A Survey on Biometrics based Cryptographic Key Generation Schemes

Mr.P.Balakumar
Associate Professor, Department of CSE,
Selvam College of Technology,
Namakkal, Tamilnadu, India

Dr.R.Venkatesan
Professor and Head, Department of CSE,
PSG College of Technology
Coimbatore, Tamilnadu, India

Abstract **- Need for information security and privacy is increasing in recent times. Since several valuable data and files are stored in an organization server system and moreover personal information are being shared in WWW, the need for providing security and permitting only the authorized user is becoming indispensable. For this purpose, biometric authentication is used in several applications and it is progressively acquiring more attention in the field of research. Several biometrics like fingerprint, iris, retina, etc., are used in rendering security to the information or key. The generation of cryptographic key from biometrics is used generally to secure the system. On the other hand, the storage and security for the biometric templates and the encryption keys are of a major concern. The effectiveness and the flexibility of the cryptographic key generation schemes make it suitable for integrating it with the biometric features (Biometric cryptosystems). Security is one of the major concerns in the present world and there is need for many researches to deal with the better biometrics based cryptographic key generation schemes. In this survey, discussed the several biometrics based cryptographic key generation schemes which will show the way for development of better security schemes using biometrics and cryptography.**

Keywords – Biometrics; BiometricCryptosystem; Encryption Algorithms; Cryptography Key Generation.

I. INTRODUCTION

The term biometrics is described as “automated recognition of individuals in accordance with their behavioral and biological characteristics” [1]. Information security and privacy has become an important factor in the present world. Biometric recognition is one of the most important techniques for the security privacy due to its distinctive nature of biometric traits such as fingerprints, iris and faces [2]. As a result, this technique is used with many other applications to enhance the security.

Biometric authentication is the process of validating the uniqueness of individuals according to their physiological (for instance, fingerprint, iris, face) or behavioral qualities (for instance, signature) [3]. During the process of authentication, biometric features of a person are compared against the accumulated biometric profile of the claimed identity and permission to access a system or data is approved only when there is adequate match.

Biometric systems are acquiring more attention since more trustable substitutions to password-dependent security systems, because there is no need to keep passwords in mind and moreover it is very difficult to steal and copy the biometric features. Furthermore, it also offers non-repudiation (does not permit an authenticated user to deny his activities).

Accordingly, Cryptographic techniques have gained its popularity due to its security purpose. In the cryptographic technique the original data is encoded by using any key so that it is very complicated for an attacker to understand it. The original data can be obtained by decoding the encoded data using the same key. Thus the privacy is well protected in this cryptographic approach. Several cryptographic approaches like DES, AES [4] and public key architectures like RSA are widely used for the authentication purpose.

The characteristic feature of cryptographic security is conditioned by an authentication step that is based on long pseudo-random keys, which are impracticable to memorize in mind [5]. This feature of incapability to memorize the cryptographic keys has been restraining the security of systems for a long time.

Biometric cryptosystems is a new method of integrating the features of biometrics with cryptographic keys, and is commonly recognized as crypto-biometric systems [6]. The integration of biometrics [7] and cryptography is broadly carried out in two distinct steps. In case of biometrics-based key generation, a biometric matching along with an input biometric signal and an accumulated template is exploited in the release of the secret key. The biometric signals are immeasurably enclosed to the keys in case of biometrics-based key generation.

The fundamental concept of biometric cryptosystems is that the biometric feature takes care of user authentication, whereas a standard key generation scheme takes care of the other components of control (for instance, secure communication).

Hence biometric cryptosystems are gaining more consideration in the research community and several authors

have concentrated on this particular domain by developing several biometric cryptosystems. Those biometric cryptosystems are clearly discussed in the following section.

II. LITERATURE SURVEY

Conventional cryptosystems, user authentication depends on the possession of secret keys and this system is not effective when the keys are not kept secret (specifically shared with non-genuine users). Additionally, keys can be not remembered, lost or stolen and as a result, cannot offer non-repudiation. Available authentication techniques depending on physiological and behavioral features of persons, for instance, fingerprints, essentially solve most of these difficulties and might substitute the authentication section of conventional cryptosystems. Uludag et al., [8] presented several techniques that monolithically combine a cryptographic key with the biometric template of a particular user accumulated in the database in some manner the key cannot be exposed without a valid biometric authentication. The author illustrated the difficulties that taken place in the construction of biometric key owing to extreme acquisition dissimilarities in the biometric identifier and the inadequate nature of biometric feature extraction and corresponding algorithms. Moreover, the author revealed the appropriateness of these approaches for digital rights management systems.

