ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 7, July 2015

An Approach for Iris Template Protection using Behavioral Trait

Sheetal Chaudhary[1], Rajender Nath[2]

Post Doctoral Fellow, Department of Comp. Sc. & App., Kurukshetra University, Kurukshetra, India[1]

Professor, Department of Comp. Sc. & App., Kurukshetra University, Kurukshetra, India[2]

Abstract: Biometric recognition refers to recognizing a person based on one or more of his/her physical (fingerprint, face, iris, hand geometry etc.) or behavioral (signature, voice, keystroke dynamics etc.) traits. Biometric traits are intrinsically associated with persons and cannot be forgotten or shared with others. Physical traits are stable, unique and do not change significantly in time as compared to behavioral traits. However, one of the most significant vulnerabilities of biometrics is that once a biometric template is compromised, it cannot be canceled and reissued. An attacker could then gain access to all the applications using that same biometric trait. In this paper, a new approach is proposed for protection of iris template using behavioral trait. Behavioral trait is only used to generate user specific key. It presents an effective combination of biometrics data with user specific biometric key for human recognition to generate cancelable and non-invertible biometric templates. Neither the key nor the image can be recovered from the resulting template. The gain obtained from the proposed approach is two-fold: cancelability and non-invertibility. Experimental evaluations are performed on a public dataset demonstrating the accuracy of proposed approach.

Keywords: Iris biometric, voice biometric, biometric template, security, user specific key, cancelability.

I. INTRODUCTION

Biometrics provides a reliable and natural solution in establishing the identity of an individual based upon person's unique body features. Acceptability of biometric systems depends upon system robustness, low error rates, high recognition performance, difficult to circumvent and user convenience. It is an essential tool in meeting the increased security requirements in a variety of applications, so vulnerabilities of the biometric system must be identified and addressed systematically. Biometric systems may become vulnerable to various potential attacks .

Some of these security vulnerabilities includes the following [1]:

- Spoofing - A biometric system sometimes can be fooled by applying fake fingerprints, face or iris image, etc.
- Replay attacks - e.g. circumventing the sensor by injecting a recorded image in the system input. It is much easier than attacking the sensor.
- Substitution attack - The biometric template must be stored to allow user verification. If an attacker gets an access to the storage, either local or remote, he/she can overwrite the legitimate user's template with his/her own stealing their identity.
- Tampering - Feature sets on verification or in the templates can be modified in order to obtain a high verification score, no matter which image is presented to the system.
- Masquerade attack - It was demonstrated that a digital "artefact" image can be created from a fingerprint template, so that this artefact, if submitted to the system, will produce a match. The artefact may not even resemble the original image. This attack poses a real threat to the remote authentication systems, since an attacker does not even have to bother to acquire a genuine biometric sample. All he needs is just to gain an access to the templates stored on a remote server.
- Trojan horse attacks - Some parts of the system, e.g. a matcher, can be replaced by a trojan horse program that always outputs high verification scores.
- Overriding Yes/No response - An inherent flaw of existing biometric systems is due to the fact that the output of the system is always a binary Yes/No (i.e., match/no match) response. In other words, there is a fundamental disconnect between the biometric and applications, which make the system open to potential attacks. For example, if an attacker were able to interject a false Yes response at a proper point of the communication between the biometrics and the application, he could pose as a legitimate user to any of the applications, thus bypassing the biometric part.

With the widespread deployment of biometric systems in various applications, there are increasing concerns about the security of biometric technology. Despite the numerous advantages of biometrics, some disadvantages also exist when compared to passwords. One of the disadvantages of biometrics is that once a biometric image or template is stolen, it is stolen forever and cannot be reissued, updated, or destroyed. Another problem associated with the use of biometrics is that once a biometric is chosen, the same biometric will be used to access many different systems. This means that, if it is compromised, the attacker will have access to all the applications. In contrast, password based authentication systems have the capability to cancel the compromised password and reissue the new one [2].

The rest of this paper is organized as follows. Section 2 discusses the related work. Section 3 presents the proposed

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 7, July 2015

architecture for a secure biometric recognition system combining iris with voice. Results and discussion are given in section 4. Finally, the summary and conclusions are given in last section.

