BioCryptosystems for Authentication and Network Security-A Survey

K. Saraswathi[1] Dr. R. Balasubramaniam[2]

GJCST Computing Classification
D.4.6, C.2.0

***Abstract*-Authentication and Network security prove to be challenging issues in data transmission between users. A number of proposed bio-crypto algorithms have limited practical applicability because of trade-off that exists between recognition performance and security of the biometric template. Most of the traditional cryptosystems that have been proposed earlier in literature have adopted secret key to authenticate the user information. The use of secret key may direct to unenviable circumstances when the secret key is lost, stolen or forgotten. This obviously makes the user to obscure their authentication and security. These controversies can be eliminated by introducing new algorithms for providing authentication based on biometrics (characterizes on physiological and behavioral traits of persons). Most of the current authentication systems are based on biometrics like fingerprint, retina, face recognition, etc. This paper generally revolves around various methods that are adopted to ensure user authentication and network security by binding a cryptographic key with a biometric template of the user. The security level is trusted since the cryptographic key cannot be exposed unless successful biometric authentication. This paper also overviews on issues in cryptographic key generation due to flawed nature of biometric feature extraction and matching algorithms.**

Keywords: Authentication, Bio-crypto algorithms, Biometrics, Cryptographic Key, Network Security.

I. INTRODUCTION

Biometrics deals with identification of individuals based on their biological and behavioral characteristics. Autonomously, both biometrics and cryptography play a critical role in providing security to user information [1]. In a cryptographic system the user authentication is tenure based. In this type of system the cryptographic keys used for encryption and decryption are long and random, hence cannot be memorized. This has led to store the cryptographic key in some other position and release it based on some alternative authentication like password. This password can be easily compromised based on social engineering techniques. Most of the users have same passwords for many applications. Upon compromising a single password can open up many doors to illegitimate users. So passwords alone can no longer ensure user authentication and security. The biometrics and cryptographic systems can be combined together using two different ways. The binding of cryptographic key along with biometric template .ensures user privacy and security as the biological and behavioral characteristics of a user cannot be revealed by another unauthorized user. In the first approach, cryptographic key generation is decoupled with biometric matching. Therefore, the cryptographic key is released when there occurs biometric matching (e.g. Smart card). This approach is known as Biometric based key Release. The second method is the biometric key generation in which both the biometric template and the cryptographic key are combined together. This combination does not need any matching operation to extract the key. The BioCryptosystems produce higher level of security since it assists the cryptographic systems to encrypt and decrypt the messages using biometric templates.

The cryptographic algorithms require their keys to be of 128 bits in length for Advanced Encryption Standards (AES) [2], [3]. The limitations of traditional passwords that are used for generation of cryptographic keys can be eliminated by BioCryptosystems. This method requires the person being authenticated to be present at the time of authentication where duplication is not possible. But because of noise, the biometric template produces only fuzzy data whereas a Digital signature requires crisp keys. Also fuzziness can be introduced due to variability in biometric data. To overcome this limitation the cryptographic system must accept some fuzziness. Therefore, fuzzy vault is such a construction used to store the secret key based on the biometric template. This paper presents an analysis of repercussion of the existing biometric techniques to the containment process.

II. RELATED WORKS

Traditional algorithms implemented using cryptosystems use long and random keys which are difficult to memorize and hence it required additional database to store the key. The release of the key is dependent on an alternate authentication approach (i.e. password) which may fail to identify the authorized user. The current BioCryptosystems alleviates this limitation by binding together cryptographic framework and the biometric features. This section describes some of the general approaches presented by various researchers towards BioCryptosystems.

A Key binding algorithm in an optical correlation based fingerprint matching system was proposed by Soutar et al. in [4], [5], and [6]. This is an algorithm developed to securely link and retrieve the digital key using the interaction of a biometric image, such as fingerprint, with a secure block of data, popularly known as Bioscrypt. The key can be used as an encryption and decryption key. This Bioscrypt comprises a filter function, which are calculated using image processing algorithm and other information which is

About [1]*Asst.Proffessor, Department of Computer Science, Govt Arts College, Udumalpet, Tirupur, India.* About [2]*Dean Academic Affairs, PPG Institute of Technology, Coimbatore, India*

required to first retrieve and then verify the validity of the key. The information from the output pattern formed via the interaction of the biometric image with the filter function is effectively utilized to retrieve the key. Therefore the design of the filter should be in such a manner that it produces consistent output patterns. Moreover, the security of the filter function should also be considered. The reported work in [4] by Soutar et al. also discusses on consistency of the output patterns and the security of the filter function. The major drawback of this approach is that the loss of entropy at each stage of algorithm has not been discussed.