Cancellable biometrics gives a better performance of security as it facilitates with more than one template for the same biometric data. Russell Ang et al., [9] proposed the measurement of the success of a particular transformation and matching algorithm for fingerprints. A key-dependent cancellable template for the fingerprint was produced by employing a key dependent geometric transform on the obtained fingerprint features.

Ignatenko and Willems [10] concentrated on the privacy issues in biometric cryptosystems. The author examined four settings. Initially, the standard Ahlswede-Csiszar secret-generation setting is examined in which two terminals monitor two correlated sequences. They combine to generate a common secret by exchanging a public message. This message is permitted to include only a small amount of information regarding the secret, however, it is necessary to disclose as modest information as possible regarding the biometric data. In this circumstance, the fundamental exchange between secret-key and privacy-leakage rates is determined. In case of the second setting, the secret is not produced instead it is selected independently, the fundamental secret-key against privacy-leakage rate balance is determined.

While considering the settings three and four, it primarily concentrates on zero-leakage systems. In these settings the public message is allowed to contain only a small amount of information on both the secret and the biometric sequence. In order to realize this, a private key is required and this can only be recognized by the terminals. For both the cases of generated-secret and the chosen-secret model, the regions of possible secret-key against private-key rate pairs are determined. In all the cases, the fundamental balance is determined for both unconditional and conditional privacy leakage.

Rather than using PINs and passwords as cryptographic keys, it can be created depending on the user-specific biometric information. Since PINs and passwords are either simple to forget or susceptible to attacks. A structure is formulated by Yao-Jen Chang et al., [11] to produce stable cryptographic keys from biometric data that is unbalanced in nature. This structure is entirely dissimilar to other previous works in which user-dependent transforms are exploited to produce more compressed and distinguishable characteristics. By this means, a longer and more constant bitstream can be created as the cryptographic key.

Asymmetric encryption approaches need the storage space to store the secret private key. Accumulated keys are generally defended by inadequately chosen user passwords that can either be estimated or acquired through brute force attacks. This is a feeble link in the entire encryption system and can possibly negotiate the reliability of sensitive data.

Integrating biometrics with cryptography is seen as a potential solution but any biometric cryptosystem must be capable of overcome tiny changes present between different acquirement of the similar biometric with the purpose of generating reliable keys. Sashank Singhvi et al., [12] developed a new technique which exploits an entropy dependent feature extraction process integrated with Reed-Solomon error correcting codes that can produce deterministic bit-sequences from the output of an iterative one-way transform.

Due to the enormous growth of Internet, Information security is turning out to be gradually more important. Conventional cryptographic technique involves the user to keep the keys in mind, but in general it is impractical. Biometrics dependent cryptographic key generation approaches produce cryptographic keys from biometrics directly. Lifang Wu et al., [13] developed a biometric cryptosystem depending on the face biometrics.

During the encryption phase, a 128-dimensional Principal Component Analysis (PCA) feature vector is initially obtained from the face image. Subsequently, a 128 bit binary vector is achieved by thresholding. Then the author selected the distinguishable bits to generate bio-key and the most favorable bit order number is accumulated in a look-up table. In addition, an Error-Correct-Code (ECC) is produced using Reed-Solomon algorithm.

The message is encrypted by means of symmetric DES with bio-key. During the decryption phase, a 128-dimensional PCA characteristic vector is obtained from the query face image. After that a bio-key is produced using the look-up table created during encryption stage. The absolute key is generated using both bio-key and ECC. At last, the author implemented the symmetric DES decryption algorithm to acquire message using final key.

In conventional Public Key Infrastructure (PKI) system, Private Key could be accumulated in central database or accumulate distributed in smart-card and provided to the users. The Private Key is typically secured by using passwords that are effortlessly estimated or stolen and thus bring about the collapse of the entire system. The present trend for PKI system is depending on physiological and behavioral features (biometrics). This system can enhance the security of Private Key, the biometric features could not be estimated or falsified. On the other hand, this approach still discloses a gap that is the susceptibility of storage device of Private Key and biometrics data. Intruders can attack to these storage spaces and acquire user identification information.

Nguyen Thi Hoang Lan and Nguyen Thi Thu Hang [14] provided a solution that utilizes Biometric Encryption Key (BEK) to encrypt Private Key and safeguard Private Key in a secure manner for this kind of information. The author also presented the BEK generation approach and the BioPKI system to support this solution.

