BIOMETRIC TEMPLATE PROTECTION: A KEY-MIXED TEMPLATE APPROACH

Shih-Wei Sun*†, Chun-Shien Lu*, and Pao-Chi Chang†
*Institute of Information Science, Academia Sinica, Taipei, Taiwan, ROC
†Dept. Electrical Engineering, National Central Univ., Chung-Li, Taiwan, ROC
E-mail: swsun@iis.sinica.edu.tw, lcs@iis.sinica.edu.tw, pcchang@ce.ncu.edu.tw

***Abstract*— This paper presents key-mixed template (KMT), which mixes a user's template with a secret key to generate another form of template, to prevent the biometric template stored in the database from back end attack, snooping, and tampering attack.**

I. INTRODUCTION

The biometric recognition techniques have been developed for several years. Most of the biometric systems store the extracted biometric template in a centralized database for authentication applications. Although the convenience of a biometric system is increasing, the biometric template protection becomes more and more important.

In [7], the author noticed and discussed the possible ways of solving the two challenging problems in the existing biometric systems.

1) Is it possible to design biometric systems such that if the biometric template in an application is compromised, the biometric signal itself is not lost forever and a new biometric template can be issued? 2) Is it possible to design biometric templates such that different applications are not able to use the same biometric template, thus securing the biometric signal as well as preserving privacy?

In this paper, the above two challenging problems will be addressed.

II. RELATED WORKS

In the literature, the template protection can be roughly divided into five categories.

The most straightforward way to protect the template data is to encrypt template in a ciphertext form. In the enrollment phase, the template is encrypted by the system server. Although the ciphertext form of a template is secure, the distinguishing of the extracted bitstream is still a challenging problem. In addition, a one-way function encryption cannot prevent the back end attacker after a template is decrypted.

In [4], the image grid morphing and block scrambling is proposed for cancelable biometrics. The concept of noninvertible transform is also proposed to deal with the cross match problem. However, from their examples of distortion transform, the morphing effect on the image is limited. Furthermore, a practical system design and the performance degrading are not discussed in their paper.

The original concept of a biometric system contains a centralized database. A smart card system, such as [3], stores the biometric template distributed. Once the smart card is lost or stolen, the attacker has the possibility to crack the smart card, obtaining the template stored in the card. Hence, the snooping and tampering attacks can still successfully crack the system.

A fuzzy vault scheme [8] stores the genuine template and some imposter templates together in the enrollment phase. But the genuine template and the imposter template can be separated efficiently by a back end attacker for cross match attack.

In [2], [6], a Helper Data Scheme (HDS)[6] is adopted for improving the biometric template security. Once a back end attacker replace the helper data as a counterfeit one without modifying the statistics and the reliable bits, the DoS attack and cross match attack can be successful. Besides, the reliable bit extraction degrades the classification performance in this work.

III. PROPOSED KEY-MIXED-TEMPLATE SCHEME

A. Problem Statement: The template security should be guaranteed by mixing the biometric template and a secret key

A biometric template should be mixed with a secret key to prevent the back end attack, snooping, and tampering attack for a cross match attack. With the increasing maturity of biometric recognition techniques, the standardization of a biometric system becomes possible. Therefore, a cross match attack from different applications make a biometric system insecure. To keep the security of a biometric system, a template should be mixed with a secret key. In the feature extraction process, the user given secret key should be mixed with the permanently biometric template to form a *key-mixed-template(KMT)*. A mixing function $M(\cdot)$ can mix the key-determined random vector V_i and the template T_i as: $KMT_i = M(T_i, V_i)$, e.g. $M(T_i, V_i) = T_i + V_i$. The KMT is useful when a user authorized the template is legal. The key for different databases should be set to be different by the same user. Assume that there are two different vendors contain two different databases DB_1 and DB_2. In the enrollment phase, the different key-mixed-template KMT_1 and KMT_2 are correspondingly stored in DB_1 and DB_2. Suppose that an attacker successfully implemented a back end attack, snooping, or tampering attack from DB_1 and going to DB_2 for authentication, the proposed KMT_1 would not match for the KMT_2 in DB_2. Therefore, the cross match attack cannot be successful.

1-4244-0763-X/07/$20.00 ©2007 IEEE

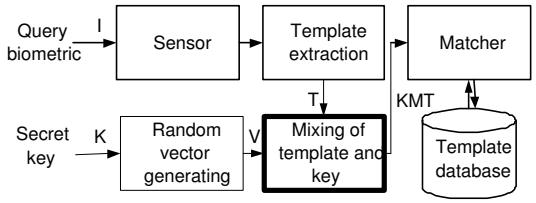

Fig. 1. Proposed biometric system.

A genuine user who owns the permanently biometric and a secret key can achieve the robustness against the back end attack, snooping, and tampering attack. Once the KMT_1 is disclosed from DB_1, a $KMT_1{}'$ can be updated in DB_1 instead of KMT_1, revoking the KMT_1 for authentication.