Davida et al. present an algorithm in [7], where the secure off-line authenticated user identification schemes based on the biometric system that can measure a user's biometric accurately (up to certain Hamming distance). The schemes presented in [7] by Davida et al., enhance identification and authorization in secure applications by binding a biometric template with authorization information on a token such as magnetic strip. This paper also discusses certain methods that are specially developed to minimize the compromise of a user's private biometric data which has been encapsulated in the authorized information. This eliminates the need of secure hardware tokens.

Monrose et al. prescribe in [8] a novel approach to enhance the security of the user password by Password Hardening based on Key stroke Dynamics. This approach efficiently hides information about which of the user's features are relevant to generating the user password, even for an attacker it is more tedious to capture all system information. This proposed scheme automatically adapts to gradual changes in a user's typing patterns while maintaining the same user hardened password across multiple logins, for use in file encryption or other type of application that requires a long term secret key. This model first combines the legitimate user's typing patterns with the password to generate a hardened authentication pattern. This hardened password seems to be highly secure. The main drawback of this approach is that a user whose typing patterns change substantially between consecutive instances of typing the password may be unable to generate the user hardened password and this led to error in login.

Juels and Wattenberg in [9] presented an improved approach of that put forth by Davida et al. in [7]. In their contribution, "Fuzzy commitment" scheme Juels and Wattenberg described more generalized and considerably improved method that can tolerate more variations in the biometric characteristics and hence determines to provide stronger security and privacy to user. In this approach the user is allowed to select a secret message at the time of enrollment. This approach utilizes the advantages of some error correcting methods to retrieve the original message. Juels and Sudan [10] prove the security of the fuzzy vault scheme in an information-theoretic sense by enhancing the previous work in [9] proposed by Juels and Wattenberg. But their algorithm fails to highlight on robustness of the algorithm to typical variations in the biometric signals. The comparison of different algorithm proposed in literature by researchers is summarized in Table 1.

A non-invertible transformation function based approach was put forth by Ratha et al. in [11], which discusses the potential security holes in a biometrics based authentication scheme, quantify the numerical strength of one method of fingerprint matching, and includes discussion on combating some of the weakness. This method employs a one way function to transform the biometric features. Their method does not involve redesigning of biometric matcher since the transformation takes place in same feature space. The main flaw of this algorithm is that it leads to increased False Rejection Rate.

Clancy et al. [12] implemented Juels and Sudan's fuzzy vault algorithm for key generation based on the fingerprint minutiae representation. Their experimental results suggested that the performance of biometric matcher described by Jain et al. [13] is not as good as those reported in current authentication systems by Maio et al. [14]. The biometric matcher is used on the authentication side, to match the user's biometric characteristics with those of the biometric templates that are stored in database to identify user longevity.

The techniques proposed by Dodis et al. in [15], apply not just too biometric information but it can be adopted for any keying material that unlike traditional cryptographic keys, cannot be reproduced precisely, and not distributed uniformly. The fuzzy extractor employed in this approach extracts nearly uniform randomness R from its biometric input. The randomness R obtained will be the same even if there is change in the input, until there remains reasonable close relationship with the original, hence this extraction is said to be error-tolerant. This R can be utilized as cryptographic key for any kind of application. This approach also provides an optimal construction of primitives for various measures of closeness of input data, such as Hamming distance, Edit distance, and Set difference.

The approach put forth by Teoh et al. in [16] involves adding user specific external randomness to biometric features. This increases the entropy of biometric features resulting in low False Accept Rate. At the same time, if the user compromises on their random information then the entropy gain decreases. Their previous work describes the integration of external randomness with user-specific biometrics, resulting in bitstring outputs with security characteristics; which is comparable to cryptographic ciphers or hashes. The technique of BioHashing introduced in their work, furthermore increases recognition effectiveness through Random Multispace Quantization (RMQ) of biometrics and external random inputs.

