Security Analysis on Gait-Based Biometric Fuzzy Commitment Scheme Using Smartphone

Zhang Min(✉)

JiMei University, Xiamen 361021, Fujian, China
flyinskyzhang@126.com

Abstract. Gait-based biometric systems using smart phones have been developed to replace traditional authentication. It is significantly important to improve the security of the gait-based biometric systems. Systems include both fields of cryptography which provides high security levels of data and gait- based biometrics without need to remember passwords. Fuzzy Commitment Scheme (FCS) is considered as a famous approach to protect the user's data. However, these gait-based biometric systems are hampered by the lack of formal security analysis to prove the security strength and effectiveness. Therefore, this paper gives a comprehensive analysis evaluation on security of fuzzy commitment and proposes a framework of gait-based biometric fuzzy commitment scheme using smart phones. The evaluation results show that a significant security strength resistant to different attacks.

Keywords: Gait-based biometric cryptosystem · Fuzzy commit scheme · Security analysis

1 Introduction

Traditional security techniques for identification and authentication generally require passwords, PIN, or tokens which are easily attacked. In recent years, biometric has been widely studied in order to address the weakness of traditional authentic mechanisms. These biometric systems refer to behavioral or physical characteristics [1]. With increasingly application of mobile Internet, smart phones have become the media of human and machine interaction. Therefore, the identity authentication of smart phones and various mobile terminals has played an important role in guaranteeing for the security and reliability.

The user identity authentication method based on an inertial mobile sensor named accelerometer has become a hot topic in the research, and the sensor has been widely used in the smart phones for its high cost performance. Therefore, the comprehensive utilization of the information collected by these sensors for identity authentication will become important in the field of identity authentication in the future.

From 2010, the sensor-based gait recognition technology is applied to support existing authentication mechanisms, which are not very convenient in mobile phones [2], and have achieved significant results [3–6]. A first approach of inertial sensor-based gait authentication on mobile phones is proposed by Thang Hoang [7]. Instead of

H. Song et al. (Eds.): SIMUtools 2019, LNICST 295, pp. 353–362, 2019.
https://doi.org/10.1007/978-3-030-32216-8_34

storing original gait templates for user identification, the user was verified via a stored key which was encrypted by gait templates collected from a mobile accelerometer.

The Fuzzy Commitment Scheme (FCS) is developed by Ari and Wattenberg [8] and is considered as one of the template protection which method is based on Error Correcting Code (ECC). A major challenge of biometric cryptosystem is the security analysis that allows comparing different systems. Adamovic [9] presents a method based on information-theoretic analysis of iris biometric that aims to extract homogeneous regions of high entropy and uses FCS to reduce the overall complexity of this kind of systems. Chauhan [10] explores the efficiency of executing fuzzy commitment scheme in conjunction with Reed Solomon code as a novel better alternative to the conventional commitment scheme. Lafkih [11] have discussed the critical elements of the security in the key binding biometric cryptosystems and he [12] proposed a security analysis framework for biometric cryptosystems based on the fuzzy vault system and in paper [13] proposed a framework to evaluate the security of biometric cryptosystems based on the FCS. In paper [14] presented an approach to secure fuzzy commitment scheme against cross-matching-based decodability attack. However, behavioral traits such as gait are rarely studied. A novel lightweight symmetric key generation scheme based on the timing information of gait is proposed in paper [15].

Gait-based biometric authentication system offers more benefits to users than traditional authentication system. However, gait-based biometric features seem to be very vulnerable which are easily affected by different attacks. A rigorous security and privacy evaluation is still missing, especially for the evaluation of real systems using smart phones. In this paper, we propose a security analysis framework of gait-based biometric cryptosystems using smart phones based on the FCS. Firstly, we comprehensively summarize the security evaluation criteria and different metrics. Secondly, we introduce the security analysis framework of gait-based biometric cryptosystems based on the FCS. Thirdly, we evaluate the proposed criteria in the fuzzy commitment scheme for gait authentication.

