The 10th International Conference on Business Information Security (BISEC-2018), 20th October 2018, Belgrade, Serbia

SECURITY EVALUATION OF CANCELABLE BIOMETRICS

NEMANJA MAČEK
School of Electrical and Computer Engineering of Applied Studies, Belgrade; Graduate School of Computer Sciences, Megatrend University, Belgrade; SECIT Security Consulting; macek.nemanja@gmail.com

IGOR FRANC
Belgrade Metropolitan University, Faculty of Information Technologies; SECIT Security Consulting; igor.franc@metropolitan.ac.rs

MILAN GNJATOVIĆ
University of Novi Sad, Faculty of Technical Sciences; milangnjatovic@uns.ac.rs

BRANIMIR TRENKIĆ
School of Electrical and Computer Engineering of Applied Studies, Belgrade; btrenkic@viser.edu.rs

ZLATOGOR MINCHEV
Institute of ICT, Joint Training Simulation & Analysis Center, Bulgarian Academy of Sciences; zlatogor@bas.bg

Abstract: *Like any personal information, biometric templates can be intercepted, stolen, replayed or altered. Due to non-revocability of biometric data aforementioned attacks and may lead to identity theft. Having that said, it becomes clear that biometric systems operate with sensitive personal information and that biometric template security and privacy are important issues one should address while designing authentication systems. One approach to biometric template security and privacy is cancelable biometrics. Two main categories of cancelable biometrics can be distinguished: intentional distortion of biometric features with non-invertible transformations and biometric salting. State of the art approaches to cancelable biometrics are presented in this paper, as well as security evaluation of cancelable biometrics.*

Keywords: *Security, Cancelable Biometrics, Non-Invertible Transformations, Biometric Salting*

1. INTRODUCTION

"Cancelable biometrics consist of intentional, repeatable distortions of biometric signals based on transformations which provide a comparison of biometric templates in the transformed domain" [1]. The inversion of such transformed biometric templates must not be feasible for potential imposters. In contrast to templates protected by standard encryption algorithms, transformed templates are never decrypted since the comparison of biometric templates is performed in transformed space which is the very essence of cancelable biometrics. The application of transformations provides irreversibility and unlinkability of biometric templates [2].

Cancelable biometric transformations are designed in a way that it should be computationally hard to recover the original biometric data. The intrinsic strength (individuality) of biometric characteristics should not be reduced applying transformations (constraint on FAR) while on the other hand transformations should be tolerant to intra-class variation (constraint on false rejection rate) [1]. In addition, correlation of several transformed templates must not reveal any information about the original biometrics (unlinkability). In case transformed biometric data are compromised, transformation parameters are changed, i.e., the biometric template is updated. To prevent impostors from tracking subjects by cross-matching databases it is suggested to apply different transformations for different applications.

Two main categories of cancelable biometrics are non-invertible transformations and biometric salting [3].

2. NON-INVERTIBLE TRANSFORMATIONS

Biometric data are transformed applying a non-invertible function. Image 1 depicts application of non-invertible transformation in face recognition process.

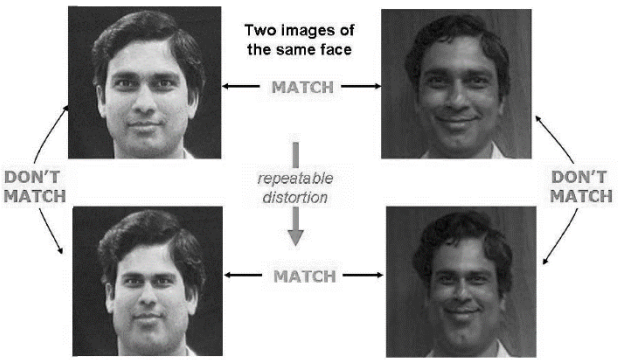

Image 1: Applying non-invertible transformation in face recognition (original image can be found in [4])

In order to provide updatable templates, parameters of the applied transformations are modified. The advantage of applying non-invertible transformations is that potential impostors are not able to reconstruct the entire biometric data even if transforms are compromised. However, applying non-invertible transformations mostly implies a

loss of accuracy. Performance decrease is caused by the fact that transformed biometric templates are difficult to align (like in biometric cryptosystems) in order to perform a proper comparison and, in addition, information is reduced. For several approaches these effects have been observed [1, 5].