II. RELATED WORK

The advent of biometrics has introduced a secure and efficient alternative to traditional authentication schemes (token based and knowledge based). A lot of work has been done in the last years in the field of iris and voice recognition yielding mature techniques.

Iris recognition using analysis of the iris texture has attracted a lot of attention and researchers have presented a variety of approaches in the literature. Daughman [3] proposed the first successful implementation of an iris recognition system based on 2-D Gabor filter to extract texture phase structure information of the iris to generate a 2048 bits iris code. Narote et al [4] proposed an algorithm for iris recognition based on dual tree complex wavelet transform and explored the speed and accuracy of the proposed algorithm. Kumar and Passi [5] presented a comparative study of the performance from the iris identification using different feature extraction methods with different templates size. Tisse et al. [6] proposed a segmentation method based on integro-differential operators with a Hough Transform. This reduced the computation time and excluded potential centers outside of the eye image. Ma et. al. [7] processed iris segmentation by simple filtering, edge detection and Hough Transform. In Masek's segmentation algorithm [8], the two circular boundaries of the iris are localized in the same way using the canny edge detector and circular Hough Transform.

Voice is a behavioral biometric which can be used in identity verification, especially over-the-phone applications such as banking. With largely available telephone networks and cheap microphones on computers, user recognition through speech becomes a natural solution. In literature, various text-independent methods have been proposed, some of which are quite successful with equal error rates under 2% using private databases [9]. On the other hand, text-dependent systems provide the flexibility of changing the biometric by changing the spoken text. Bellegarda et al introduced a text-dependent system by using singular value decomposition for spectral content matching and dynamic time warping for temporal alignment of the utterances. They have achieved an EER of 4% in a database of 93 speakers [10]. Li et al proposed a method employing Hidden Markov Models for the alignment of utterances with a global phoneme model and achieved an EER of 2.6% with a database of 100 speakers [11]. A lot of work has been done in this field and generated a certain number of applications of access control for telephone companies [12].

Security is another major concern in building biometric systems, besides low error rates. The template protection schemes proposed in the literature can be broadly classified into two categories, feature transformation approach and biometric cryptosystem approach [13]. Numerous architectures have been proposed in recent years, aiming to protect biometric templates stored in central repositories [14]. Among those, fuzzy vault technique is one of the most widely used methods where the fingerprint minutiae points are stored with randomly generated chaff points [15]. Yanikoglu and Kholmatov proposed another method based on the idea of combining multiple biometrics in order to increase both privacy and security [16] [17]. Brunelli and Falavigna used the hyperbolic tangent for normalization and weighted geometric average for fusion of voice and face biometrics [18]. Kittler et al have experimented with fusion techniques for face and voice on the matching score level [19]. Hong and Jain proposed an identification system using face and fingerprint where the database is pruned via face matching before fingerprint matching [20].

III. PROPOSED WORK

The most potentially damaging attack on a biometric system is against the biometric templates that are stored in the system database. To defeat the problems related with template security (misuse of templates, modifying an existing template, stolen templates etc.), a new approach is proposed that represents an effective combination of physical biometric trait (iris) with behavioral biometric trait (voice) for making iris template more secure. It is based on the biometric encryption process [1] [21] which securely bind a randomly generated key to a biometric, so that neither the key nor the biometric can be retrieved from the stored template. Here, the key is linked with the biometric at a more fundamental level during enrollment, and is later retrieved using the biometric during verification.

A. Architecture of proposed approach

Fig. 1 shows the architecture of the proposed approach combining iris with voice pattern to generate a secure, cancelable and non-invertible iris template. It consists of two processes: enrollment process and verification process. The feature set extracted from iris image is represented as IrisCode that is the 2048-bit binary representation of an iris [22] and feature set extracted from voice pattern is represented as a vector consisting of $MFCC_s$ (mel frequency cepstral coefficients) [17].

