levels of information, the foreground ridges and the background valleys.

ROI extraction by morphological operations: We perform morphological opening on the grayscale or binary image with the structuring element. We also performed morphological closing on the grayscale or binary image resulting in closed image. The structuring element is a single structuring element object, as opposed to an array of objects for both open and close . Then as the result this approach throws away those leftmost, rightmost, uppermost and bottommost blocks out of the bound so as to get the tightly bounded region just containing the bound and inner area.

c) Minutiae extraction

The last image enhancement step normally performed is thinning. Thinning is a morphological operation that successively erodes away the foreground pixels until they are one pixel wide. Ridge Thinning is to eliminate the redundant pixels of ridges till the ridges are just one pixel wide uses a Ridge Thinning algorithm, which is used for Minutiae points' extraction in our approach. The image is divided into two distinct subfields in a checkerboard pattern. In the first sub iteration, delete pixel p from the first subfield if and only if the conditions G1, G2, and G3 are all satisfied. In the second sub iteration, delete pixel p from the second subfield if and only if the conditions G1, G2, and G3' are all satisfied.

The key used in the AES encryption is the generated key from the whole process. Once after the key is generated, AES encryption progressed to generate a secured feature matrix, but initially encryption process doesn't occur in the key generation from the whole process.

The generated Secured feature matrix is irreversible, moreover it cannot be hacked by an attacker because of the strength of AES and the mathematical operations involved in the generation.

5. Security Analysis

Security of the proposed algorithm is strengthen by these three robust features

- Cancelable Transform
- Feature Matrix Security Analysis
- Irreversible Analysis

A. Cancelable Transform

Cancelable transform is used to generate a cancelable template. The core intention of the cancelable transformation is to provide cancelable skill a "non-invertible" transform. Normally, it decreases the discriminative power of the original template. Therefore, the cancelable templates and the secure templates of an individual in different applications will be different. In turn, the cross matching across databases will not be feasible. Moreover, the secure template can be cancelled and reissued by changing the cancelable transform parameters.

B. Feature Matrix Security Analysis

In our algorithm security is more strengthened by AES encryption. Once after the template is formed and minutia points are acquired, a feature matrix is generated by following a sequence of steps. This feature matrix is then encrypted using AES. Reinforced by AES, the feasibility of decrypting the ciphered feature matrix is almost negligible. Anticipating a worst-case scenario, that if a hacker succeeds in decrypting the AES encryption with an intend obtain the feature matrix; the chances of reorganizing the minutia point and the templates are almost nil. Furthermore, there is no possibility of conjecturing the steps we followed to generate the feature matrix and it is absolutely chanceless to restructure the template by any means.

The key thus formed cannot be traced back to the origin i.e. to the template and moreover the key itself cannot be regenerated falsely using the template. This irreversible aspect makes the key armored and reliable and even resistant to brute force attacks. This shatter-proof property emanates from the very essence of preserving the confidentiality of the battery of operations we follow in transforming minutia points to a Feature matrix.

To decrypt the key we generated, the steps we followed to create it have to be performed in the reverse order . First the feature matrix encrypted using AES, have to be deciphered, then the sequence of steps proceed for forming the feature matrix should be executed from bottom-up. These operations will yield the minutia points acquired from the template in the inception.

C. Irreversible Analysis

To enunciate the concept further tracing out the matrix using the determinant or reorganizing shuffled data is totally infeasible just like attempting to generate an original document using a hashed bits after hashing function is applied.

The security of our algorithm is strengthened by the inherent irreversible nature, by this tracing the minutiae points from the keys generated is practically impossible. The proposed algorithm is more suitable and specific for data like the ones used for handling minutiae points arrived using the above process .

6. Conclusion

Biometrics-based Key Generation has many usability advantages over traditional systems. Particularly, users can never lose their biometrics, and the biometric signal is complicated to forge for steal. The proposed cancelable Cryptographic System is an all-new method for encryption and decryption that yields the synergistic power fingerprint is intentionally distorted in irrevocable manner new print is used. If old fingerprint is "stolen", basically "new" fingerprint can be achieved by simply modifying the parameters of the distortion process . This also consequences in improved privacy for the user since his true fingerprint is nowhere used, and different transformations for distortions can be used for different types of accounts Overwhelming the stated method is something near to impossible because of its inherent intricate nature, as it is solely based on the individuality of the attributes dealt.

The approach can further be streamlined and refined with the fusion of any evolving cryptographic systems.

References

[1] A. Menezes, P. van Oorschot and S. Vanstone, “Handbook of Applied Cryptography”, USA: CRC Press, pp 180, 1997.

[2] D. Feldmeier and P. Karn. “UNIX password security—Ten years later” In Advances in Cryptology—CRYPTO ’89 Proceedings (Lecture Notes in Computer Science 435), 1990.

[3] D. Klein. “Foiling the cracker: A survey of, and improvements to, password security”. In Proceedings of the 2nd USENIX Security Workshop, August 1990.

[3] R. Morris and K. Thompson. “Password security: A case history” Communications of the ACM, 22(11):594-597, November 1979.

[4] E. Spafford. “Observations on reusable password choices “In Proceedings of the 3rd USENIX Security Symposium, September 1992.

[5] T. Wu. “A real-world analysis of Kerberos password security.” In Proceedings of the 1999 Network and Distributed System Security Symposium, February 1999. 12

[6] F. Hao, R. Anderson, and J. Daugman, "Combining Crypto with Biometrics Effectively," IEEE Transactions on Computers, vol. 55, pp. 1081-1088, 2006.

[7] F. Monrose, M. K. Reiter, L. Qi, and S. Wetzel, “Cryptographic key generation from voice," in Security and Privacy, 2001. S&P 2001.

[8] Proceedings. 2001 IEEE Symposium on, pp. 202-213, 2001.

[9] M. Freire-Santos, J. Fierrez-Aguilar, and J. Ortega-Garcia, “Cryptographic key generation using handwritten signature,” in Biometric Technology for Human Identification III, vol. 6202 of Proceedings of SPIE, pp. 225-231, Orlando, Fla, USA, April 2006.

[10] U. Uludag, S. Pankanti, S. Prabhakar, and A. K. Jain, "Biometric cryptosystems: issues and challenges," Proceedings of the IEEE, vol. 92, pp. 948-960, 2004.

[11] Russell Ang, Reihaneh Safavi-Naini, Luke McAven: “Cancelable Key-Based Fingerprint Templates.” ACISP 2005: 242-252.

[13] Image Systems Engineering Program, Stanford University. Student project By Thomas Yeo, Wee Peng Tay, Ying Yu Tai http: //scien.stanford.edu /class /ee368 /projects2001/

[11] L.C. Jain, U.Halici, I. Hayashi, S.B. Lee and S.Tsutsui. “Intelligent biometric techniques in fingerprint and face recognition” 1999, the CRC Press.

[12] D.Maio and D. Maltoni. “Direct gray-scale minutiae detection in fingerprints” IEEE Trans. Pattern Anal. And Machine Intell. 19(1):27- 40, 1997.

[13] www.Wikipedia.com