Ratha et al. [1] were the first to introduce the concept of cancelable biometrics applying non-invertible transformations. Generally, at enrollment, non-invertible transformatioms are applied to biometric inputs choosing application-dependent parameters. During authentication, biometric inputs are transformed and a comparison of transformed templates is performed.

Several types of transformations for constructing multiple cancelable biometrics from pre-aligned fingerprints and face biometrics have been introduced in [1, 4, 6] including Cartesian transform and functional transform. In further work [5], different techniques to create cancelable iris biometrics have been proposed. The authors suggest four different transforms applied in image and feature domain where only small performance drops are reported.

Hammerle-Uhl et al. [7] applied classic transformations suggested in [1] to iris biometrics. Furthermore, in [8] it is shown that applying both transformations to rectangular iris images, prior to preprocessing, does not work. Similar to [7] Rathgeb and Uhl [9] suggest to apply row permutations to iris-codes.

Maiorana et al. [10-12] apply non-invertible transformations to obtain cancelable templates from online signatures. In their approach, biometric templates, which represent a set of temporal sequences, are split into non-overlapping sequences of signature features according to a random vector which provides revocability. Subsequently, the transformed template is generated through linear convolution of sequences. The complexity of reconstructing the original data from the transformed template is computationally as hard as random guessing.

Boult et al. [13, 14] proposed cryptographically secure bio-tokens which they applied to face and fingerprints. In order to enhance security in biometric systems, bio-tokens, which they refer to as Biotope™, are adopted to existing recognition schemes (e.g., PCA for face).

3. BIOMETRIC SALTING

Biometric salting usually denotes transforms of biometric templates which are selected to be invertible. Any invertible transform of biometric feature vector elements represents an approach to biometric salting even if biometric templates have been extracted in a way that it is not feasible to reconstruct the original biometric signal [15]. As a consequence, the parameters of the transform have to be kept secret. In case user-specific transforms are applied, the parameters of the transform (which can be seen as a secret seed [16] have to be presented at each authentication. Impostors may be able to recover the original biometric template in case transform parameters are compromised, causing a potential performance decrease of the system in case underlying biometric algorithms do not provide high accuracy without secret transforms. While approaches to biometric salting may maintain the recognition performance of biometric systems non-invertible transforms provide higher security [4].

Savvides et al. [15] generate cancelable face biometrics by applying so-called minimum average correlation filters which provide non-invertibility. User-specific secret personal identification numbers (PINs) serve as seed for a random basis for the filters similar to [17].

Another approach to biometric salting was presented by Wang and Plataniotis [18] in which face features are transformed based on a secret key. Non-invertibility is achieved by means of quantization.

Ouda et al. [19, 20] propose a technique to obtain cancellable iris-codes. Out of several enrollment templates a vector of consistent bits (BioCode) and their positions are extracted. Revocability is provided by encoding the Bio-Code according to a selected random seed. Pillai et al. [21] achieve cancelable iris templates by applying sector random projection to iris images. Recognition performance is only maintained if user-specific random matrices are applied.

4. PERFORMANCE IMPLICATIONS

While in the majority of proposed approaches to cancellable biometrics template alignment is non-trivial and applied transformations are selected to be non-invertible, still some schemes [22, 16] report an increase in performance. In case user-specific transforms are applied at enrolment and authentication, by definition, two-factor authentication is yielded which may increase the security but does not affect the accuracy of biometric authentication.

