ISSN 2229-6956(ONLINE)
DOI: 10.21917/ijsc.2010.0006

A STUDY ON BIOMETRIC TEMPLATE SECURITY

N. Radha[1] and S. Karthikeyan[2]
Department of Computer Science and Engineering, Karpagam University, India
E-mail: lakshmin07@sify.com[1], skaarthi@gmail.com[2]

Abstract
The increasing popularity of biometrics and cryptography is driven by the widespread stipulation on information security. Abundant efforts have been made in developing successful methods in these areas in order to accomplish an enhanced level of information security. There are two dominant issues in information security enhancement. One is to defend the user ownership and control the access to information by authenticating an individual's identity. The other is to make sure the privacy and integrity of information and to secure communication. Cryptography is the science of writing in secret code. Secret-key cryptography and public-key cryptography are the two most important cryptographic architectures. The security of a cryptographic system is reliant on the secrecy of the cryptographic key. Biometric authentication or simply biometrics refers to establishing automatic personal recognition based on the physical and behavioral characteristics of an individual (e.g. face, voice, fingerprint, gait, hand geometry, iris, gene, etc.). Biometrics offers superior security and easier than traditional identity authentication systems (based on passwords and cryptographic keys).Since biometrics characteristics are naturally related with a particular individual, making them insusceptible to being stolen, forgotten, lost or attached. This paper presents a survey on various techniques proposed earlier in developing an authentication system for ensuring individual's information security by combining biometric characteristics of that particular individual and the cryptographic techniques. In addition, it provides some fundamental idea for future research that may help in eliminating the problems associated with the present authentication systems.

Keywords:
Authentication, Cancelable Biometrics, Bio-Cryptosystems, Fuzzy Vault, Multimodal Biometrics, Soft Biometrics

1. INTRODUCTION

The ever-increasing stipulate for further consistent and suitable security systems generates a transformed interest in human identification based on biometric identifiers such as fingerprints, iris, voice and gait. In view of the fact, that biometrics cannot be lost or forgotten like e.g. computer passwords. Biometrics has the prospective to put forward higher security and more convenience for the users. A widespread approach to biometric authentication is to confine the biometric templates of all users during the enrollment phase and to store the templates in a reference database. During the authentication phase new measurements are matched against the database information [26].

The biometric approach for authentication is increasing the security, accuracy, reliability, usability, and friendliness. Moreover, if the biometric templates are captured or if their digital representations are stolen, they cannot be merely replaced or modified in any way, as it can be done with passwords or tokens [1]. Even though biometric authentication approaches are much more secure than the conventional approaches, they are not indestructible. Biometric systems are defenseless to many attacks including replay, database and brute-force attacks.

Both Cryptographic techniques and cancellable biometrics can be used for encryption. The difference between these two approaches is that cancellable biometrics performs matching in transform domains while cryptographic techniques require decryption before feature extraction and/or matching. In other words, decryption is not necessary for cancellable biometrics. When matching speed is an issue, e.g., identification in a large database, cancellable biometrics is more suitable for hiding the private information and when privacy and security of biometric database is required then cryptographic techniques can be used for encrypting the biometric images in the database [14].

Different approach has been presented to concentrate on the problem of supporting personal verification based on human biometric traits, while preserving privacy of digital templates [2]. The majority of approaches depend on jointly exploiting the characteristics of biometrics and cryptography [15] [27]. The most important is that of devising biometric templates and authentication procedures which do not reveal any information on the original biometric traits, for example replicating the usual approach adopted in password-based authentication system. Correspondingly, biometric templates are generated by using appropriate cryptographic primitives so as to save from harm their privacy and make sure that an attacker cannot regain any information on the original biometric trait used for the generation of the template. In this way, user's privacy is guaranteed. Furthermore, even if a template is compromised (stolen, copied, etc.) it is always possible to generate a novel template by starting from the same original biometric trait.

The remainder of this paper is organized as follows. Section II discusses some of the earlier proposed research work on providing security and authentication using biometrics and cryptography. Section III provides a fundamental idea on which the future research work focuses on. Section IV concludes the paper with fewer discussions.

2. RELATED WORK

There are numerous works that suggest the combination of biometrics and cryptography [3] [16] are referred to cancellable biometrics, which uses one way transformation to convert the biometric signal into irreversible form. This section of the paper discusses some of the relevant work proposed earlier in literature for developing a user authentication system using soft biometric characteristics and fuzzy vault scheme.