The rest of the paper is organized as follows: In Sect. 2, an overview of security analysis of FCS is briefly presented. Section 3 will propose scenarios of attacks and different metrics to evaluate the performance and security of gait authentication on smart phones based on the FCS. Section 4 shows the results of the proposed framework. Conclusion and future work are mentioned in Sect. 5.

2 An Overview of Security Analysis of the FCS

The main idea of the FCS is to assign a random key to a subject to replace the biometric data itself. In the enrollment phase, we generate the key with gait-based biometric data by using an XOR-ed function which results in a new data called helper data. In the authentication stage, if the query features are close enough to enrolled features which is generated by key and helper data. The gait-biometric cryptosystem based FCS is shown in Fig. 1 as follows.

The enrollment and authentication phases of fuzzy commitment share the helper data (*HD* for short) and two correlated gait signal feature templates w and w'. They try to extract exactly the same hash code of the key m.

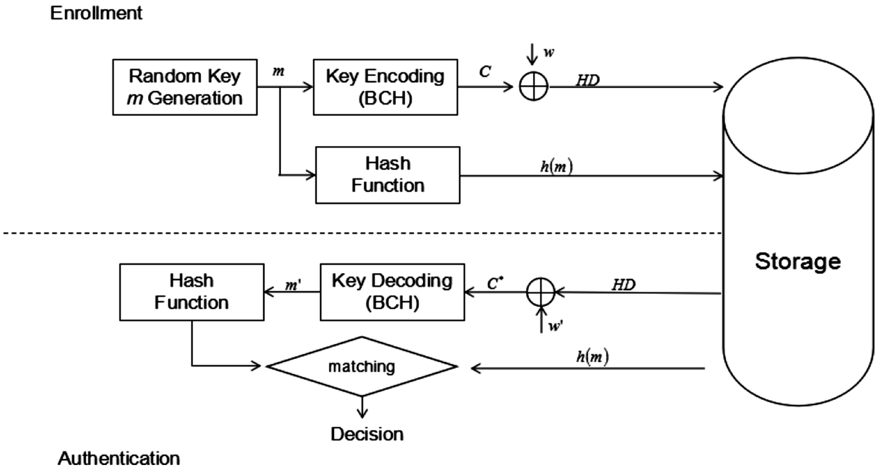

Fig. 1. Gait-based biometric cryptosystem based FCS.

The binary BCH code C as the error correcting code corresponds to the key m. The stored secure template consists of the hash of the key $h(m)$ and HD. The helper data HD is obtained by codeword C XOR with gait signal template w.

$$HD = C \oplus w \tag{1}$$

In the authentication phase, the gait signal template binarized and extracted from the queried biometric sample is XOR-ed with the stored helper data HD to obtain codeword C^*:

$$C^* = HD \oplus w' = (C \oplus w) \oplus w' = C \oplus (w \oplus w') \tag{2}$$

Then the codeword C^* can be rewritten as

$$C^* = C \oplus er \tag{3}$$

The matching module compares the hash value of m' which is decoded by BCH with stored hash value $h(m)$. The same hash values of m and m' results into a match. If the hamming distance $D(w, w') = \|w \oplus w'\| = \|er\| \leq \varepsilon$, then there is a match where ε is the error correction capability of the code.

The security and privacy performance of fuzzy commitment is well analyzed theoretically. In literature, many papers discussed the security analysis of the FCS [9, 12–16]. Rathgeb and Uhl [16] discussed the key elements of the security in biometric cryptosystems. Zhou *et al.* [17] studied the security in biometric security of the FCS. Their work focused on measuring the security and the privacy using the entropy to evaluate the independence and distribution of biometric features.

Lafkih [9, 12, 13] studied the security of key binding biometric cryptosystems based on fuzzy vault and fuzzy commitment respectively. Lafkih [13] proposed a security analysis framework based on several kinds of attacks that could affect biometric cryptosystems and applied on FCS. Different settings would be studied and other metrics would be proposed to analyze the security level of different biometric cryptosystems.