The key generation algorithm however, suffers from many limitations such as requiring pre-aligned representations, having a limited choice of flexible operating points, and hence the implementation results in higher complexity in overall system, and requires more intensive computation

TABLE 1 Comparison of Various Biometrics based Key generation and Key release algorithms. High, Medium and Low are represented by H, M and L respectively

R and G denote key Release and key Generation function respectively. U stands for Undetermined

Algorithm	Biometric Representation	Classification	Privacy Protection	Practicality	Sensitivity to invariance	Security
Soutar et al.	Fingerprint (Image)	R	H	M	H	U
Davida et al.	Iris (Iris code)	G	H	H	L	U
Juels et al.	No Evaluation	G	H	H	M	H
Monrose et al.	Keystroke, Voice	G	H	H	H	M
Ratha et al.	Fingerprint	G	H	H	M	H
Teoh et al.	No Evaluation	G	H	H	L	H

III. BIOCRYPTOSYSTEM

The biometric characteristics that have been widely used in various applications are human face, iris, retina, hand geometry, signature, voice etc [17]. Each biometric characteristic have its merits and demerits, and the choice of implementation is based on the type of application. No single biometric is expected to meet all the essential requirements. Some important requirements of biometrics are acceptability, performance, and accuracy. The properties of biometric characteristics and the requirements of applications determine the match between the specific biometric and an application.

The Biometric Key Cryptography (BKC) is an emerging reliable alternative that can resolve key management problem, larger key computational process and address the non-repudiation problem. The major properties of biometric identifiers are universality, distinctiveness, permanence, and collectability. Similarly, attributes of biometric systems are acceptability, performance and circumvention [18]. Use of many biometric characteristics such as retina, odor, ear, and DNA in commercial authentication systems are also being examined [17]. Depending on the operational situation, different biometric characteristics are used for different Digital Rights Management (DRM) applications. A brief comparison of some of the biometric identifiers based on seven factors is summarized in the Table 2.

The BioCryptosystems utilizes the merits of biometrics and the cryptographic framework. This approach enhances user authenticity. Therefore experiments are conducted in this area to determine the efficiency of the algorithms implemented to measure the accuracy and privacy of the user information. Moreover, biocryptosystem analyzes various properties and attributes of biometric identifier in determining the efficiency of the proposed algorithms.

Fuzzy vault [10] is a cryptographic framework designed using biometric features that defined as unordered set of genuine points and chaff points. One of the major of fuzzy vault is dealing the intra class variations in the biometric data and working with unordered sets. Hardening of fuzzy vault using biometrics enhances the security and the privacy of the user. Fuzzy vault hardened with biometrics utilizes the advantages of both cryptographic frame work and the biometric template. The randomness in the biometric data can be eliminated. Moreover, this fuzzy vault scheme provides improves user authentication.

TABLE 2 Comparison of Various Biometric Identifiers based on Properties and Attributes of Biometric Identifiers. High, Medium and Low are represented by H, M and L respectively

Biometric Identifier	Universality	Uniqueness	Permanence	Collectability	Performance	Acceptability	Circumvention
Face	H	L	M	H	L	H	H
Fingerprint	M	H	H	M	H	M	M
Iris	H	H	H	M	H	L	L
Voice	M	L	L	M	L	H	H
Signature	L	L	L	H	L	H	H

The Biocryptosystem is created by binding the cryptographic key generation algorithm along with biometric features to enhance the security and privacy of user. This approach cannot be broken by an imposter as the security level of this approach is upgraded by password and biometric features of the user. The compromising of user password anyhow will not affect the performance of fuzzy vault scheme, since the security provided by fuzzy vault will be the same and therefore the addition of password just acts as an additional layer of security.

IV. FUTURE WORK

The necessary of implementation of BioCryptosystems for real world applications increases day by day. Therefore, the security and privacy of user is the major concern. In future one of the following approaches may be adopted to authenticate user. Many cryptographic techniques are available to ensure user authentication. Use of crypto biometrics which is a blend of cryptography and soft biometrics ensures security. The soft biometrics used may be behavioral characteristics of user which cannot be provoked by attackers. Biomapping is another approach which can be employed to increase the user authentication. Biomapping is a blend of feature extraction, non-invertible transform and anonymous query as a whole. Iris biometrics can be combined with custom cryptographic schemes to obtain an efficient BioCryptosystems. Such BioCryptosystems prove to show development especially in the field of generating longer cryptographic key strings while keeping the system quality. Another interesting approach can be given by combining Biometrics, cryptography and data hiding. This combination may provide an effective and often complementary solution to information security from different perspectives. Moreover, this approach of combining biometrics, cryptography and data hiding mainly focus on the problems of cryptographic key management and biometric template protection. Future enhancement concentrates on developing an economical and advanced BioCryptosystem that improves the network security and user authentication.

