

Accuracy and Security Evaluation of Multi-Factor Biometric Authentication

Hisham Al-Assam, Harin Sellahewa, Sabah Jassim
Department of Applied Computing
University of Buckingham
Buckingham, MK18 1EG, United Kingdom
{hisham.al-assam, harin.sellahewa, sabah.jassim}@buckingham.ac.uk

Abstract

This paper aims to evaluate the security and accuracy of Multi-Factor Biometric Authentication (MFBA) schemes that are based on applying User-Based Transformations (UBTs) on biometric features. Typically, UBTs employ transformation keys generated from passwords/PINs or retrieved from tokens. In this paper, we not only highlight the importance of simulating the scenario of compromised transformation keys rigorously, but also show that there has been misevaluation of this scenario as the results can be easily misinterpreted. In particular, we expose the falsehood of the widely reported claim in the literature that in the case of stolen keys, authentication accuracy drops but remains close to the authentication accuracy of biometric only system. We show that MFBA systems setup to operate at zero (%) Equal Error Rates (EER) can be undermined in the event of keys being compromised where the False Acceptance Rate reaches unacceptable levels. We demonstrate that for commonly used recognition schemes the FAR could be as high as 21%, 56%, and 66% for iris, fingerprint, and face biometrics respectively when using stolen transformation keys compared to near zero (%) EER when keys are assumed secure. We also discuss the trade off between improving accuracy of biometric systems using additional authentication factor(s) and compromising the security when the additional factor(s) are compromised. Finally, we propose mechanisms to enhance the security as well as the accuracy of MFBA schemes.

1. Introduction

Authentication methods can be broadly categorised into three groups: 1) knowledge-based, typically using

a password or a PIN. 2) object-based, which relies on possession of a token. 3) biometric-based, which relies on the uniqueness of physical/behavioural characteristics of a person such as fingerprint, facial features, iris, and voice. Each authentication method has its own advantages and disadvantages. A random password can offer an extremely strong security mechanism for user authentication. However, in practice, secret passwords that humans can easily remember are often short and easy to guess. On the other hand, the major security drawback of a physical token is that, if lost or stolen, an impostor can gain unauthorized access. However, unlike compromised passwords, in case of a lost or stolen token, the token's owner has physical evidence and can consequently react to prevent any further misuse of his/her token. In biometric-based authentication, a legitimate user does not need to remember or carry anything and it is known to be more reliable than traditional authentication schemes. However, the security of biometric systems can be undermined in a number of ways. For instance, a biometric template can be replaced by an impostor's template in a system database or it might be stolen and replayed. Moreover, it has been shown that it is possible to create a physical spoof starting from standard biometric templates [1], [2].

In the recent past, research has focused on securing biometric templates as a mean of maintaining security and integrity of biometric systems. Several multi-factor biometric authentication schemes have been proposed to enhance both security and accuracy of biometric systems. An important example of two-factor biometric authentication is the use of a User-Based Transformation (UBT) on biometric features as illustrated in Figure 1. Perfect authentication results (0% EER) have been reported in many cases under the assumption that transformation keys are secure [3], [4], [5], [6], [7], and [8].