Hong [7] investigated the security of the gait authentication on mobile phones using biometric cryptosystems and fuzzy commitment scheme. But the paper didn’t give a detailed framework for security analysis. Sapkal [18] presented a biometric cryptosystem with both fuzzy vault and fuzzy commitment techniques for fingerprint system. In [19], a novel template protection scheme based on fuzzy commitment and chaotic system, and the security analysis approach for unimodal biometric leakage were proposed.

3 Proposed Security Analysis Framework of Gait-Based Biometric Cryptosystems Using Fuzzy Commitment

Previous studies on security analysis are mostly based on information-theoretical measurements (such as entropy and leakage rate) which are difficult to estimate in the case of unknown biometric features distribution. There are few security analysis on gait-based biometric cryptosystems using smart phones. Therefore, our contribution is to offer simple, yet theoretically and practically detailed security analysis framework on gait-based biometric cryptosystem using smart phones.

In this paper we propose a security analysis framework for gait-based biometric cryptosystems using fuzzy commitment scheme against different attacks.

3.1 Evaluation Criteria and Metrics

For a fuzzy commitment scheme, we take consideration on security, privacy protection ability and unlinkability as security measures referred to [17]. In order to evaluate the performance of gait-based biometric cryptosystems, we use the False Acceptance Rate (FAR) and False Rejection Rate (FRR) which reflect the security and friendless of the system. The security is so important that we would like to achieve the FAR of 0% and the FRR as low as possible.

In order to measure the evaluation criteria, we need to define evaluation metrics against several threats including intrusion, correlation, combination and injection as referred to [13]. The evaluation metrics are used to quantify the different criteria.

3.2 Intrusion Threat

The adversary tries to access a system S_2 based on the information of another system S_1 (helper data HD_1 and the key m_1), on the assumption that both systems use the same gait-based biometric feature templates (w and w'). The adversary can generate gait-based biometric feature template of S_1 and use them to access to the second system S_2. We calculate the probability using the distance between the helper data HD_2 of the system S_2 XOR-ed with the gait-based biometric feature template w and the enrolled

BCH codeword C_2 is inferior to a threshold ε as the Intrusion Rate in Different System (IRDS).

$$IRDS(\varepsilon) = P(D(HD_2 \oplus w, C_2) < \varepsilon) \tag{4}$$

In order to measure the evaluation criteria, we need to define evaluation metrics against several threats including intrusion, correlation, combination and injection.

3.3 Correlation Threat

Nagar *et al.* [20] proposed cross matching attack in order to determine whether two 'helper data' are generated from the same user. The error pattern with the smallest hamming distance is considered as the cross-matching distance score.

$$\begin{aligned} HD_{XOR} &= HD_1 \oplus HD_2 = (w_1 \oplus C_1) \oplus (w_2 \oplus C_2) = (w_1 \oplus w_2) \oplus (C_1 \oplus C_2) \\ &= er \oplus C_3 \end{aligned} \tag{5}$$

If the adversary knows both 'helper data' of both systems S1 and S2, the adversary can estimate the distance between both gait features of the user in both systems.

$$CM_s = min_{C \in X} ||HD_{XOR} \oplus C|| \tag{6}$$

The cross-matching distance score $CM_s = \|er^*\| \leq \varepsilon$ only if the error pattern can be written as $er = er^* \oplus C_i$.