Biometrics-based authentication systems provide observable usability merits over conventional password and other authentication techniques. On the other hand, large number of privacy issues is developing in the field of biometrics. A biometric is everlastingly coupled with a user and it is very complicated to alter unless any severe damage occurs to that particular biometric feature. Consequently, when a biometric identifier is compromised, it is vanished forever and probably for all application where the biometric is exploited. Furthermore, in case when the similar biometric is utilized in several applications, a user can probably be tracked from one application to the subsequent through cross-estimation biometric databases. Ratha et al., [15] illustrated several techniques to produce multiple cancelable identifiers from fingerprint images to avoid these difficulties.

In particular, a user can be specified as many biometric identifiers as required by issuing a new transformation “key”. The identifiers can be ignored and substituted when compromised. The author revealed that it is possible to accomplish revocability and thwart cross-estimation of biometric databases and moreover these transforms are noninvertible since it is practically as complicated to recover the original biometric identifier from a altered version as by arbitrarily guessing. The author also revealed that feature-level cancelable biometric construction is feasible in bulky biometric deployments.

A standard management on creating biometric keys from binary biometric templates is developed by Rathgeb and Uhl [16]. A context-based examination is carried out using iris biometric feature vectors depending on which constant biometric keys are extracted. Most consistent bits in binary iris codes are distinguished and exploited to build keys from fuzzy biometric data. This key generation technique is personalized to different iris biometric feature extraction approaches. Additionally, this technique is modified to offer complete revocable biometric keys, long adequate to be implemented in generic cryptosystems.

Hao et al., [17] presented a realistic and secure way to incorporate the iris biometric into cryptographic applications. They deliberated on the error patterns within iris codes and developed a two-layer error correction technique that merges Hadamard and Reed-Solomon codes. The key was produced from the iris image of the subject through the auxiliary error correction data that do not disclose the key and can be saved in a tamper-resistant token like a smart card. It was established that an error-free key can be reproduced reliably from genuine iris codes with a success rate of 99.5 percent. It is possible to produce up to 140 bits of biometric key, more than adequate for 128-bit AES.

An iris feature-based PKI key generation is developed by Yazhuo Gong et al., [18]. This key generation scheme includes a common approach for distinguishable iris feature creation and a PKI key generation method. This technique is different from previous approaches of using pseudo random number to produce cryptographic keys. By this means, a longer and additional distinguishable bitstream can be produced for PKI key generation.

A cancellable biometric technique called PalmHashing was developed by Connie et al., [19] with the purpose of dealing with the non revocable biometric problem. In this technique, the palmprint templates are hashed with a collection of pseudo-random keys to obtain a distinctive code identified as the palmhash.

Jo et al., [20] proposed a simple technique for the generation of digital signatures and cryptography communication with the aid of biometrics. The generation of the signature is necessary in such a way that it becomes possible to verify the same with a cryptographic algorithm in existence like the RSA without altering its own security constraint and infrastructure.

Biometric authentication is gradually attaining more recognition in an extensive range of applications. On the other hand, the storage space of the biometric templates and/or encryption keys is a subject of severe issue that are indispensable for these kind of applications, since the negotiation of templates or keys inevitably compromises the information protected by those keys. Weiguo Sheng et al., [21] developed a new technique, which needs neither the storage of biometric templates nor the encryption keys, by openly producing the keys from statistical characteristics of biometric data.

An overview of this technique is as follows: provided biometric samples and a collection of statistical features are initially obtained from each sample. On every feature subset or single feature, his technique models the intra and interuser dissimilarity by clustering the data into natural clusters by means of a fuzzy genetic clustering approach. In accordance with the modeling outcome, this technique subsequently measures the steadiness of each feature subset or single feature

for all the users. By directly choosing the most reliable feature subsets and/or single features for every user independently, this technique creates the key consistently without compromising its comparative security.

Table I: An overview of the existing Biometrics-based authentication systems

Method	Technique Used
Uludag et al., [8]	Monolithically combined a cryptographic key with the biometric template in some manner the key cannot be exposed without a valid biometric authentication.
Russell Ang et al., [9]	Key-dependent cancellable template for the fingerprint using geometric transform**.**
Yao-Jen Chang et al., [11]	Formulated a structure to produce stable cryptographic keys from biometric data. Capable of generating longer and more constant bitstream.
Sashank Singhvi et al., [12]	Entropy dependent feature extraction process integrated with Reed-Solomon error correcting codes to produce bit-sequences from the output of an iterative one-way transform.
Lifang Wu et al., [13]	Biometric cryptosystem depending on the face biometrics. Principal Component Analysis (PCA) is used during the encryption phase.
Nguyen Thi Hoang Lan and Nguyen Thi Thu Hang [14]	Biometric Encryption Key (BEK) to encrypt Private Key and safeguarding Private Key in a secure manner.
Ratha et al., [15]	Multiple cancelable identifiers from fingerprint images.
Rathgeb and Uhl [16]	Generating biometric keys from binary biometric templates. Binary iris codes are exploited to build keys from fuzzy biometric data.
Hao et al., [17]	Secure way to incorporate the iris biometric into cryptographic applications. Two-layer error correction technique that merges Hadamard and Reed-Solomon codes.
Yazhuo Gong et al., [18]	Iris feature-based PKI key generation scheme. Longer and additional distinguishable bitstream can be produced for PKI key generation.
Connie et al., [19]	Palmprint templates are hashed with a collection of pseudo-random keys to obtain a distinctive code.
Jo et al., [20]	Simple technique for the generation of digital signatures and cryptography communication with the help of biometrics.