Nandakumar et al. in [17] described an approach for multibiometric template security using fuzzy vault scheme. Template security is a significant concern in biometric systems for the reason that biometric templates cannot be effortlessly revoked and reissued. Despite the fact that multibiometric systems prevail over limitations such as non-universality and high error rates that have an effect on unimodel biometric systems, they necessitate storage of multiple templates for the same user. Securing the dissimilar templates of a user separately is not most favorable in terms of security. Hence, they proposed a method for securing multiple templates of a user as a single entity. They derived a single multibiometric template from the individual templates and secured it using the fuzzy vault framework. They also demonstrated that a multibiometric vault provides better recognition performance and higher security compared to a single biometric vault. For example, the multibiometric vault based on fingerprint and iris achieves a GAR of 98.2% at a FAR of 0.01%, while the equivalent GAR values of the individual iris and fingerprint vaults are 88% and 78.8%, respectively. Additionally, they also showed that the security of the system is only 41 bits when the iris and fingerprint vaults are stored separately. On the other hand, the multibiometric vault based on fingerprint and iris provides 49 bits of security.

Security analysis was proposed by Zhou et al. in [4]. Biometric features make available substantial usability benefits. At the same time, the lack of ability to invalidate templates and likelihood of adversaries being able to capture features raise security concerns. In recent times, more than a few template protection mechanisms have been proposed, which provide a one-way mapping of templates onto multiple pseudo-identities. At the same time as these proposed schemes make assumptions common for cryptographic algorithms, the entropy of the template data to be protected is considerably lower per bit of key material used than assumed owing to correlations arising from the biometric features. They reviewed several template protection schemes and existing attacks followed by a correlation analysis for a selected biometric feature set and illustrated that these correlations leave the stream cipher mechanism employed vulnerable to, among others, known plaintext-type attacks. Moi et al. in [18] put forth an approach for identity document using iris biometric cryptography. They presented an approach to create a distinctive and more secure cryptographic key from iris template. The iris images are processed to generate iris template or code to be utilized for the encryption and decryption tasks. The international standard cryptography algorithm – AES has been adopted in their work to produce a high cryptographic strength security protection on the iris information. Their proposed approach comprises of two processes. They are encryption and decryption process. Template matching is the process used for pattern recognition. The utilization of biometric as a key is to enhance security in a more efficient way, decrease human mistakes during identification, increase user convenience and automation of security function. Their experimental results revealed that their proposed approach out performed some of the traditional techniques in providing authentication for the user.

A two-phase authentication mechanism for federated identity management systems was described by Abhilasha et al. in [19]. The first phase consists of a two-factor biometric authentication based on zero knowledge proofs. They employed techniques from vector-space model to engender cryptographic biometric keys. These keys are kept secret, thus preserving the confidentiality of the biometric data, and at the same time make use of the advantages of a biometric authentication. The second authentication combines several authentication factors in concurrence with the biometric to make available a strong authentication. A key advantage of their approach is that any unexpected combination of factors can be used. Such authentication system leverages the information of the user that is available from the federated identity management system. Their proposed approach improves privacy, reliability, and security of the biometric data.

Sunil et al. in [5] put forth a novel 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 cancelable biometric features. They proposed a technique to produce cancelable key from fingerprint so as to surmount the limitations of traditional approaches. Cryptography is merged with biometrics in Biometric cryptosystems, otherwise known as crypto-biometric systems [2]. They have introduced the concept of cancelable biometrics that was earlier proposed in [20]. Their approach facilitates the every incidence of enrollment to utilize a distinct transform thus making expose cross matching unachievable. Generally, the transforms utilized for distortion are chosen to be non-invertible. Thus it is not possible to recover the original (undistorted) biometrics despite knowing the transform method and the resulting transformed biometric data.

An effective authentication scheme by combining crypto with biometrics was projected by Hao et al. in [6]. They projected the first practical and secure way to integrate the biometric into cryptographic applications. A repeatable binary string, which we call a biometric key, is generated reliably from genuine iris codes. The key is generated from a subject’s iris image with the support of auxiliary error-correction data, which do not disclose the key and can be saved in a tamper-resistant token, such as a smart card. The reproduction of the key depends on two factors: the iris biometric and the token. The attacker has to get hold of both of them to compromise the key. Moreover they evaluated the technique using iris samples from 70 different eyes, with 10 samples from each eye. As a result they found that an error-free key can be reproduced reliably from genuine iris codes with a 99.5 percent success rate. One can generate up to 140 bits of biometric key, more than enough for 128-bit AES. The extraction of a repeatable binary string from biometrics opens new possible applications, where a strong binding is required between a person and cryptographic operations.

