International Journal For Technological Research In Engineering
Volume 5, Issue 10, June-2018 *ISSN (Online): 2347 - 4718*

A REVIEW ON BIOMETRIC TEMPLATE SECURITY

Shikha[1], Paru Raj[2]
[1]Student, [2]Assistant Professor,
Department of Computer Science Engineering, Prannath Parnami Institute of Management and Technology, Chaudharywas, Hissar, Haryana, India

ABSTRACT: With the rapid increase in number of biometric recognition systems, an attacker's benefit in staging a system compromise is also increasing and thus is the need to ensure system security and reliability. This dissertation grants a thorough analysis of the vulnerabilities of a biometric recognition system with emphasis on the vulnerabilities related to the information stored in biometric systems in the form of biometric templates. To encourage the improvement of techniques to protect biometric templates, we show the use of biometric cryptography in the existing systems. While biometric cryptosystems permit binding a secure key to the biometric data to obtain a so called secure sketch from which no information regarding the biometric data or the key can be retrieved again, cancelable biometric template transformation techniques non-invertibly transform the biometric template with the user's password. To analyze and improve the biometric cryptosystems, we have studied its two main examples: fuzzy vault and the fuzzy commitment. Fuzzy vault is the technique used to secure templates characterized in the form of a finite set of points whereas fuzzy commitment is used for the security of templates represented as binary vectors. A superior security analysis is provided that makes biometric template more secure. A framework to effectively combine multiple biometric representations and efficiently verify an individual is also proposed. Various template transformation techniques proposed in literature are studied and the amount of security they impart is evaluated using a comprehensive set of metrics. First, we analyze the weak points of biometrics and mentioned existing system and make it strong by applying cryptography. The proposed approaches are shown to be very successful in improving the security of biometric devices. We believe that the security analysis presented in this dissertation will streamline the development of new techniques and help in finding a robust solution for protecting biometric data.

I. INTRODUCTION

In todays modern and high-tech world the security concern is highly significant to overcome the imposters and the fake authenticated users for the authentication purposes. To identify a person with a high confidence is a seriousissue in various applications, such as access control,passenger clearance,e-banking, etc.. It is well known that humanbeings instinctively make use of somebody characteristics, e.g. face, gait, or voice, torecognize each other. A biometric system is basically a pattern recognition system that acquires biometricdata from an individual, extracts a salient feature set and compares this featureset against the feature set(s) stored in the database, and takes an action based on the result of the comparison. Figure 1.1 shows the generic architecture of a typicalbiometric system.

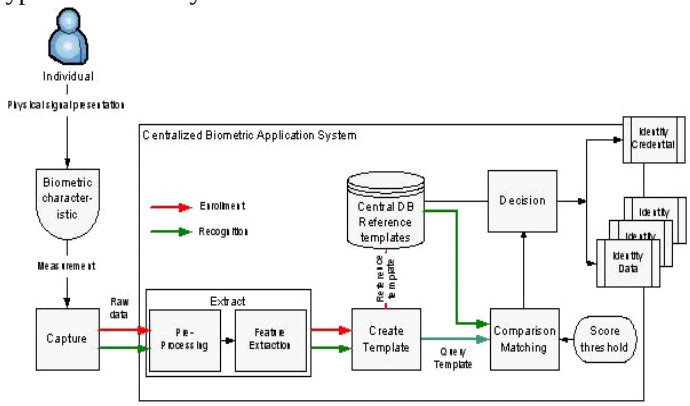


Figure 1.1 Architecture of a Biometrics System.

Establishing (determining or verifying) the identity of a person is called personrecognition or authentication and it is a critical task in any identity management system [1]. Therefore, it is apparent that knowledge-based and token-based mechanisms alone are insufficient for reliable identity purposes and strongerauthentication schemes based on "something you are", namely biometrics, are needed.Biometric systems have now been used in variouscivilian,forensic, andcommercial applications as a means of establishing identity

II. BIOMETRIC SYSTEM

A number of physical and behavioral body traits can be used for biometric recognition(see Figure 1.2). Examples of physical traits include face, fingerprint, iris, palm print,hand geometry and ear shape. Gait, signature and keystroke dynamics are some of thebehavioral characteristics that can be used for person authentication. Therefore, there is no universally best biometric trait and the choice of biometric dependson the nature and requirements of the applicationAs identified by Ross et al., there areseven factors that can determine the suitability of a physical or behavioral trait to be usedas a biometric identifier, including:

Universality: it means that every person should possess the trait.