In our proposed scheme, the mixture of the permanently biometric template and a user defined secret key should be finished in the user end, such as shown in Fig. 1. In the system end, the obtained KMT is well mixed, not disclosing the original permanently biometric template. The two challenging problems proposed in [7] is also solved. In addition, because the number of attackers in back end attack is limited, collusion from different attackers should not be as easy as the known pliantext attack in cryptography. Our proposed scheme is mainly designed to deal with the back end attack, snooping, and tampering attacks in a certain level.

From the implementation point of view, if the existing biometric system would like to enhance the template security, only a mixing function and a secret key given by the users is necessary, such as depicted in Fig. 1. The key and KMT generation are the additional necessary operations, which can be integrated to the existing biometric systems easily. The limited cost by the vendor can improve the template security from back end attack, snooping, and tampering attack.

IV. Experimental Results

In the experimental results, the system proposed in [1] was adopted as a case study. In addition, their released Matlab demo code [9] was utilized for implementing our proposed case study. The fingerprint database in set B of DB1 [10] (fingers from 101 to 110), which contains 80 images obtained from 10 different fingers with 8 impressions each, was utilized for evaluation. There were three different evaluations implemented in this paper.

Evaluation 1: false match rates. The false match rates are calculated based on the threshold setting from matching score 1 to 50. The line with original is based on the implementation in [9]. The keys k_1 and k_2 are tested in our scheme, simulating that the identical keys are presented by the genuine user. From Fig. 2, the false match rates are quite similar from the original, k_1, and k_2 schemes, which shows that our proposed scheme would not decrease the performance of the adopting biometric system.

Evaluation 2: false non-match rates. The system performance is not decreased by applying our scheme to a biometric system.

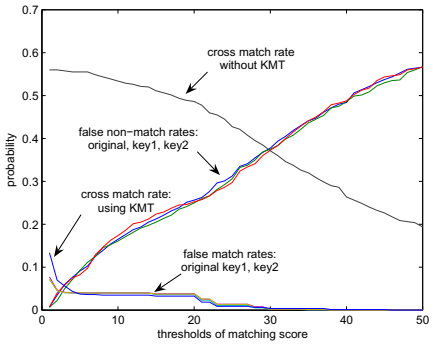

Fig. 2. False detection rates.

Evaluation 3: cross match rates. Assume that the template T_1 stored in a database DB_1 is back end attacked, snooping, or tampering attacked, the T_1 would be sent to DB_2 for verification. Without the key protection using the proposed KMT scheme, the $T_1 = T_2$ in DB_2. The cross match rate is very high under this scenario. When a template is mixed with a user given key to form KMT_1 and KMT_2 in DB_1 and DB_2, because $KMT_1 \neq KMT_2$, the cross match attack cannot be successful. As a result, the detected cross match rate is much lower than the scheme without KMT protection.

V. Conclusions

In conclusion, the proposed KMT scheme can efficiently prevent the back end attack, snooping, and tampering attack, without reducing the performance of the original biometric system. A fingerprint verification system [1] was taken as a case study for evaluating the possibility of practical use. Furthermore, the propose scheme can be adopted by the existing biometric systems to enhance the security of template protection.

References

[1] S.S. Chikkerur, "Online fingerprint verification system," *M.S. thesis, State Univ. of New York at Buffalo,* 2005.

[2] T.A.M. Kevenaar, G.J. Schrijen, M. vander Veen, A.H.M. Akkermans, and F. Zuo, "Face Recognition with Renewable and Privacy Preserving Binary Templates," *IEEE Workshop on Automatic Identification Advanced Technologies (AutoID),* pp. 21-26, 2005.

[3] M. Mimura, S. Ishida, and Y. Seto, "Fingerprint verification system on smart card," *Proc. IEEE ICCE,* pp. 182-183, 2002

[4] N.K. Ratha, J.H. Connell, and R.M. Bolle, "Enhancing Security and Privacy in Biometrics-based Authentication Systems," *IBM Systems Journal,* Vol. 40, No. 3, pp.614-634, 2001.

[5] S. Prabhakar, S. Pankanti, and A.K. Jain, "Biometric Recognition: Security and Privacy Concerns," *IEEE Security and Privacy Magazine,* pp. 33-42, March/Aprial, 2003

[6] P. Tuyls, A.H.M. Akkermans, T.A.M. Kevenaar, G.J. Schrijen, A.M. Bazen, and R. N.J. Veldhuis, "Practical Biometric Authentication with Template Protection," *AVBPA 2005, LNCS 3546,* pp. 436-446, 2005.

[7] U. Uludag, S. Pankanti, S. Prabhakar, and A.K. Jain, "Biometric Cryptosystems: Issues and Challenges," *Proceedings of the IEEE,* Vol. 92, No.6, pp. 948-960, June 2004

[8] S. Yang and I. Verbauwhede, "Automatic Secure Fingerprint Verification System Based on Fuzzy Vault Scheme," *Proc. IEEE ICASSP,* pp. 609-612, 2005

[9] *http://www.cubs.buffalo.edu*

[10] Fingerprint verification competition. *http://bias.csr.unibo.it/fvc2000/.*