Voice feature set is given as input to the key generation module to generate a user specific key from it. Voice pattern is required only to generate user specific key during enrollment phase. For security purposes, it is better to use user specific key than randomly generated key. The reason for using behavioral trait to generate key is that it is changeable or cancelable as compared to physical trait. If the template stored in the database seems to be compromised, it can be regenerated by changing the voice pattern and generating new key. But this is not the case with physical traits because once stolen these are compromised forever. By integrating iris with voice, it is also benefited with the advantages of multimodal biometric systems. Voice biometric alone is not sufficient for recognition to systems that require high security. But it becomes more powerful when used in conjunction with another form of authorization, such as physical biometric

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 7, July 2015

traits. There is no storage of original biometric image and user specific key in the database as these are discarded when template is generated. Thus, it eliminates the possibility of data misuse. Also, there is no threat of substitution attacks because the attacker cannot create his own template since he does not know biometric image and user specific key that had been used to create the legitimate template. A large number of templates for the same biometric can be created for different applications and thus making impossible to link together templates from multiple applications. The template stored in database is non-invertible as neither the biometric (iris) nor the key (voice) can be independently obtained from it. A Yes/No response (one bit of information) generated by other biometric systems is susceptible to be overridden by hackers. Thus as a final result, instead of producing simple Yes/No response, it facilitates key release for user verification. This makes it more secure.

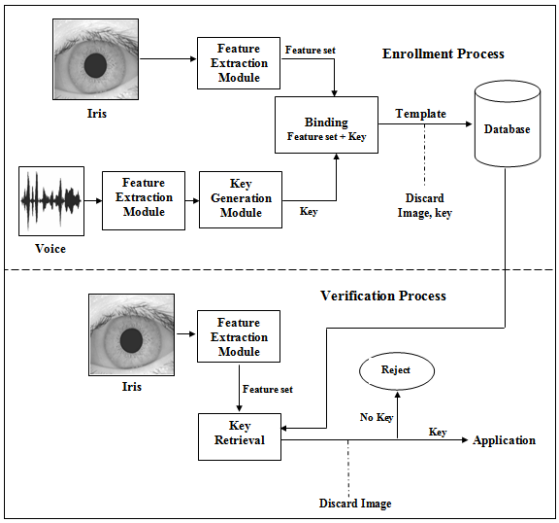

Fig. 1 Architecture of proposed approach

B. User specific key generation from voice

Voice biometric uses the pitch, tone, and rhythm of speech. Each person's voice differs in pitch, tone, and volume enough to make it uniquely distinguishable. Several factors contribute to this uniqueness: size and shape of the mouth, throat, nose, and teeth, which are called the articulators and the size, shape, and tension of the vocal cords. The chance that all of these are exactly the same in any two people is low. The manner of vocalizing further distinguishes a person's speech: how the muscles are used in the lips, tongue and jaw. Speech is produced by air passing from the lungs through the throat and vocal cords, then through the articulators. Different positions of the articulators create different sounds. This produces a vocal pattern that is used in the analysis [23].

The feature vector generated from voice pattern is represented by a 12 dimensional vector $\{\Phi_1, \Phi_2, \ldots, \Phi_{12}\}$. The approach for generating a key from biometrics requires that there must be a way of mapping $\{\Phi_1, \Phi_2, \ldots, \Phi_{12}\}$ to an m-bit key (k). The *i*-th bit k(*i*) of key k could be obtained by comparing Φ_1 to a fixed threshold and assigning k(*i*) to be 0 or 1 depending on whether Φ_1 was less than or greater than the threshold. Ideally, it should separate users in the sense that keys produced by the same user are "sufficiently similar" (i.e., small intra-user variation), but ones produced by different users are "sufficiently different" (i.e., large inter-user variation) [24].

C. Proposed algorithm

The steps involved in the proposed algorithms can be summarized as given below:

Algorithm: Key Binding Process
Begin
(i) Obtain Iris image using appropriate sensor.
(ii) Generate Feature set from Iris image.
(iii) Obtain Voice pattern using appropriate sensor.
(iv) Generate Feature set from Voice pattern.
(v) Generate user specific key from Voice.
(vi) Apply Biometric Encryption Process
  a. Bind the user specific key with Iris Feature Set.
  b. Generate secure and cancelable Iris template.
  c. Discard Biometric image and key.
  d. Store template in the database.

End

Algorithm: Key Retrieval Process
Begin
(i) Obtain current Iris image of the person to be verified.
(ii) Generate Feature set from Iris image.
(iii) Apply Biometric Encryption Process
  a. Compare Feature set with template stored in the database to retrieve key.
  If (key is retrieved)
    User is verified / authenticated.
  Else
    User is rejected / not authenticated.
  b. Discard Biometric image.