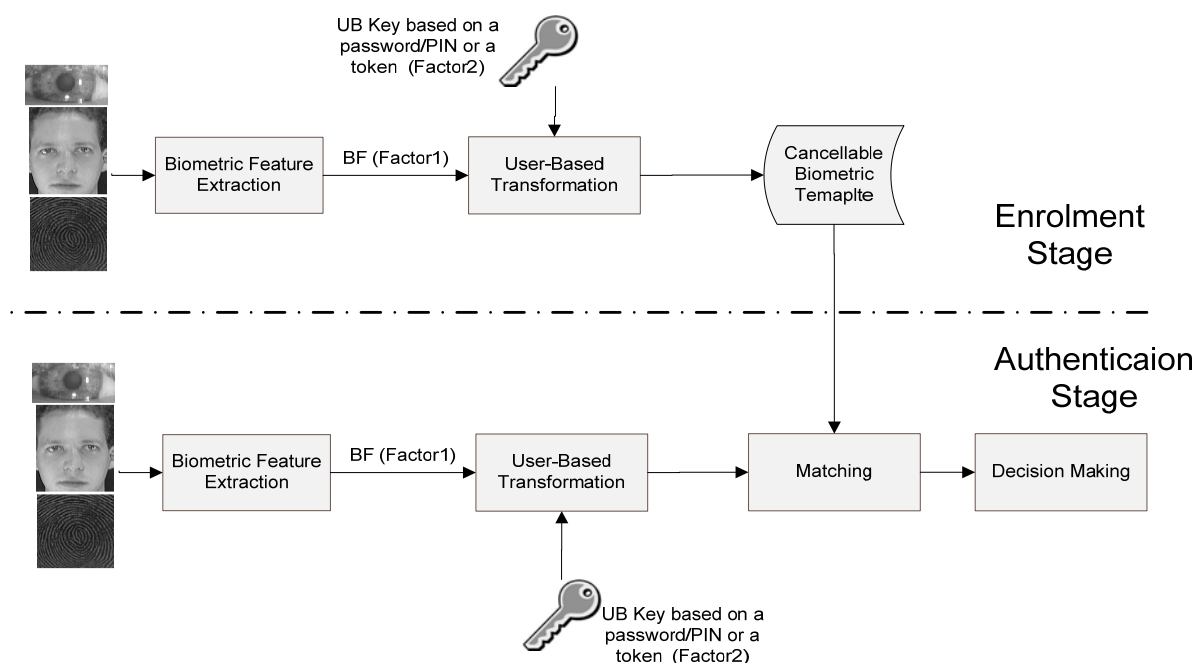


Figure 1. General operations of a Multi-factor biometric authentication system based on UBTs approach during enrollment and authentication stages

Several researchers [9], [10],[11] have emphasised the importance of simulating the case of impostors using stolen keys, and argued that assuming that the additional factor will never be compromised is a biased assumption. Here, we argue that the performance of the multi-factor biometric authentication system in the scenario of compromised keys has not been simulated properly, and there has been misvaluation/misinterpretation of simulation results.

This paper is primarily concerned with the case of biased evaluation of two-factor biometric authentication in a scenario of stolen keys. We attempt to substantiate our claim that in such a scenario, a system setup to maintain zero (%) EER has serious security implications due to unacceptable levels of FAR.

The rest of the paper is organized as follows: Section 2 reviews two-factor authentication schemes. In Section 3, we evaluate the performance of two-factor biometric authentication for three scenarios: biometric only authentication, two-factor authentication with secure keys and two-factor authentication with compromised keys. Further discussion and analysis will be presented in Section 4. Conclusion will be in Section 5.

2. Background

2.1 User-Based Transformations (UBTs)

Multi-Factor Biometric Authentication (MFBA) schemes are mostly based on applying User-Based Transformations (UBTs) on biometric features. Typical UBTs rely on transformation keys generated from passwords/PINs or retrieved from tokens. Figure 1 illustrates the operations of a typical MFBA system based of UBTs approach during the enrollment and authentication stages. In this section we briefly describe two types of UBTs: Random Projections (RP) and password-based shuffling. RP is a technique that uses random orthonormal matrices to map a vector space into another while preserving distances and other geometric measures. RP has been proposed as a secure transform for biometric templates [5], [12] to meet the revocability property for biometric-based authentication systems. It is used to generate a cancellable template for fingerprint data [3] and face image data [8]. A quantization step might be added to make the transform non-invertible [6].

Typically, RP is applied in two stages: 1) generate a user-based orthonormal $n \times n$ matrix A , where n is the size of biometric feature vectors, and 2) transform the original template feature vector x to a secure domain using matrix product: $y=Ax$.

Random orthonormal matrices are generated from a user-based key or token using Gram-Schmidt algorithm [5], [12] or using an efficient method based on the fact that small size orthonormal matrices can be generated without a need for Gram-Schmidt procedure [13].

Another type of UBTs is Password-Based Shuffling (PBS) [14]. A shuffling key of size k generated from password is used to shuffle an iris code that is divided into k block. As illustrated in Figure 2, if a bit in the key is 1, the corresponding iris code block is moved to the beginning; otherwise it is moved to the end (see [14] for further details).

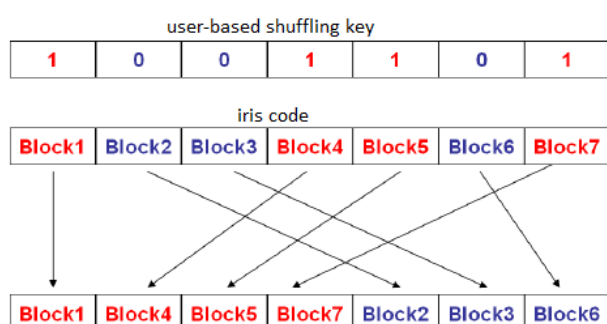


Figure 2. User-based shuffling for iris codes as it was proposed in [14]

2.2 Existing Work

Jain et al [5] and Teoh et al [3] employed a UBT (namely an RP) on fingerprint features as a two-factor fingerprint authentication, and a perfect verification of 0% EER was reported in the two papers. In [5], fixed size FingerCode features are extracted using the method described in [16]. Then a user-based RP is applied in two scenarios: secure and stolen transformation keys. It was reported that in the scenario where the impostor knows the true key, i.e. has access to the user's RP, the performance of the system is close to the case when no RP technique is applied i.e. FRR \approx 7% at FAR=1%. In [3], wavelet transforms are used as a feature extraction technique followed by user-based RP to secure fingerprint features. A 0% EER is attained assuming that the UBT is unknown to the impostor.