We can evaluate the vulnerability of the system to this attack by the probability that the distance between different helper data (HD_{XOR}) and codeword C_i is lower than a threshold ε:

$$CR_{FC}(\varepsilon) = P(D(HD_1 \oplus HD_2, C_i) < \varepsilon) \tag{7}$$

3.4 Combination Threat

The adversary knows part of the user gait-based biometric features in this attack, and extracts part of his/her own features to complete the biometric template ($w_A = w + w_F$) in which w_F is part of his/her own features) used in the authentication system. We define the probability that the distance between the helper data XOR-ed with the combined template and the enrolled codeword is lower than a threshold ε as follows:

$$CA_{FC}(\varepsilon) = P(D(HD \oplus w_A, C) < \varepsilon) \tag{8}$$

3.5 Injection Threat

The adversary can also inject his/her own gait-based biometric features in the database in order to be accepted by the system. For example, the adversary replaces the stored 'helper data' by a false 'helper data' ($HD_f = replace(HD)$). We measure this criterion via the probability that the distance between the ‘helper data’ which is forfeited by the adversary and the enrolled codeword C is lower to a threshold ε.

$$IA_{FC}(\varepsilon) = P(D(HD_f \oplus w, C) < \varepsilon) \tag{9}$$

4 Simulation and Experimental Results

We used the system on the dataset [4] collected from a built in accelerometer in smart phone for evaluating the security analysis framework. The original dataset consists of gait signals of 30 users carrying a waist-mounted smart phone with embedded inertial sensors. At first, we classify the dataset referred to [4] and extract the walking data as the original dataset. In this study, we consider the gait-based biometric authentication system based on different features extraction approaches. The SFS and SFFS algorithm are used in the first system [21] and BCS system is used in the second system [7]. The performance measurement and security analysis are based on the results achieved from the following part.

4.1 Performance Measurement

Receiver Operating Characteristic (ROC) [17] curves are obtained by computing the performance of systems in multiple operating points based on variation of FAR and FRR with tolerance. The overall error rates of our system is also represented by a receiver operating characteristic (ROC) curve which illustrates the relationship between the FAR and the FRR as shown in Fig. 2.

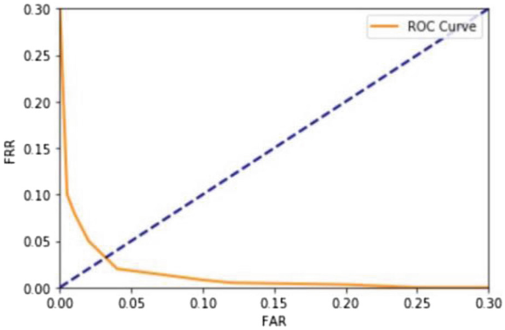

Fig. 2. ROC curves of gait authentication system

The Equal Error Rate (EER) is 3.48%, corresponding to an acceptable threshold of ε = 15.289. The ERR indicates the rate at which both FAR and FRR are equal.

4.2 Security Analysis Framework of the FCS

Figure 3 shows the IRDS curve. The adversary uses the first system's data and tries to access to the second system. The IRDS rate is increased in accordance with the value of threshold. If the error correction capability is minimal then the adversary is rejected by the system. As shown in Fig. 3, the ability to prevent this attack from being successful is affected by the intra-class variability.

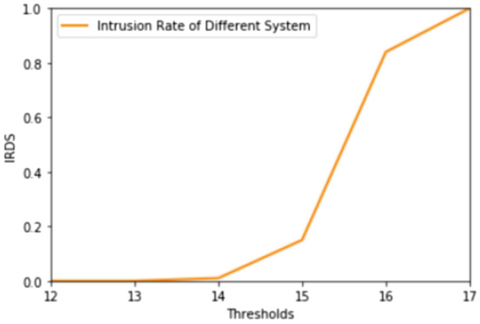

Fig. 3. IRDS curve

In cross-matching attack, the adversary links two different systems' helper data using the same gait-based biometrics of the same user. The adversary can easily access to both systems as the system can correct the distance between both helper data (Fig. 4).