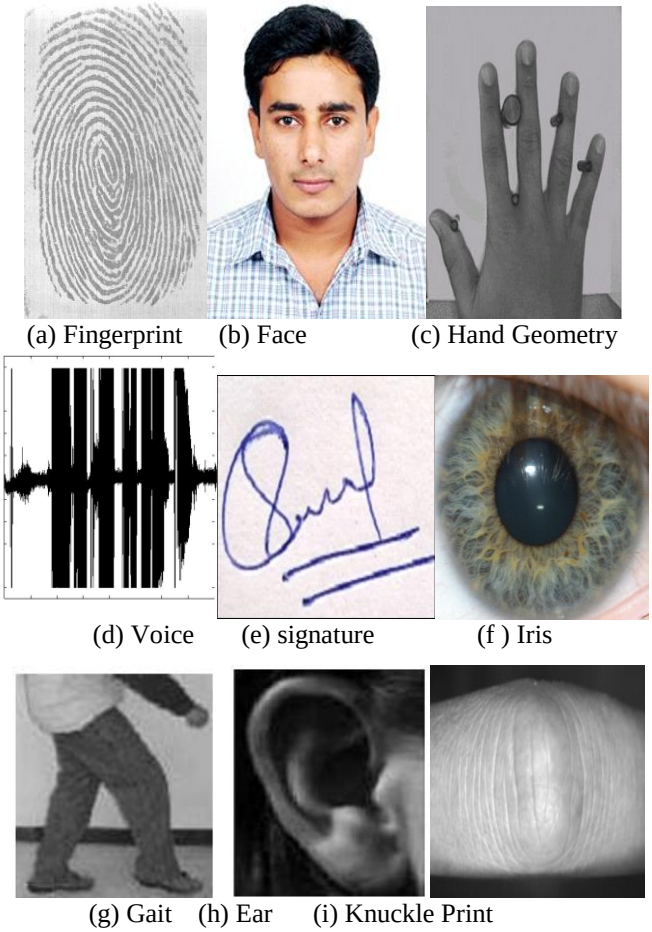
Uniqueness: it indicates that no two persons should be the same in terms of the trait.

Permanence: it means that the trait should not change with time. A trait that changes significantly with time is not a good biometric trait.

Collectability: it means that it should be possible to acquire

 Copyright 2018.All rights reserved.

and digitize the trait using suitable devices without causing any inconvenience to user.
Performance: it refers to the possible recognition speed, robustness, accuracy, and the resources required to achieve the accuracy and speed.



(a) Fingerprint (b) Face (c) Hand Geometry
(d) Voice (e) signature (f) Iris
(g) Gait (h) Ear (i) Knuckle Print

Figure 1.2: Some of the body traits that can be used for biometric recognition

III. LITERATURE REVIEW

Soutar et al[1].suggested an approach named as Mytec1 and Mytec2 (Biometric Encryption TM):the first refined approach to biometric key-binding based on fingerprints images. The existingsystem was called Mytec2, Mytec1 is predecessor of Mytec2, which were the first BCS but turned out to beunrealistic in terms of security and accuracy. Mytec1 and Mytec2 were formerly calledBiometric Encryption TM; the brand was abandoned in 2005. The base of the Mytec2 andMytec1 algorithm is the method of relationship.

Zheng et al.[2] use error tolerant lattice functions. In test a FRR of _3.3% and a FAR of _0.6% are accounted. Dodis et al.initiated the so-called syndrome production.
Juels and Sudan in 2002 establishes one of the most accepted BCSs called fuzzy vault.

