Research Journal of Applied Sciences, Engineering and Technology 8(12): 1450-1455, 2014
DOI:10.19026/rjaset.8.1120
ISSN: 2040-7459; e-ISSN: 2040-7467

Submitted: June 20, 2014 Accepted: July 19, 2014 Published: September 25, 2014

Research Article

Ear Authentication and Template Protection using Bio-key

[1]K. Annapurani, [2]M.A.K. Sadiq and [1]C. Malathy
[1]Department of Computer Science and Engineering, SRM University, Chennai-603203, India
[2]Department of Information Technology, Ministry of Higher Education, Oman

Abstract: Biometric authentication is gaining popularity in the current scenario. Biometric based authentication is the science of using physical or behavioral characteristic for ensuring that the person is the claimed identity. Biometric authentication system is also vulnerable to attacks in various phases. The biometric data stored in the template has to be protected, since variety of attacks like circumvent, covert acquisition affects the normal functioning of the system. An attacker may create new biometric data or steal the template or modify the template. Once the biometric template is compromised then the entire system is lost. So securing biometric template is an important aspect in biometric authentication system. In this study ear biometric template is secured by a new method of generating bio key from the ear fused template. Here the transformed template is stored in the database. During verification phase, for the new biometric sample a bio key is generated. Using this bio key the person is authenticated if the transformed feature generated is matched with the stored one. Hence the template is protected with the bio key. The authenticated person alone can access the system, since the key to decrypt the encrypted template is obtained from the ear trait of the authenticated person. FAR and FRR are used to evaluate the system performance.

Keywords: Authentication, biometric template, bio key, circumvent, encrypted template, transformed feature

INTRODUCTION

Traditional authentication systems based on passwords and cryptographic keys are less secure than biometrics, since the characteristics of biometrics are associated with an individual.

In the field of biometrics, a lot of research works are being carried out to generate biometric authentication systems with improved accuracy and security. Emerging trend in the field of biometric is authentication using features of ear. Ear image acquisition is perceived as less invasive**.** Ear structure does not vary with ageing and thus it is more stable. Unlike face, expressions due to emotions do not affect ear.

Researchers have developed interest in this particular biometric modality due to its significant features. Initiatives to find these evidences were taken by Mark and Wilhelm (1999). Based on the experiment conducted by Yan and Bowyer (2007) it appears that ear recognition based on 3D shape is more powerful than based on 2D appearance. Chen and Bhanu (2005) were the first to develop and experiment with a 3D ear biometric system. They used the shape model-based technique for locating human ears in side face range images and a local surface patch (LSP) representation and the Iterative Closest Point (ICP) algorithm for ear recognition. The ICP based approach to 3D ear recognition by Yan and Bowyer (2007) statistically outperforms the 2D ear recognition result obtained with a state-of-the-art PCA-based ear recognition algorithm. According to Chang *et al*. (2003) Images of ear provide better performance than face and the combination of ear and face provides better performance than individual.

A biometric system provides two functions, verification and identification. Verification ensures that the claimed identity is true that is one to one process where as identification identifies the person among all the identities that is one to many process.

Wide-spread use of biometrics implies that biometric reference information is stored in a large number of locations. It is not secure to store the biometric information, called template. Attackers might easily get access to the biometric information. Hence the template used in the biometric systems must be protected against abuse. Biometric templates once compromised cannot be replaced and the total system is lost. It is necessary to protect the template from the attackers (Jain *et al*., 2008). The biometric template is protected by three main categories:

- Protecting biometrics and adding revocability to biometrics-e.g., cancelable biometrics, etc.

Corresponding Author: K. Annapurani, Department of Computer Science and Engineering, SRM University, Chennai-603203, India