End

IV. RESULTS AND DISCUSSION

This paper describes how the security of traditional iris recognition system can be improved by integrating it with behavioral biometrics. The proposed approach was implemented using MATLAB. The sample biometric data for iris and voice was taken from CASIA database [25] and XM2VTS database [26] respectively.

To calculate the performance of proposed approach, ROC curve is plotted for Genuine Accept Rate (GAR) against False Accept Rate (FAR) by applying different threshold values as shown in Fig. 2.

FAR is the percentage of imposter pairs whose matching score is greater than or equal to threshold value. GAR (1-FRR) is the fraction of genuine scores exceeding the threshold value. False Reject Rate (FRR) is the percentage of genuine pairs whose matching score is less than threshold value.

Table 1 shows comparison between GAR of the proposed approach and traditional iris [27] recognition system.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 7, July 2015

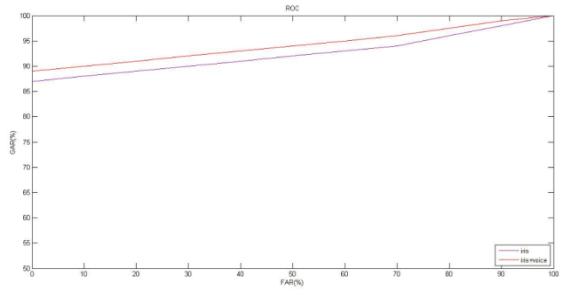

Fig. 2 ROC curve showing the performance of proposed approach

An improvement in the Genuine Acceptance Rate (GAR) can be observed from Table 1 over a wide range of values of False Acceptance Rate (FAR). Thus, it can be concluded from Fig. 2 and Table 1 that the proposed approach has improved recognition performance as compared to the traditional iris recognition system.

TABLE I: COMPARISON BETWEEN GAR OF PROPOSED APPROACH AND EXISTING SYSTEM

S.No.	FAR (%)	Existing Iris System GAR (%)	Proposed (Iris + Voice) Approach GAR (%)
1	0	87	89
2	30	90	92
3	60	93	95
4	80	96	97.5
5	90	98	99

V. CONCLUSION

With the widespread deployment of biometric recognition systems in various applications, security of biometric templates has become an important issue because compromised biometric templates cannot be canceled and reissued. In this paper, a new approach has been proposed to improve security of iris template by integrating iris with voice. Here, voice is used only to generate user specific key to bind with biometric image of iris. The key is completely independent of the biometric data, thus allowing the key to be easily modified or updated if template gets compromised. Behavioral trait is changeable and thus provides the ability to cancel the compromised template and generate new key to reissue the template. The proposed approach requires no storage of biometric image or conventional template, thus the original biometric image or the key cannot be recreated from the template stored in the database. Experiments are conducted to investigate the performance of the proposed approach. ROC curve show that the proposed approach gives a considerable performance over traditional system where no methodology is used for template protection. Future work will be focused on inclusion of liveness detection as it will provide a better solution for increased security requirements.