V. CONCLUSION

This paper marginally details a survey of various algorithms presented by researchers in literature to develop systems that provide authenticity to user. However, every algorithm has its own advantages and limitations. The current authentication system employs a hybrid approach to ensure security and privacy to user. This paper signifies the necessity of BioCryptosystems in ensuring the authentication and privacy to the user. The BioCryptosystems engages the advantages of biometrics and cryptographic framework such a combination cannot be degraded by any attacker. The BioCryptosystems can be used to ensure user authentication and network security, though the comprised password does not affect the security level of the fuzzy vault system, since it acts as an additional layer of security. There occur a lot of issues in combining the biometrics with the cryptographic system due to imperfect nature of biometric matching algorithms and degraded nature of biometric features. But even then biometrics is the only essential component of identity-based security system, as no other technology can be implemented in “Identifying the authorized person based on their intrinsic distinctive traits”. Therefore, it is of greater necessity for crypto biometric system to provide user authentication

VI. REFERENCE

1) F. Hao, R. Anderson, J. Daugman, "Combining Cryptography and Biometrics," Technical Report No. 640, University of Cambridge Computer Laboratory, 2000.
2) W. Stallings, "Cryptography and Network Security: Principles and practices," 3rd edition, Upper Saddle river, NJ: Prentice-Hall 2003.
3) Advanced Encryption Standard (AES), Federal information processing standards publication 197, National Institute of Standards and Technology, 2001.
4) C. Soutar, D. Roberge, S. A. Stojanov, R. Gilroy, and B. K. V. Vijaya Kumar, "Biometric Encryption using Image Processing," in Proc. SPIE, Optical Security and Counterfeit Deterrence Techniques II, vol. 3314, 1998, pp. 178-188.
5) C. Soutar, D. Roberge, S. A. Stojanov, R. Gilroy, and B. K. V. Vijaya Kumar, "Biometric Encryption - enrollment and verification Procedures," in Proc. SPIE, Optical Pattern Recognition IX, vol. 3386, 1998, pp. 24-35.
6) C. Soutar, D. Roberge, S. A. Stojanov, R. Gilroy, and B. K. V. Vijaya Kumar, "Biometric Encryption," in ICSA Guide to Cryptography, R. K. Nichols, Ed. New York, McGraw-Hill, chapter 22, 1999.
7) George I. Davida, Y. Frankel, and B. J. Matt, "On enabling secure applications through off-line biometric identification," in proc. IEEE Symposium Privacy and Security, 1998, pp. 148-157.
8) F. Monrose, M. K. Reiter, and S. Wetzel, "Password Hardening based on Keystroke Dynamics," in Proceedings 6th ACM Conference Computer and Communications Security, 1999 pp. 73-82.
9) Juels and M. Wattenberg, "A Fuzzy Commitment Scheme," in Proc. 6th ACM Conference, Computer and Communications Security, G. Tsudik, Ed., 1999, pp. 28-36.
10) Juels and M. Sudan, "A Fuzzy vault Scheme," in Proc. IEEE International Symposium Information Theory, A. Lapidoth and E. Teletar, Eds., 2002, p. 408.
11) N. K. Ratha, J. H. Connell, and R. M. Bolle, "An Analysis of Minutiae Matching Strength," Proceedings of audio and video based Biometric person authentication, vol. 2091,Sweden 2001, pp.223-228.
12) T. C. Clancy, N. Kiyavash, and D. J. Lin, "Secure Smart-card based fingerprint Authentication," in Proc. ACM SIGMM Multimedia, Biometrics methods and Applications workshop, 2003, pp. 45-52.
13) K. Jain, L. Hong, S. Pankanti, and R. Bolle, "An identity authentication system using fingerprints," IEEE Transaction, vol. 85, September 1997,pp. 1365-1388.
14) D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, and A. K. Jain, "FVC2002: Fingerprint Verification Competition," in Proc. International Conference Pattern Recognition (ICPR) 2002, pp. 744-747.
15) Y. Dodis, L. Reyzin, and Adam Smith, "Fuzzy Extractors: How to generate Strong Keys from biometrics and other noisy data," Proceedings of International Conference on Theory and Applications of Cryptographic Techniques, 2004, pp. 523-540.
16) B. J. Teoh, A. Goh, and D. C. L. Ngo, "Random Multispace Quantization as an Analytic Mechanism for Bio Hashing of Biometrics and Random Identity Inputs," IEEE Transaction on Pattern Analysis and Machine Intelligence, vol. 28, no. 12,2006, pp. 1892-1901.
17) Anil K. Jain, Ruud Bolle, and Sharath Pankanti, "Biometrics: Personal Identification in Networked Society," Kluwer Academic Publishers, 2009.
18) J. L. Wayman, "Fundamentals of biometric authentication technologies," Int. J. Image graph, vol. 1, no. 1, 2001, pp. 93-113.