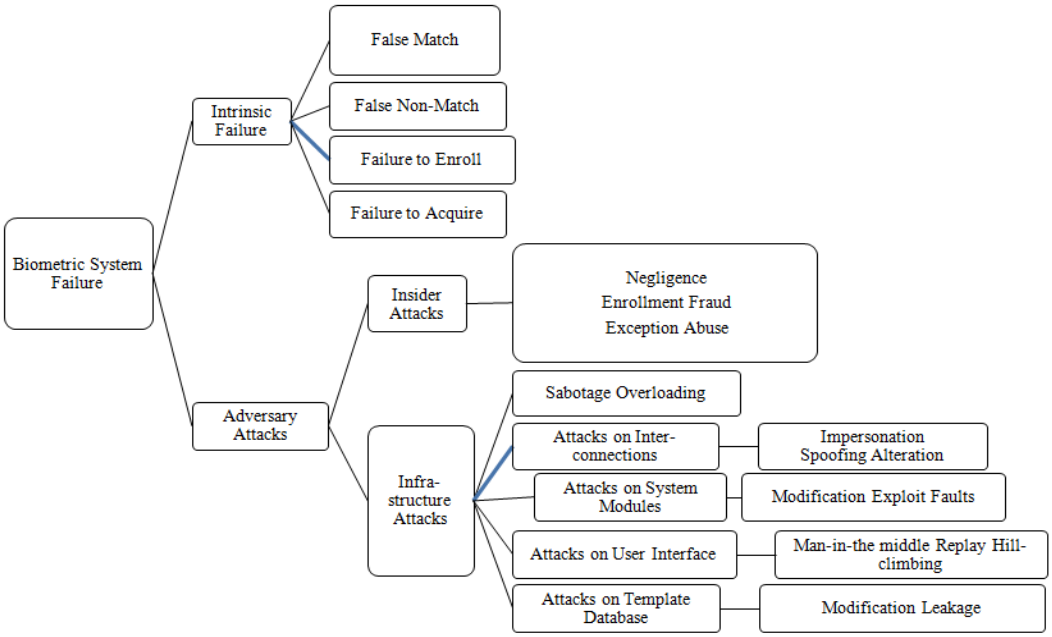

Fig. 1: Taxonomy of attacks that can be mounted against a biometric system

- Cryptographic key generation from biometrics-e.g., hardened password, Fuzzy extractors, etc.
- Cryptographic key regeneration using biometrics-e.g., fuzzy vault, fuzzy commitment, etc., Jain *et al*. (2005) discusses about the security threats in the biometric system. The taxonomy of the threats in the biometric system is shown in Fig. 1.

Even though several researches are being carried out to enhance the biometric system performance and security, it has not fulfilled the requirements needed for wide scale adaption of biometric system. Fuzzy vault, investigated by Juels and Sudan (2002) is a cryptographic construct used to bind key with biometric features. The main principle of fuzzy vault is that it can tolerate intra class variability in the biometric data. In the field of biometric, many new schemes of fuzzy vault are being researched. Juels and Wattenberg (1999) presented a fuzzy commitment scheme which could achieve three security goals:

- Static (offline) authentication
- Challenge-response authentication
- Encryption/decryption

The idea of the fuzzy commitment scheme F is to conceal the codeword c using hash function h(c) and to leave the offset in the clear. Juels and Sudan (2002) improved their own on fuzzy commitment scheme Juels and Wattenberg (1999) to generate fuzzy vault scheme that offers properties in terms of security, changeable key and flexibility.

Biometric Encryption (Cavoukian and Stoianov, 2009) is a class of emerging untraceable biometric technologies that seek to transform the biometric data provided by the user. It is the process that securely binds a PIN or a cryptographic key to a biometric, so that neither the key nor the biometric can be retrieved from the stored template. The key is re-created only if the correct live biometric sample is presented on verification. This is an existing method as the biometric is not directly stored in database this mechanism provides protection against database attack. Considering the worst case, even if the template stored is captured by the hacker, the hacker cannot retrieve users original biometric from it. Thus, the information stored in the database gives no information to the attacker.

Boult (2006) has discussed about the face recognition supporting revocable biometric tokens and Boult *et al*. (2007) also has done on fingerprint biotokens. Cancellable biometrics for iris recognition using Bioencoding is proposed by Ouda *et al*. (2010) and Pillai *et al*. (2011) have done secure and robust iris recognition. Li and Zhichun (2012) discuss an encryption method for ear biometric template based on fuzzy vault and Biohashing.

In our proposed work during enrollment phase the features are captured and stored in a reference database as encrypted template using bio key generated from the fused template of the ear.

The system is divided into different phases:

- Preprocessing of biometric data of ear
- Feature Extraction of the global and local features of the ear
- Fusion of the global and local features of an ear
- Generation of bio key from the fused ear template
- Encrypting the template using bio key

- Decrypting the template and Matching
- FAR and FRR are used for evaluating the system performance

Here an ear template protection system is developed to authenticate a person by generating a bio key and mapping in a secured template.