A significant increase of recognition rates can be caused by unpractical assumptions during performance evaluations. If user-specific transforms are applied to achieve cancellable biometric these transforms have to be considered compromised during inter-class comparisons. Otherwise, biometrics becomes meaningless as the system could rely on secret tokens parameters without any risk [23]. Secret tokens, be it transform parameters, random numbers or any kind of passwords are easily compromised and must not be considered secure [24]. Thus, performance evaluations of approaches to cancellable biometrics have to be performed under the so-called “stolen-token scenario” where each impostor is in possession of valid secret tokens.

5. SECURITY EVALUATION

While in the vast majority of approaches, security is put on a level with obtained recognition accuracy according to a reference system, analysis with respect to irreversibility and unlinkability is rarely done. According to irreversibility, i.e., the possibility of inverting applied transformations to obtain the original biometric template, applied feature transformations have to be analysed in detail. For instance, if (invertible) block permutation of biometric data (e.g., fingerprints in [4] or iris in [7]) is utilized to generate cancelable templates the computational effort of reconstructing (parts of) the original biometric data has to be estimated. While for some approaches,

analysis of irreversibility appear straight forward for others more sophisticated studies are required (e.g., in [11] irreversibility relies on the difficulty in solving a blind deconvolution problem).

In order to provide renewability of protected biometric templates, applied feature transformations are performed based on distinct parameters, i.e., employed parameters define a finite key space (which is rarely reported). In general, protected templates differ more as more distant the respective transformation parameters are [12]. To satisfy the property of unlinkability, different transformed templates, generated from a single biometric template applying different parameters, have to appear random to themselves (like templates of different subjects), i.e., the amount of applicable parameters (key space) is limited by the requirement of unlinkability.

The aim of attacking cancellable biometric systems is to expose the secret transformation (and parameters) applied to biometric templates. Thereby potential attackers are able to apply substitution attacks. If transforms are considered invertible, original biometric templates may be reconstructed. Since most approaches to biometric salting become highly vulnerable in case secret tokens are stolen [23], false accept attacks could be effectively applied. If the salting process is invertible, templates may be reconstructed and applied in masquerade attacks.

5. CONCLUSION

Cancelable biometrics is expected to increase the confidence in biometric authentication systems (trusted identification). This technology permanently protects biometric templates against unauthorized access or disclosure by providing biometric comparisons in the encrypted domain, preserving the privacy of biometric characteristics [25]. Cancelable biometrics keep biometric templates confidential meeting security requirements of irreversibility, and unlinkability.

REFERENCES

[1] N. K. Ratha, J. H. Connell, R. M. Bolle RM, "Enhancing security and privacy in biometrics-based authentication systems", IBM Syst J 2001, 40:614-634.

[2] A. Cavoukian, A. Stoianov, "Biometric encryption", in Encyclopedia of Biometrics Springer; 2009.

[3] A. Ross A, J. Shah, A. K. Jain, "From template to image: reconstructing fingerprints from minutiae points", IEEE Trans Pattern Anal Mach Intell 2007, 29(4):544-560.

[4] N. K. Ratha, J. H. Connell, S. Chikkerur, "Generating cancelable fingerprint templates", IEEE Trans Pattern Anal Mach Intell 2007, 29(4):561-572.

[5] J. Zuo, N. K. Ratha, J. H. Connel, "Cancelable iris biometric", In Proc, of the 19th Int. Conf. on Pattern Recognition 2008 (ICPR'08) 2008, 1-4.

[6] N. K. Ratha, J. H. Connell, R. M. Bolle, S. Chikkerur, "Cancelable biometrics: a case study in fingerprints", In Proc. of the 18th Int. Conf. on Pattern Recognition 2006, pp. 370-373.

[7] J. Hämmerle-Uhlr, E. Pschernig, A. Uhl, "Cancelable iris biometrics using block re-mapping and image warping", In Proc. of the Information Security Conf. 2009 (ISC'09) LNCS 2009, 5735:135-142.