III. Problems and Directions

There are several issues in the above discussed biometric cryptosystems in providing proper security to the valuable information and authentication of specific users. In addition, a perfect biometric cryptosystems should permit the authorized users to access the information without any difficulty and it should not allow the unauthorized user. In order to overcome these difficulties numerous researches has to be done. The research may be focussed on the following areas.

A. Preprocessing Biometric Features to Remove Noise

The major difficulty is that the biometric data are naturally noisy and several researches has to be done to remove these noises.

B. Securing Biometric Features with Cryptographic Techniques

Moreover, biometric data are not extremely secret. People may leave their fingerprints all over the places they touch. Similarly iris images can be captured easily by using a hidden camera.

Another major concern in a biometric system is to provide proper security to the unique biometric data, since there is chances for stealing the biometric data and can be misused.

The mounting requirement for improved security systems has shown the way for an exceptional interest in the field of biometric based cryptograpgic key generation schemes. In general, most of the biometric systems are simply based on a single biometric feature.

C. Using Multimodal Biometric Features

Certain unimodal systems have offered significant improvement in consistency and accuracy, but still they undergo enrollment difficulties because it contains noisy data. These systems are susceptible to several difficulties like noisy data, intra-class variations, inter-class similarities, non-universality and spoofing. It leads to considerably high False Acceptance Rate (FAR) and False Rejection Rate (FRR), inadequate discrimination potential, upper bound in performance and lack of permanence.

Hence it is potential to use to two or more biometric features (multimodal) for cryptographic key generation, since a fingerprint or iris feature can be easily captured. Moreover, care should be taken in using the cryptographic key generation scheme and in choosing the biometric features. In such a way at least one biometric feature should be very difficult to capture. Two or more biometric features along with better cryptographic key generation scheme will definitely provide secured biometric cryptosystems.

IV. Conclusion

Security is of a major concern in the present scenario. Providing security to the information in a system and allowing

only the authorized users becomes most challenging task since the number of intruders and security attacks are increasing constantly. The conventional security system uses password or security key for authentication; but those password and security keys can be easily stolen or estimated. To overcome these issues, biometrics of a person is used to secure the system. But, if the biometrics is stolen one time, it can be used by theft to access the system until it exists. Moreover multiple applications use the same biometric feature, and hence if a biometric feature of a particular person is stolen then it can be used for all the applications. This provides huge difficulty for the researchers to develop a new secure technique.

From this survey it is concluded that a single biometric possibly will not be able to satisfy the growing demand of the security in the current real world applications. As discussed in the previous section, using multimodal biometric features along with better cryptographic key generation scheme can help in satisfying the growing demand against the security.

REFERENCES

[1] Hossein Bidgoli, "Handbook of Information Security Threats, Vulnerabilities, Prevention, Detection, and Management (Volume-3)", John Wiley and Sons Publishers, 2005.

[2] Y.C. Feng, P.C. Yuen and A.K. Jain, "A hybrid approach for face template protection", Proceedings of SPIE Conference of Biometric Technology for Human Identification, Orlando, USA, Vol. 6944, Pp. 325, 2008.

[3] A.K. Jain, A. Ross and S. Prabhakar, "An introduction to biometric recognition", IEEE Transactions on Circuits and Systems for Video Technology, Vol. 14, Pp. 4–20, 2004.

[4] N. I. of Standards and Technology, "Announcing the Advanced Encryption Standard (AES)", FIPS 197, Technical Report, National Institute of Standards and Technology, 2001.

[5] F. Ayoub and K. Singh, "Cryptographic techniques and network security", IEE Proceedings of Communications, Radar and Signal Processing, Vol. 131, No. 7, Pp. 684 – 694, 1984.

[6] F. Chafia, C. Salim and B. Farid, "A biometric crypto-system for authentication", International Conference on Machine and Web Intelligence (ICMWI), Pp. 434 – 438, 2010.