METHODOLOGY

The sample ear images undergo preprocessing steps of normalization, median filtering and adaptive histogram equalization. Then the local and global features are extracted from the preprocessed ear images and fused together to form fused ear template. Bio key is generated from the fused ear template and AES encryption algorithm uses this bio key for encrypting the fused ear template and this encrypted template is stored in the database to ensure the security of the data. The ear template protection system is shown in Fig. 2.

In this study we propose the different methods to protect the ear template and analyze the efficient method; in the first method using hash algorithm the hash code is obtained for the fused ear template. This hash code is XORed with the random generator code produced from the seed value of their id. This result is concatenated with the three random values generated with the seed values kept in the interval of 50's added with their id, that is, say for id 1the seed value obtained will be 51,and so on. This is the new bio key generated. The bio key which is generated from the fused ear feature is used as the secret key for the encryption of the template using AES algorithm. The computation time is 19.3 sec.

In the next method, code word of the each subject generated using random generator is subtracted from the fused ear feature to encode into a new feature which is stored in the database along with the codeword. On decoding it from the query fused feature if it matches with the stored codeword, then the person is authenticated. The computation time is 2.72 sec which is less compared to the first one and the accuracy is almost same.

Bio-key generation from the fused ear feature: The shape of the ear represented as S and the tragus represented as T extracted are combined together to form a fused template FT. Here the two local and global features of tragus and shape of the ear are added together since they are homo traits instead of concatenation:

$$FT = \sum_{i=1}^{N} Si + Ti$$

where, N is the features $1 \le i \le N$.

Hash algorithm SHA is applied to the fused features. This is then XORed with the randomly generated value s taking their id as the seed. This resultant is concatenated with keys s1, s2 and s3 obtained randomly from the pseudorandom generator taking at the interval of 50's added with their id as seeds to produce a bio-key BK:

$$BK = \text{horcat}((H(FT) \oplus s), s1, s2, s3)$$

Encrypted template of the fused ear feature: The Bio- Key (BK) obtained in the section above is used as the secret key for the conventional encryption of the AES algorithm. The Fused Template (FT) is encrypted with the BK to produce an Encrypted Template (ET). This ET is stored as template for further reference instead of the original template:

$$ET = E(BK, FT)$$

During verification the template is decrypted only if the same bio-key is produced, otherwise not. That is only if the same person claims only can access the system:

$$FT = D(BK, ET)$$

Encoded template of the fused ear feature: In this the codeword of each subject w is generated from the pseudo random generator taking their id as seed, it

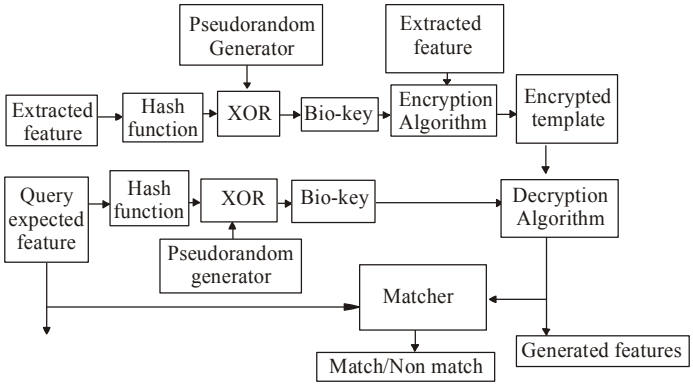

Fig. 2: Generation of bio-key to protect the template of ear authentication system

is subtracted from the Fused Template (FT).This results in the production of the Encoded Template (ECT):

$$ECT = FT-w$$
$$h = H(w)$$

In the database now the encoded template is stored along with the hash value of the codeword h instead of the original template. The template is decoded if the same fused trait is given and compared with the hash value of the generated codeword and the stored codeword. If both are same then the person is authenticated:

$$w = FT-ECT$$

EXPERIMENTS AND RESULTS

The ear image is preprocessed and the extracted tragus and helix is shown in Fig. 3 and 4.

The extracted tragus and helix are fused together to form the fused template. It is shown in Fig. 5.