Chung et al. in [7] described a method for biometric based secret key generation for protection mechanism. An authority through a digitally signed data structure called a biometric certificate provides the binding of the user’s identity and biometric feature data to an entity. Therefore, the main goal (or contribution) of their work is to propose a simple method for generating biometric digital key with biometric certificate on fuzzy fingerprint vault mechanism. Biometric digital key from biometric data has many applications such as automatic identification, user authentication with message encryption, etc. Therefore, their work analyzed the related existing scheme and proposed a simplified model where a general fuzzy fingerprint vault using biometric certificate with security consideration.

An intelligent fingerprint based security system was designed and developed by Suriza et al. in [11]. Traditionally, user authentication is meant to provide an identification number or a password that is unique and well protected to assure the overall system security. This type of security system is very fragile in an area where a higher level of security system is required. Biometrics-based system offers a new and better approach to user authentication. Biometrics authentication is an automated method whereby an individual identity is confirmed by examining a unique physiological trait or behavioral characteristic, such as fingerprint, iris, or signature, since physiological traits have stable physical characteristics. The design and development of a fingerprint-based security system, comprising the scanner, interface system, Boltzmann machine neural network and access control system is discussed in their paper. The integration between the hardware and the software is completed by using Visual Basic 6 programming language. The results obtained both for the simulation studies and testing of the integrated system with real-life physical system have demonstrated the practicality of such system as well as its potential applications in many fields.

Dutta et al. in [21] presented a novel method for providing security using biometric and cryptography. They proposed a biometrics-based (fingerprint) Encryption/ Decryption Scheme, in which unique key is generated using partial portion of combined sender's and receiver's fingerprints. From this unique key a random sequence is generated, which is used as an asymmetric key for both Encryption and Decryption. Above unique Key is send by the sender after watermarking it in sender's fingerprint along with Encrypted Message. The computational requirement and network security features are addressed. Proposed system has an advantage that for public key, it has not to search from a database and security is maintained.

A method for enhancing the security of biometrics, cryptography and data hiding was proposed by Dong et al. in [12]. In their paper, they endeavor to present an outline of the state-of-the-art of research in this increasingly imperative topic by putting biometrics, cryptography and data hiding in the same context of security enhancement. Given the practical importance of cryptographic keys and biometric templates, their primary focus will be on methods which seek combinations of biometrics, cryptography and data hiding to improve the security of these keys and templates. Their paper is anticipated to afford a reference point for newcomers and to promote more activities in this important area. The most capable solution to security enhancement of biometrics and cryptography is perhaps the so-called fuzzy vault scheme where the safety of cryptographic keys and biometric templates is bounded in a two-in-one fashion.

Soutar et al. in [13] projected a new, more advanced approach of biometric-key binding algorithm using an optical correlation based fingerprint matching system. Their algorithm binds a cryptographic key with the user's fingerprint images at the time of enrollment and uses Fourier processing to pay compensation for fingerprint image displacement. A filter is designed in order to obtain a tradeoff between distortion tolerance and discrimination of these images. A key with 128 bits is associated to the output data by means of a lookup table and an error correcting code. Analogous work was done on palmprint cryptosystem in [22]. A 1024-bit binary string is extracted from the palmprint images using differential operations and then translated to a 128 bits encrypting key using a hash function with error correcting code.

Clancy et al. in [23] put forth a fingerprint vault. A combination of biometrics and cryptography has the prospective to make available a higher assurance of the legal information holder. At the enrollment, five fingerprints of a user are acquired. The fingerprint minutiae position is extracted from each fingerprint. Correspondence between the minutiae from the five fingerprints is established based on a bounded nearest-neighbor algorithm. Then the vault is created using polynomial encoding and error correction, combined with the chaff points. Satisfying results are obtained in their experiments. The limitation of their work is that it assumes the fingerprints are pre-aligned and it is also not clear about their database used in their experiments.

A new technique called biohashing was introduced and applied to face images by Goh and Ngo in [8]. A set of random orthogonal vectors (which are kept secret) are generated and an inner product between each vector and the biometric feature set is computed and binarized to produce a 80-bits key with a 0.93% false rejection rate for the system. Their work also begins a parameters based bio-cryptosystem. Monrose et al. in [9] introduced a technique called biometrically hardened passwords. It deals with keystroke dynamics or voice recognition. A password provided by the user is pre-pended by a key extracted from a biometric component, thus making the password hardened with the biometrics. Martini and Beinlich in [24] proposed a virtual PIN scheme, which is practically identical to the fuzzy commitment scheme [15].