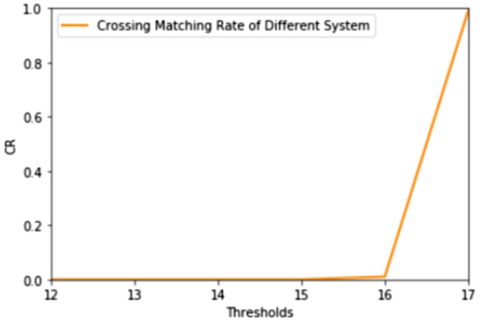

Fig. 4. CR curve

In combination threat, the adversary can randomly combine both gait-biometric features. The adversary tried to use part of the forfeit of the user data instead of the real user data. Figure 5 shows that even if the threshold is minimal, the adversary can have access to the system using combined features with a high probability.

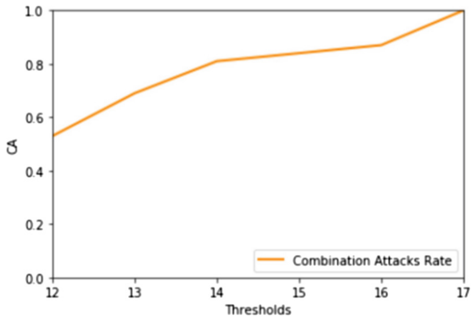

Fig. 5. CA curve

In injection attack, the adversary submits fake gait-based biometric features in order to be accepted by the system. As described in Fig. 6, the adversary can have access to the system with a high probability despite of the minimal threshold and random injection.

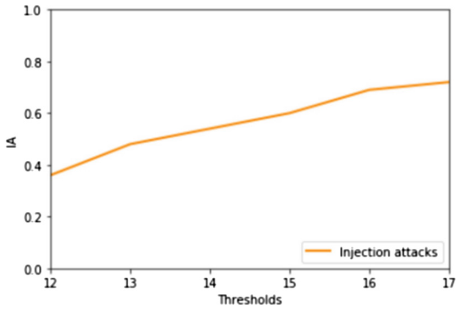

Fig. 6. IA curve

If the adversary knows both ‘helper data’ of both systems S1 and S2, the adversary can estimate the distance between both gait-based biometric features of the user in both systems. As a result, the system can easily refuse the trusted user with the thought of that the stored *HD* is modified in comparison to the enrollment process and contained the fake gait-based biometric templates injected by the adversary.

5 Conclusions and Future Work

In this paper, we proposed a security evaluation framework of gait-based biometrics against several attacks that could affect biometric cryptosystems and applied this analysis on gait authentication system on mobile phone by employing fuzzy commitment scheme. The investigation confirms theoretically and practically that cryptosystems based on FCS using smart phones can achieve promising performance in terms of FAR and FRR, and ensure the security level and protection of privacy.

On the field of gait biometric in general there is still a lot of work to do. The performance of gait authentication systems is not competitive to other biometrics. So the future work will focus on the studies of different settings and other metrics proposed to analyze the security level of different biometric cryptosystems.

Acknowledgment. This research project was supported by grant no. JAT170325 from Fujian Provincial Education Department Project of China and grant no. 2018J01537 from Fujian natural foundation project.

The author wants to thank the UCI Machine Language Repository and especially the researchers who kept the records and developed the Human Activity Recognition Using Smart Phones Data Set.

