Matrix Mapping of Crypto-Biometrics for more security implementation

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 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 biometric template by generating Secured Feature Matrix and keys for cryptographic techniques applied for data Encryption or Decryption with the aid of 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 crypto-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 biometric features for securely storing the biometric 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 biometric features enhances the robustness and reliability of the cryptography technique. There are several biometric systems invented for cryptography, but the proposed biometric cryptography technique fashions novel biometric systems to generate Cryptographic Key.

Keyword: **Re-cipher**, **Biometrics, crypto-Biometrics, Cryptography, Key generation, Irrevocable Key, Fingerprint, Minutiae Points, Security Analysis**.

1. Introduction

Biometrics (or biometric authentication) 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 under surveillance.

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 is 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. Proposed Methodology

I have proposed a re-cipher **(caeser method)** method in which biometric data may transform into many encoded forms, and these encrypted biometric data will generate a crypto key which is associated with every transform and will be saved in **(Ri,Cj) matrix**, every repeated transform will give more security to the biometric data, and will provide the ease to get the same biometric data to decrypt at the time of authentication. To form **(Ri,Cj) matrix** I have proposed re-cipher technique by which biometric data will have on each repetition incremented row and column(1 each time) will have a crypto key, and will store into the matrix ,on n rounds we will have n keys of the same biometric data ,so it will diminish the problem of recoverability of biometric data, if somebody will lose or hack the key, biometric data will be re-generated by passing or asking row and column, more deep row and column means more security**.**

3. Conclusion

Biometrics-based crypto 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 Cryptographic System is an all-new method for encryption and decryption that yields the synergistic power *biometric data* is intentionally distorted in irrevocable manner new print is used. If old *biometric data* is "stolen", basically "new" *biometric data* can be achieved by simply asking the row and column of (Ri,Cj) matrix . This also consequences in improved privacy for the user since his true *biometric data* 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.

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] 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