Clancy et al[3]. introdued the first realistic and most obvious execution of the fuzzy vault scheme by catching minutiae points in a fingerprint vault‖. Minutiae points st, A, are record onto a polynomial p and chaff points are arbitrarily added to create the vault. During authentication, Reed-Solomon codes are used to recreate a 128-bit key of the polynomial p. A pre-arrangement of fingerprints is supposed which is seldom the case in practice (feature arrangement signifies a basic step in conventional fingerprint recognition systems).
Buhan et al[4] have exposed that there is a direct relation between the error rates of the biometric system and the maximum length k of cryptographic keys. The authors describe the relation, which has well-known as one of the most general matrices used to compute the entropy of biometric inputs. This means that a best BCS would have to preserve an FAR 2logk which shows to be a fairly rigorous upper bound that may not be feasible in practice.
Vielhauer et al[5]. explained the issue of deciding important features of online signatures and establish three measures for feature estimation: inter personal entropy of hash value components, intra personal feature deviation, and the relationship between both. By examining the distinctiveness of chosen features the authors show that the used feature vector can be compact by 45% preserving error rates.
Boult et al[6].projected cryptographic secure bio tokens which they practical to fingerprints and face. To improve security in biometric systems, which they refer as Biotope TM, are accepted to existing identification schemes (e.g. PCA for face).
It is stated that MRP (which is applied to speech and face) retains identification performance in the fake token scenario. Additionally, the authors projected a technique to produce cancelable keys out of active hand signatures based on the arbitrary mixing step of Bio Phasor and user-particular 2N discretization. To offers CB removed features are arbitrarily mixed with a token T using a Bio Phasor integration method.

IV. CONCLUSION

With the rapid increase in number of biometric recognition systems in commercial sector, security of the stored biometric data is increasingly becoming crucial. As assessed in this dissertation, current biometric systems have a number of vulnerabilities and a motivated adversary can undoubtedly cause severe harm to a biometric system as well as the users enrolled in the system. Furthermore, due to the permanent nature of biometrics data its theft and misuse may be irreparable. If someone‘s fingerprints or iris patterns are stolen and are falsely linked to high susceptibility of a dreaded disease, the person may be unable to obtain a medical insurance. Stolen biometric data may devoid a person of any conveniences offered by the biometric systems due to the concern of being easily impersonated using spoof biometrics. While these threats may not appear to be imminent, the spaces at which biometric systems are increasing rapidly, the wealth of information one may harness by staging extensive theft of biometric data would definite motivate the con men.

The developed technique shows a significant improvement in terms of security as it combines the advantage of cryptography and cancelable biometrics. The system can be used for any biometric trait and can also be successful in

 Copyright 2018.All rights reserved.

multibiometric systems and hence will make a multibiometric system simpler as well as secure. The other proposed system is also developed which is overcomes the problem of time and cost in multimodal biometrics. The system can be used to efficiently verify a person in a simple way. Hence, in future we can use the former approach to be used in multimodal biometrics and and we can also extend the system for various other attack points.

REFERENCES

[1] C. Soutar, D. Roberge, A. Stoianov, R. Gilroy, and B. V. K. Vijya Kumar, ―Biometric Encryption Using Image Processing‖, im proceedings of SPIE, optical security and counterfeit deterrence techniques II, volume 3314, pages 178- 188, 1998.

[2] G. Zheng, W. Li, and C. Zhan, ―Cryptographic key generation from biometric data using lattice mapping,‖ 18th Int. Conf. on Pattern Recognition (ICPR 2006), vol. 4, pp. 513–516, 2006.

[3] T. C. Clancy, N. Kiyavash, and D. J. Lin, ―Secure smartcard-based fingerprint authentication,‖ Proc. ACM SIGMM 2003 Multimedia, Biometrics Methods and Applications Workshop, pp. 45–52, 2003.

[4] I. R. Buhan, J. M. Doumen, P. H. Hartel, and R. N. J. Veldhuis, ―Fuzzy extractors for continuous distributions,‖ University of Twente, Technical Report, 2006.

[5] C. Vielhauer, R. Steinmetz, and A. Mayerh¨ofer, ―Biometric hash based on statistical features of online signatures,‖ in ICPR ‘02: Proc. of the 16 th Int. Conf. on Pattern Recognition (ICPR‘02) Volume 1, 2002, p. 10123.

[6] T. Boult, ―Robust distance measures for face-recognition supporting revocable biometric tokens.‖ in FGR ‘06: Proc. of the 7th Int. Conf. on Automatic Face and Gesture Recognition, 2006, pp. 560–566

 Copyright 2018.All rights reserved.