References

1. Jain, A.K., Flynn, P.J., Ross, A.A. (eds.): Handbook of Biometrics. Springer, Berlin (2008). https://doi.org/10.1007/978-0-387-71041-9
2. Tam, L., Glassman, M., Vandenwauver, M.: The psychology of password management: a tradeoff between security and convenience. Behav. Inf. Technol. **29**(3)
3. Frank, J., Mannor, S., Precup, D.: Activity and gait recognition with time-delay embeddings. In: AAAI, pp. 1581–1586 (2010)
4. Hoang, T., Choi, D., Vo, V., Nguyen, A., Nguyen, T.: A lightweight gait authentication on mobile phone regardless of installation error. In: Janczewski, L.J., Wolfe, H.B., Shenoi, S. (eds.) SEC 2013. IAICT, vol. 405, pp. 83–101. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-39218-4_7
5. Derawi, M., Bours, P.: Gait and activity recognition using commercial phones. Comput. Secur. **39**, 137–144 (2013)
6. Lu, H., Huang, J., Saha, T., Nachman, L.: Unobtrusive gait verification for mobile phones. In: Proceedings of the 2014 ACM International Symposium on Wearable Computers, pp. 91–98. ACM (2014)
7. Hoang, T., Nguyen, T., Nguyen, T.: Gait authentication on mobile phone using biometric cryptosystem and fuzzy commitment scheme. Int. J. Inf. Secur. **14**(6), 549–560 (2015)
8. Ari, J., Wattenberg, M.: A fuzzy commitment scheme (1999). http://www.arijuels.com/wp-content/uploads/2013/09/JW99.pdf
9. Adamovic, S., Milosavljevic, M., Veinovic, M., et al.: Fuzzy commitment scheme for generation of cryptographic keys based on iris biometrics. IET Biometrics **6**(2), 89–96 (2017)
10. Chauhan, S., Sharma, A.: Fuzzy commitment scheme based on reed solomon codes. In: International Conference on Security of Information & Networks, pp. 96–99. ACM (2016)
11. Lafkih, M., Mikram, M., Ghouzali, S., and El Haziti, M.: Security analysis of key binding biometric cryptosystems. In: Proceedings of the 5th International Conference on Image and Signal Processing, pp. 269–281 (2012)
12. Lafkih, M., Mikram, M., Ghouzali, S., El Haziti, M., Aboutajdine, D.: Biometric cryptosystems based fuzzy vault approach: security analysis. In: Proceedings of the 2nd International Conference on Innovative Computing Technology, pp. 27–32, Casabkabca (2012)

13. Lafkih, M., Mikram, M., Ghouzali, S., EI Haziti, M., Aboutajdine, D.: Biometric cryptosystems based fuzzy commitment scheme: a security evaluation. Int. Arab J. Inf. Technol. **13**(4), 443–449 (2016)
14. Chauhan, S., Sharma, A.: Securing fuzzy commitment scheme against decodability attack-based cross-matching. In: Woungang, I., Dhurandher, S.K. (eds.) WIDECOM 2018. LNDECT, vol. 18, pp. 39–50. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-75626-4_4
15. Sun, Y., Wong, C., Yang, G. Z., et al.: Secure key generation using gait features for Body Sensor Networks. In: IEEE, International Conference on Wearable and Implantable Body Sensor Networks, pp. 206–210. IEEE (2017)
16. Rathgeb, C., Uhl, A.: A survey on biometric cryptosystems and cancelable biometrics. EURASIA J. Inf. Secur. **2**, 1–25 (2011)
17. Zhou, X., Kuijper, A., Veldhuis, R., et al.: Quantifying privacy and security of biometric fuzzy commitment. In: International Joint Conference on Biometrics, vol. 207, pp. 1–8. IEEE Computer Society (2011)
18. Sapkal, S., Deshmukh, RR.: Biometric template protection with fuzzy vault and fuzzy commitment. In: International Conference on Information and Communication Technology for Competitive Strategies, pp. 1–6. ACM (2016)
19. Wang, N., Li, Q., et al.: A novel template protection scheme for multi biometrics based on fuzzy commitment and chaotic system. Signal Image Video Process. **9**(1), 99–109 (2015)
20. Nagar, A., Nandakumar, K., Jain, A.: Biometric template transformation: a security analysis. In: Proceedings of SPIE Workshop on Electronic Imaging, Media Forensics and Security, San Jose (2010)
21. Anguita, D., Ghio, A., Oneto, L., Parra, X., Reyes-Ortiz, J.L.: A public domain dataset for human activity recognition using smartphones. In: 21th European Symposium on Artificial Neural Networks, Computational Intelligence and Machine Learning, ESANN 2013. Bruges, Belgium, pp. 24–26 (2013)