[8] P. Färberböck, J. Hämmerle-Uhl, D. Kaaser, E. Pschernig, A. Uhl, "Transforming rectangular and polar iris images to enable cancelable biometrics", In Proc. of the Int. Conf. on Image Analysis and Recognition (ICIAR'10), Volume 6112. Springer LNCS; 2010:276-386.

[9] C. Rathgeb, A. Uhl, "Secure iris recognition based on local intensity variations", In Proc. of the Int. Conf. on Image Analysis and Recognition (ICIAR'10). Volume 6112. Springer LNCS; 2010:266-275.

[10] E. Maiorana, M. Martinez-Diaz, P. Campisi, J. Ortega-Garcia, A. Neri, "Template protection for HMM-based on-line signature authentication", In Proc. Of Workshop Biometrics CVPR Conference 2008, 1-6.

[11] E. Maiorana, M. Martinez-Diaz, P. Campisi, J. Ortega-Garcia, A. Neri, "Cancelable biometrics for hmm-based signature recognition", In Proc of the 2nd IEEE Int. Conf. on Biometrics: Theory, applications and systems (BTAS'08) 2008, 1-6.

[12] E. Maiorana, M. Martinez-Diaz, P. Campisi, J. Ortega-Garcia, A. Neri, "Cancelable templates for sequence-based biometrics with application to on-line signature recognition", Trans Syst Man Cybernet A Syst Hum 2010, 40(3):525-538.

[13] T. Boult, "Robust distance measures for face-recognition supporting revocable biometric tokens", FGR '06: Proc. of the 7th Int. Conf. on Automatic Face and Gesture Recognition 2006, 560-566.

[14] T. Boult, W. Scheirer, R. Woodworth, "Revocable fingerprint biotokens: Accuracy and security analysis", IEEE Computer Society Conference on Computer Vision and Pattern Recognition 2007, 1:1-8.

[15] M. Savvides, B. Kumar, P. Khosla, "Cancelable biometric filters for face recognition", ICPR '04: Proc of the Pattern Recognition, 17th Int Conf on (ICPR'04) 2004, 3:922-925.

[16] A. B. J. Teoh, Y. W. Kuan, S. Lee, "Cancellable biometrics and annotations on biohash", Pattern Recognition 2008, 41(6):2034-2044.

[17] C. Soutar, D. Roberge, A. Stoianov, R. Gilroy, B. V. Kumar, "Method for secure key management using a biometrics", US Patent 2001, 6219794.

[18] Y. Wang, K. Plataniotis, "Face based biometric authentication with changeable and privacy preservable templates", In Proc. of the IEEE Biometrics Symposium 2007, pp. 11-13.

[19] O. Ouda, N. Tsumura, T. Nakaguchi, "Bioencoding: a reliable tokenless cancelable biometrics scheme for protecting iris codes", IEICE Trans Inf Syst 2010, E93.D:1878-1888.

[20]. O. Ouda, N. Tsumura, T. Nakaguchi, "Tokenless cancelable biometrics scheme for protecting iris codes",

Proc of the 20th Int. Conf. on Pattern Recognition (ICPR'10) 2010, 882-885.

[21] J. K. Pillai, V. M. Patel, R. Chellappa, N. K. Ratha, "Sectored random projections for cancelable iris biometrics", In Proc. of the IEEE Int Conf. on Acoustics Speech and Signal Processing (ICASSP) 2010, 1838-1841.

[22] E. Reddy, I. Babu, "Performance of Iris Based Hard Fuzzy Vault", Int J Comput Sci Netw Secur (IJCSNS) 2008, 8(1):297-304.

[23] A. Kong, K-H Cheunga, D. Zhanga, M. Kamelb, J. Youa, "An analysis of BioHashing and its variants", Pattern Recognition 2006, 39:1359-1368.

[24] A. K. Jain, A. Ross, S. Prabhakar S, "An introduction to biometric recognition", IEEE Trans Circ Syst Video Technol 2004, 14:4-20.

[25] A. K. Jain, P. J. Flynn, A. A. Ross, "Handbook of Biometrics", Springer; 2008.