REFERENCES

[1] Ann Cavoukian, Alex Stoianov, "Biometric Encryption: A Positive-Sum Technology that Achieves Strong Authentication, Security AND Privacy", March 2007.
[2] B. Schneier, "Inside Risks: The Uses and Abuses of Biometrics", Communications of the ACM, Vol. 42, No. 8, pp. 136, August 1999.
[3] C. Chena, C. Chub. "High Performance Iris Recognition based on 1-D Circular Feature Extraction and PSO–PNN Classifier". Expert Systems with Applications journal, 36(7): 10351-10356, 2009.
[4] A. Poursaberi,B.N. Araabi. "Iris Recognition for Partially Occluded mages: Methodology and Sensitivity Analysis". EURASIP Journal on Advances in Signal Processing, 2007(1): 12-14, 2007.
[5] C. Tisse, L.Martin, L. Torres, and M. Robert, "Person identification technique using human iris recognition," In Proceedings of ICVI'02, 294–299, (2002).
[6] L. Ma, Y. Wang, and T. Tan, "Iris recognition using circular symmetric filters," Proceedings of the 25th International Conference on Pattern Recognition, vol. 2, pp. 414–417, (2002).
[7] Libor Masek and Peter Kovesi, "Biometric Identification System Based on Iris Patterns", The School of Computer Science and Software Engineering, The University of Western Australia, 2003.
[8] Iris Recognition Technology for Improved Authentication, By Penny Khaw, SANS Security Essentials (GSEC) Practical Assignment, Version 1.3, SANS Institute 2002.
[9] J.G. Rodrguez, S. Cruz and J. Ortega, "Biometric Identification through Speaker Verification over Telephone Lines", Proceedings of IEEE Carnahan Conference on Security Technology, pp. 238-242, ISBN:0-7803-5247-5, Madrid, 1999.
[10] J.R. Bellegarda, D. Naik, M. Neeracher, K.E.A. Silverman, " Language-independent, Short-enrollment Voice Verification over a Far-field Microphone", IEEE International Conference on Acoustics, Speech and Signal Processing, 1:445-448, 2001.
[11] Q. Li, B.H. Juang, C.H. Lee, Q. Zhou, and F.K. Soong, "On Speaker Authentication", IEEE workshop on Automatic Identification Advanced Technologies, Stony Brook, NY, pp.3-6, Nov. 1997.
[12] J. P. Campbell, "Speaker recognition: A tutorial," Proc. IEEE, vol. 85, pp. 1437–1462, 1997.
[13] A. K. Jain, K. Nandakumar and A. Nagar, "Biometric Template Security", EURASIP Journal on Advances in Signal Processing, January 2008.
[14] N. Ratha, J. Connell, and R. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," IBM Syst. J., vol. 40, no. 3, pp. 614–634, 2001.
[15] A. Juels, M. Sudan, "A Fuzzy Vault Scheme", in Proceedings of the 2002 IEEE Int. Symp. On Inf. Theory, Lausanne, Switzerland 408, 2002.
[16] B. Yanikoglu, A. Kholmatov, "Combining Multiple Biometrics to Protect Privacy", proceedings of ICPRBCTP Workshop, Cambridge, England, August 2004.
[17] Eren Camlikaya, Alisher Kholmatov, Berrin Yanikoglu, "Multi-biometric templates using fingerprint and voice" , Proc. SPIE, Vol. 6944, 2008.
[18] R. Brunelli and D. Falavigna, "Person identification using multiple cues," IEEE Trans. Pattern Anal. Machine Intell., vol. 17, pp. 955–966, Oct. 1995.
[19] J. Kittler, M. Hatef, R. P. W. Duin, and J. Matas, "On combining classifiers," IEEE Trans. Pattern Anal. Machine Intell., vol. 20, pp. 226–239, 1998.
[20] L. Hong and A. K. Jain, "Integrating faces and fingerprint for personal identification," IEEE Trans. Pattern Anal. Machine Intell., vol. 20, 1997.
[21] Colin Soutar, Danny Roberge, Alex Stoianov, Rene Gilroy, and B.V.K. Vijaya Kumar, "Biometric Encryption™", chapter 22 in ICSA Guide to Cryptography, edited by Randall K. Nichols, McGraw-Hill (1999).
[22] J. Daugman. "Statistical Richness of Visual Phase Information: Update on Recognizing Persons by Iris Patterns". International Journal of Computer Vision, 45(1): 25-38, 2001.
[23] Lisa Myers, "An Exploration of Voice Biometrics", SANS Institute Reading Room, 2004.
[24] Fabian Monrose, Michael K. Reiter, Qi Li, Susanne Wetzel, "Using Voice to Generate Cryptographic Keys", In Proc. of Odyssey 2001, The Speaker Verification Workshop, June 2001.
[25] Chinese Academy of Sciences, Center of Biometrics and Security Research, Database of Eye Images. http://www.cbsr.ia.ac.cn/IrisDatabase.htm
[26] K. Messer, J. Matas, J. Kittler, J. Luttin, and G. Maitre, "XM2VTSDB: The extended M2VTS database," in Proc. 2nd Int. Conf. Audio-Video Based Biometric Person Authentication, Washington, D.C., Mar. 22–23, 1999, pp. 72–77.
[27] J. G. Daugman, "High Confidence Visual Recognition of Persons by a Test of Statistical Independence", IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol.15, No. 11, pp. 1148–1161, 1993.