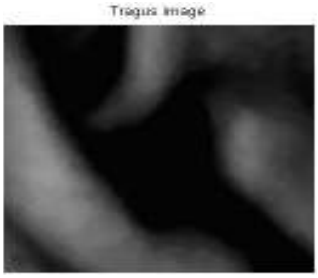

Fig. 3: Extracted tragus image

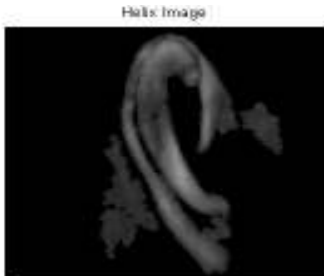

Fig. 4: Extracted helix image

Fig. 5: Fused ear image

The bio key is generated from the fused image as discussed in the previous section and that key is used as the secret key in the AES -128 algorithm to encrypt the fused template. Figure 6 shows the encrypted template which is stored in the database instead of the original fused template.

During verification phase the person has to give is id and ear image, then the ear image is pre-processed, features are extracted, fused and the bio key is generated as done in the enrolment process. The AES-128 algorithm uses this key and decrypts the encrypted template, the same image is obtained if the genuine user logs in otherwise the person is not authenticated. The decrypted template for the same subject is shown in Fig. 7.

The False Acceptance Rate (FAR) and the False Rejection Rate (FRR) are calculated. From IIT Delhi database three images are taken for each subject. Totally 125 subjects are considered. So the total number of images is 375. The Euclidean method calculates the distance between the objects. Here the training and testing images distance are calculated. The pair which has the smallest distance is said to be the same i.e., the correct image.

In each subject one image is taken for training, so 125 images are trained. All 375 images are tested against the 125 trained images to generate the genuine scores. Each subject is tested against the remaining subjects for imposter scores. It results in (3*124)*124

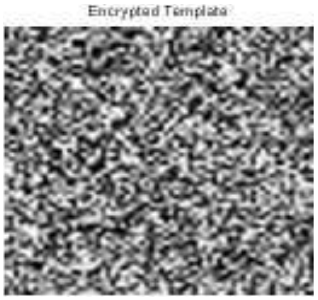

Fig. 6: Encrypted template of fused ear image

Fig. 7: Decrypted template

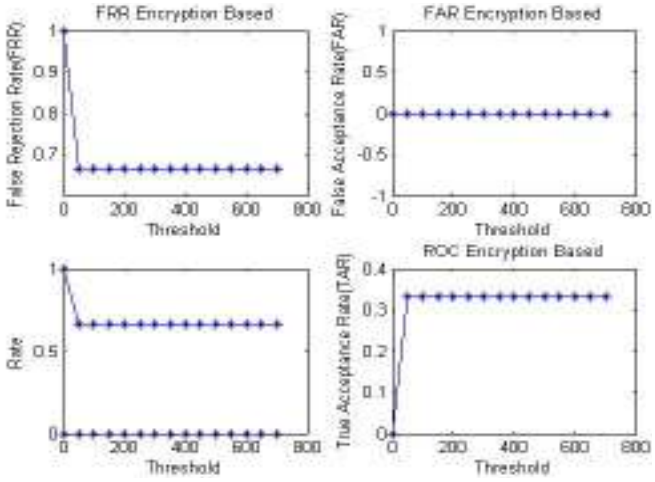

Fig. 8: Performance characteristics of encrypted template

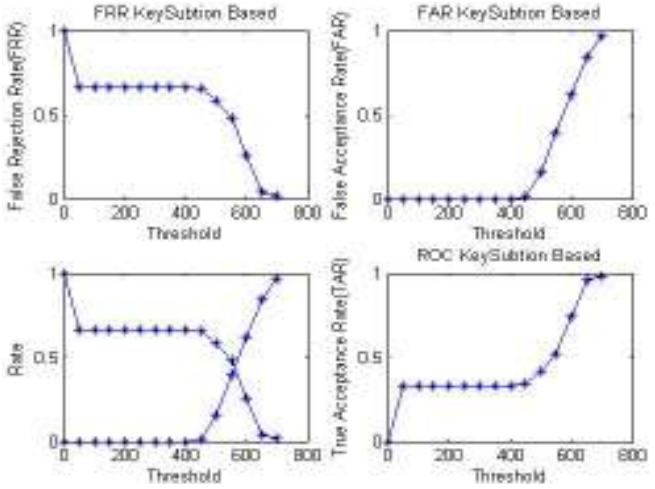

Fig. 9: Performance characteristics of encoded template

impostor scores. The authentication process is carried against each subject, first by identifying the subjects' identity and then the images are authenticated based on the Euclidean distance. Figure 8 shows the FAR, FRR and the true acceptance rate of the system.