Amioy kumar et al. in [10] described an approach for the development of new cryptographic construct using fuzzy vault. The integration of cryptology and biometrics has come into view as promising constituent of information security. Despite the current popularity of palmprint biometric, there has not been any challenge to examine its usage for the fuzzy vault. Their paper consequently investigates the achievable usage of palmprint in fuzzy vault to build up a user friendly and consistent crypto system. They suggested the use of both symmetric and asymmetric approach for the encryption. The ciphertext of any document is generated by symmetric cryptosystem; the symmetric key is then encrypted by asymmetric approach. Additionally, Reed and Solomon codes are used on the generated asymmetric key to provide some error tolerance while decryption. The experimental results from the proposed approach on the palmprint images advocated its possible usage in an automated palmprint-based key generation system.

Biometrics based asymmetric cryptosystem design was put forth by Nagar et al. in [25]. They put forth a new biometrics cryptosystem where one can send and receive secure information using just the fingerprints. This cryptosystem is a well thought-out intermingles of the asymmetric cryptosystem like RSA and the symmetric fuzzy vault scheme having the advantages of both the aforementioned crypto systems. They have proposed a modification of the fuzzy vault scheme to make it more forceful against variations in the values of biometric features. To end with, they proposed the use of invariant features as a key to producing a hierarchical security system where the same key (fingerprint) can be used to generate encrypted messages at different levels of security.

3. FUTURE ENHANCEMENT

Even though considerable advancement has been made in security enhancement of biometrics and cryptography over the past decade, much remains to be done. Since each single biometric modality has its own weaknesses. It may not be adequate to provide more security that is required for all the applications. For this reason, the multibiometric models and multi factor authentication systems, schemes that simultaneously secure multibiometric templates and multiple authentication factors deserve further study. Growing efforts are being made to get rid of the limitations and to further enhancement in information security by taking advantage of the respective strength of biometrics and cryptography. Additional efforts has to be made on building the bridge between the fuzziness of biometric matching and the exactness of cryptographic key validation.. Moreover, a larger and common database should be built for performance evaluation of bio-cryptosystems. An assortment of cryptographic techniques has been applied to save biometric template.

4. CONCLUSION

In this paper, we have presented a concise overview on the state-of-the-art of research on the Biometric template security using cryptographic techniques against identity theft and various security related threats. Biometric authentication is becoming a most popular and most reliable user authentication mechanism. Even it is vulnerable to attacks. The interest in biometric approaches for authentication is increasing for their advantages such as security, accuracy, reliability, usability, and friendliness. Several methods have been suggested in the literature to protect biometric templates from informative essential private information. The best way of securing template from unauthorized persons during transmission or storage is encryption. The security of a cryptographic system is reliant on the secrecy of the cryptographic key. Biometrics offers superior security and easier than traditional identity authentication systems (based on passwords and tokens). Since biometrics characteristics are naturally related with a particular individual, making them insusceptible to being stolen, forgotten, lost or attached. Additional efforts should be made on building the bridge between the fuzziness of biometric matching and the exactness of cryptographic key validation.

REFERENCES

[1] B. Schneier, 1999, “The uses and abuses of biometrics”, Communication of the ACM, Vol. 42, No. 8: pp. 136.

[2] U. Uludag, S. Pankanti, S. Prabhakar, and A. Jain, 2004, “Biometric cryptosystems: Issues and challenges”, In Proceedings of the IEEE, Special Issue on Enabling Security Technologies for Digital Rights Management, Vol. 92: pp.948–960.

[3] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, 2007, “Generating Cancelable fingerprint templates”, IEEE Transactions on Pattern Analysis and Machine Learning, Vol. 29, No. 4: pp. 561-572.

[4] Xuebing Zhou, Stephen D. Wolthusen, Christoph Busch and Arjan Kuijper: 2009, “A Security Analysis of Biometric Template Protection Schemes, Image Analysis and Recognition”, Springer link:pp. pp. 429-438.

[5] Sunil V. K. Gaddam, and Manohar Lal, 2010, “Efficient Cancelable Biometric Key Generation Scheme for Cryptography”, International Journal of Network Security, Vol.11, No. 2: pp. 57-65.

[6] Feng Hao, Ross Anderson, and John Daugman, 2006, “Combining Crypto with Biometrics Effectively”, IEEE Transactions on Computers, Vol. 55, No. 9: pp. 1081-1088.