[7] Alexander P. Pons and Peter Polak, "Understanding user perspectives on biometric technology", Communications of the ACM, Vol. 51, No. 9, Pp. 115-118, 2008.

[8] U. Uludag, S. Pankanti, S. Prabhakar and A.K. Jain, "Biometric cryptosystems: issues and challenges", Proceedings of the IEEE, Vol. 92, No. 6, Pp. 948 – 960, 2004.

[9] Russell Ang, Rei Safavi–Naini and Luke McAven, "Cancellable key-based fingerprint templates", Australasian Conference on Information Security and Privacy (ACISP), Pp. 242-252, 2005.

[10] T. Ignatenko and F.M.J. Willems, "Biometric Systems: Privacy and Secrecy Aspects", IEEE Transactions on Information Forensics and Security, Vol. 4, No. 4, Pp. 956 – 973, 2009.

[11] Yao-Jen Chang, Wende Zhang and Tsuhan Chen, "Biometrics-based cryptographic key generation", IEEE International Conference on Multimedia and Expo (ICME), Vol. 3, Pp. 2203 – 2206, 2004.

[12] R. Sashank Singhvi, S.P. Venkatachalam, P.M. Kannan and V. Palanisamy, "Cryptography key generation using biometrics", International Conference on Control, Automation, Communication and Energy Conservation (INCACEC), Pp. 1 – 6, 2009.

[13] Lifang Wu, Xingsheng Liu, Songlong Yuan and Peng Xiao, "A novel key generation cryptosystem based on face features", IEEE 10th International Conference on Signal Processing (ICSP), Pp. 1675 – 1678, 2010.

[14] Nguyen Thi Hoang Lan and Nguyen Thi Thu Hang, "An approach to protect Private Key using fingerprint Biometric Encryption Key in BioPKI based security system", 10th International Conference on Control, Automation, Robotics and Vision (ICARCV), Pp. 1595 – 1599, 2008.

[15] N.K. Ratha, S. Chikkerur, J.H. Connell and R.M. Bolle, "Generating Cancelable Fingerprint Templates", IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 29, No. 4, Pp. 561 – 572, 2007.

[16] C. Rathgeb and A. Uhl, "Context-based biometric key generation for Iris", IET Computer Vision, Vol. 5, No. 6, Pp. 389 – 397, 2011.

[17] F. Hao, R. Anderson and J. Daugman, "Combining crypto with biometrics effectively", IEEE Transactions on Computers, Vol. 55, Pp. 1081-1088, 2006.

[18] Yazhuo Gong, Kaifa Deng and Pengfei Shi, "PKI Key Generation Based on Iris Features", International Conference on Computer Science and Software Engineering, Vol. 6, Pp. 166 – 169, 2008.

[19] T. Connie, A. Teoh, M. Goh and D. Ngo, "Palm hashing: A novel approach for cancellable biometrics", Information processing letters, Vol. 93, No. 1, Pp. 1-5, 2005.

[20] J.G. Jo, J.W. Seo, and H.W. Lee, "Biometric digital signature key generation and cryptography communication based on fingerprint," First Annual International Workshop, Pp. 38-49, Springer Verlag, 2007.

[21] Weiguo Sheng, G. Howells, M. Fairhurst and F. Deravi, "Template-Free Biometric-Key Generation by Means of Fuzzy Genetic Clustering", IEEE

Transactions on Information Forensics and Security, Vol. 3, No. 2, Pp. 183 – 191, 2008.

AUTHOR'S PROFILE

P.Balakumar received the B.E. and M.E. degrees in Computer Science and Engineering from PSG College of Technology, Coimbatore, in 1997 and Anna University, Chennai in 2004 respectively. During 1999-2001, he worked as Lecturer in PSG College of Technology in Coimbatore. Later during 2003-2008, he worked as Lecturer & Assistant Professor in AMS Engineering College, Namakkal. He now with Selvam College of Technology, Namakkal, Tamilnadu, India as Associate Professor in Department of Computer Science and Engineering.

Dr.R.Venkatesan was born in Tamilnadu, India, in 1958. He received his B.E (Hons) degree from Madras University in 1980. He completed his Masters degree in Industrial Engineering from Madras University in 1982. He obtained his second Masters degree MS in Computer and Information Science from University of Michigan, USA in 1999. He was awarded with Ph.D from Anna University, Chennai in 2007. He is currently Professor and Head in the Department of Computer Science and Engineering, PSG College of Technology, Coimbatore, India. His research interests are in Simulation and Modeling, Software Engineering, Algorithm Design, Software Process Management.