In the second method the code word is generated and subtracted from the fused template, this subtracted value and the hash function of the code word are stored in the database instead of the fused template. During verification process if the same fused template is obtained only the transformed template can be decoded. This leads to the protection of the template. The FAR and FRR of the system is shown in the Fig. 9.

DISCUSSION

In the first method of encrypted template the accuracy of the system is 99.77 % and the FAR is 0. This means that the unauthenticated persons are not allowed to access. But the FRR of the system is 0.6667 which means that the genuine person might be rejected. Since here the concentration is on authentication the system is perfect with 0 FAR. Due to encryption process the time taken is average of 19 sec. In order to reduce the processing time the transformed template is generated as discussed in the previous section.

In the next method of encoded template the FAR is 0 for the lower thresholds then increases for the threshold of 500 and above. Beyond the threshold of 600 the FRR is good, since we are interested in authentication the lower threshold is taken and the accuracy of the system is 99.5%. But the processing time is on an average of 2.7 sec. If the computation time is considered this method can be adopted, if perfect authentication is required then the encrypted process might be adopted.

CONCLUSION

Security of the template is considered and the template is here protected in the first method by the process of encryption where the FAR is 0, hence the

system is good for authentication since it doesn't allow any non-genuine users into the system. But the processing time is longer, hence in the encoded method the processing time is reduced, but the system well behaves only for the lower threshold, here there is a possibility that the non-genuine users might be allowed to access the system. But that the rate of rejection of genuine users is less compared to the encryption process.

The other methods of bio tokens, homomorphic encryption, bio mapping and the hybrid of fuzzy vault with other technique in multi biometric can be considered for the future work.

REFERENCES

Boult, T., 2006. Robust distance measures for face-recognition supporting revocable biometric tokens. Proceeding of 7th International Conference on Automatic Face and Gesture Recognition, pp: 560-566.

Boult, T., W. Scheirer and R. Woodworth, 2007. Revocable fingerprint biotokens: Accuracy and security analysis. Proceeding of IEEE Conference on Computer Vision and Pattern Recognition, pp: 1-8.

Cavoukian, A. and A. Stoianov, 2009. Biometric encryption. In: Encyclopedia of Biometrics. Springer, US, pp: 260-269.

Chang, K., K. Bowyer and V. Barnabas, 2003. Comparison and combination of ear and face images in appearance-based biometrics. IEEE T. Pattern Anal., 25: 1160-1165.

Chen, H. and B. Bhanu, 2005. Shape model-based 3D ear detection from side face range images. Proceeding of the IEEE Conference on Computer Vision and Pattern Recognition-Workshop (CVPR, 2005). San Diego, CA, USA, pp: 122.

Jain, A.K., A. Ross and U. Uludag, 2005. Biometric template security: Challenges and responses. Proceedings of European Signal Processing Conference (EUSIPCO), pp: 1934-1937.

Jain, A.K., K. Nandakumar and A. Nagar, 2008. Biometric template security. EURASIP J. Adv. Sig. Pr., 2008(113): 1-17.

Juels, A. and M. Wattenberg, 1999. A fuzzy commitment scheme. Proceeding of 6th ACM Conferences on Computer and Comm. Security, pp: 28-36.

Juels, A. and M. Sudan, 2002. A fuzzy vault scheme. Proceeding of IEEE International Symposium on Information Theory, pp: 408-412.

Li, Y. and M. Zhichun, 2012. An ear template protection method. Proceeding of 31st Chinese Control Conference (CCC, 2012), pp: 3858-3862.

Mark, B. and B. Wilhelm, 1999. Ear biometrics. BIOMETRICS: Personal Identification in a Networked Society, pp: 273-286.

Ouda, O., N. Tsumura and T. Nakaguchi, 2010. BioEncoding: A reliable tokenless cancelable biometrics scheme for protecting IrisCodes. IEICE T. Inf. Syst., E93-D (7): 1878-1888.

Pillai, J., V. Patel, R. Chellappa and N. Ratha, 2011. Secure and robust iris recognition using random projections and sparse representations. IEEE T. Pattern Anal., 33(9): 1877-1893.

Yan, P. and K.W. Bowyer, 2007. Ear biometrics using 2D and 3D images. IEEE T. Pattern Anal., 29(8): 1297-1308.