[7] Yunsu Chung, Kiyoung Moon, and Hyung-Woo Lee, 2007, “Biometric Certificate Based Biometric Digital Key Generation with Protection Mechanism”, Frontiers in the Convergence of Bioscience and Information Technologies, pp. 709-714.

[8] Goh and D. C. L. Ngo, 2003, “Computation of cryptographic keys from face biometrics”, International Federation for Information Processing, Vol. 2828.

[9] F. Monrose, M. K. Reiter, and R. Wetzel, 2002, “Password hardening based on keystroke dynamics”, International Journal on Information Security, Springer, Vol. 1, No. 2: pp. 69-83.

[10] Amioy Kumar and Ajay Kumar, 2009, “Development of a New Cryptographic Construct Using Palmprint-Based Fuzzy Vault”, EURASIP Journal on Advances in Signal Processing, Vol. 2009.

[11] Suriza Ahmad Zabidi, and Momoh-Jimoh E. Salami, 2004, “Design and Development of Intelligent Fingerprint-Based Security System”, Knowledge-Based Intelligent Information and Engineering Systems, Book Chapter on Springer link, Vol. 3214: pp. 312-318.

[12] Jing Dong and Tieniu Tan, 2003,”Security Enhancement of Biometrics”, Cryptography and Data Hiding by Their Combinations.

[13] C. Soutar and D. Roberge, 1999, “Biometric encryption”, ICSA Guide to Cryptography, McGraw-Hill.

[14] Saroj Kumar Panigrahy, Debasish Jena, Sathya Babu Korra, and Sanjay Kumar Jena, 2009, On the Privacy Protection of Biometric Traits: “Palmprint, Face, and Signature,” CCIS: pp. 182–193.

[15] Juels, and M. Wattenberg, 1999, “A fuzzy commitment scheme”, In Proceedings of the 6th ACM conference on Computer and communications security (CCS 1999): pp.28–36, ACM Press, New York.

[16] M. Savvides, B. V. K. V. Kumar, and P. K. Khosla, August 2004, “Cancelable Biometric filters for face recognition”, Proceedings of ICPR, Vol. 3: pp. 922-925, Cambridge, UK.

[17] K. Nandakumar, and A. K. Jain, 2008, “Multi biometric Template Security Using Fuzzy Vault”, 2nd IEEE International Conference on Biometrics: Theory, Applications and Systems: pp. 1-6.

[18] Sim Hiew Moi, Nazeema Binti Abdul Rahim, Puteh Saad, Pang Li Sim, Zalmiyah Zakaria, and Subariah Ibrahim, 2009, “Iris Biometric Cryptography for Identity Document”, IEEE Computer Society, International Conference of Soft Computing and Pattern Recognition: pp. 736-741.

[19] Abhilasha Bhargav-Spantzel, Anna Squicciarini, and Elisa Bertino, 2006, “Privacy preserving multi-factor authentication with biometrics”, Conference on Computer and Communications Security: pp. 63-72.

[20] R. Ang, R. Safavi-Naini, and L. McAven, 2005, "Cancelable key-based fingerprint templates", ACISP 2005: pp.242-252.

[21] Sandip Dutta, Avijit Kar, N. C. Mahanti, and B. N. Chatterji, 2008, "Network Security Using Biometric and Cryptography", Proceedings of the 10th International Conference on Advanced Concepts for Intelligent Vision Systems: pp. 38-44.

[22] K. Wang, X. Wu and D. Zhang, 2007, "A palmprint cryptosystem", In Proceedings of International Conference of Biometrics: pp. 1035–1042.

[23] T. C. Clancy, N. Kiyavash, and D. J. Lin, 2003, "Secure smartcard-based fingerprint authentication", In Proceedings of ACMSIGMM, Vol. 4263: pp. 45–52.

[24] U. Martini and S. Beinlich, Virtual, 2003, "Biometric encryption using coding theory", In Proceedings of the 1st Conference on Biometrics and Electronic Signatures of the GI Working Group: pp. 91-99.

[25] Nagar and S. Chaudhury, August 2006, "Biometrics based asymmetric cryptosystem design using modified fuzzy vault scheme", in Proceedings of the 18th International Conference on Pattern Recognition (ICPR '06), Vol.4 : pp.537–540, Hong Kong,

[26] Pim Tuyls and Jasper Goseling, 2006, "Capacity and Examples of Template-Protecting Biometric Authentication Systems".

[27] F. Hao, R. Anderson, and J. Daugman, July 2005, "Combining cryptography with biometrics effectively", Technical Report UCAMCL-TR 640, Computer Laboratory, University of Cambridge, United Kingdom.