RP was also used in [6] and [8] to protect facial features and achieve cancellable biometrics. It was applied in two scenarios: secure and stolen keys. Both papers reported 0% EER in case of secure transformation keys. In [8], the same recognition accuracy was reported in cases of stolen keys (i.e. the UBT is known to the impostor) and biometric only (no

secure transformation), EER=7.19% in the two cases. In [8], 16.21% EER was reported in stolen keys scenario compared to 15.63% EER in case of biometric only face recognition.

In [14], the authors reported better accuracy when the keys are secure whereas compromised keys scenario was not reported. Furthermore, UBTs were also proposed to protect iris [6] and palm [9] features with enhanced performance. Again, zero (%) EER was reported under the assumption that keys are secure. In [4], the performance of iris recognition only was slightly better than the performance in a stolen keys scenario whereas in [7], the authors simulated the case only when transformation keys are secured.

The biasness of the assumptions on security of MFAS, on the other hand, has also been noticed.

Konga et al, in [9] and [10], have explained that achieving zero (%) EER is based on a false assumption that the token or a password that used to generate a UBT key would never be lost, stolen, shared or duplicated. Beside the authors work [15], recently Rathgeb and Uhl [11] questioned the accuracy improvement of two-factor biometric authentication demonstrating that high accuracy achieved when iris codes were XORed with a user-based random bits relies on impractical assumption, that the user-based random bits will never be compromised.

3. Performance Evaluation of Two-Factor Biometric Authentication

This section aims to evaluate the performance of two-factor biometric system under different assumptions about the security of the non-biometric factor. Three biometric traits, namely fingerprint, iris, and face, are tested in three scenarios: 1) *scenario A* - biometric only authentication, 2) *scenario B* - two-factor authentication with a biometric and a secure key, and 3) *scenario C* - two-factor authentication with a biometric and a compromised (stolen) user-based key. Our evaluations are based on 3 commonly used datasets:

1) The FVC2002-DB2 fingerprint is a publicly available database [17]. It consists of 100 different fingers with 8 impressions per finger.

2) The ORL face database [18] consisting of 40 persons; each has 10 images, taken at different times with some variations in facial expressions and pose.

3) The Chinese Academy of Sciences, Institute of Automation (CASIA) iris database [19] consisting of 756 greyscale eye images for 108 individuals where each individual has 7 eye images.

3.1 Two-Factor Fingerprint Evaluation

FingerCode-based fingerprint recognition approach described in [16] produces fixed length templates (feature vectors) whereas minutia-based fingerprint recognition approach [17] produces templates whose sizes are not necessarily the same. Applying random projection to produce cancellable biometric template requires fixed length feature vectors, which makes FingerCode approach is the most appreciated choice for our implementation.

FingerCode algorithm [16] can be summarized as follows. After tessellating the Region Of Interest (ROI) around the reference point, a bank of Gabor filters are applied in eight directions (0 degree, 22.5, 45, 65.5 degree, 90, 112.5, 135, 157.5) with respect to x-axis to capture both local and global features of a fingerprint image (see [16] for further details). In our experiment, the ROI was divided into 64 sectors. Each sector is represented by one value that is the standard deviation of eight filters [16]. As a result, the fixed length of a FingerCode features= 64x8 discs (eight directions) resulting 512 features in total in each FingerCode.

In our demonstration, we consider only the first three impressions from each finger because extracting FingerCode features requires an accurate detection of the reference points. The first image of each user is used as a template and the remaining two images are employed for testing i.e. 100 images form a gallery set and 200 images form a probe set.

RP has been applied on fingerprint features in two cases: secure and compromised keys. In the secure key scenario, each FingerCode is secured by random projection using a user-based key. Figure 3 shows the performance of fingerprint authentication system in terms of FAR and FRR for the three scenarios. One can see that in the second case, the two-factor fingerprint authentication has an incredible performance of zero (%) EER exactly as reported in the literature. Moreover, the performance in the case of compromised key is exactly the same as that of biometric-only authentication due to the fact that orthonormal matrices preserve Euclidean distances (see [13], [20] for further details). Note that, the operating point (OP) in this two-factor authentication is far apart from the OP of the biometric only authentication. A perfect performance, i.e. 0% EER, can be achieved by the two-factor scheme for any OP selected in the range [44..58]. Even if the OP of the two-factor scheme is chosen as the lowest threshold that produces 0% EER under the assumption that the key is secure, the performance of the scheme is significantly lower than that of the biometric-only scheme when the key is stolen with an FAR in excess of 33%. If the OP is selected in the middle of the

range, i.e. 51, FAR increases significantly to nearly 60% when the key is stolen. Perhaps, if nothing can be done about protecting the key, one should select the OP with care.

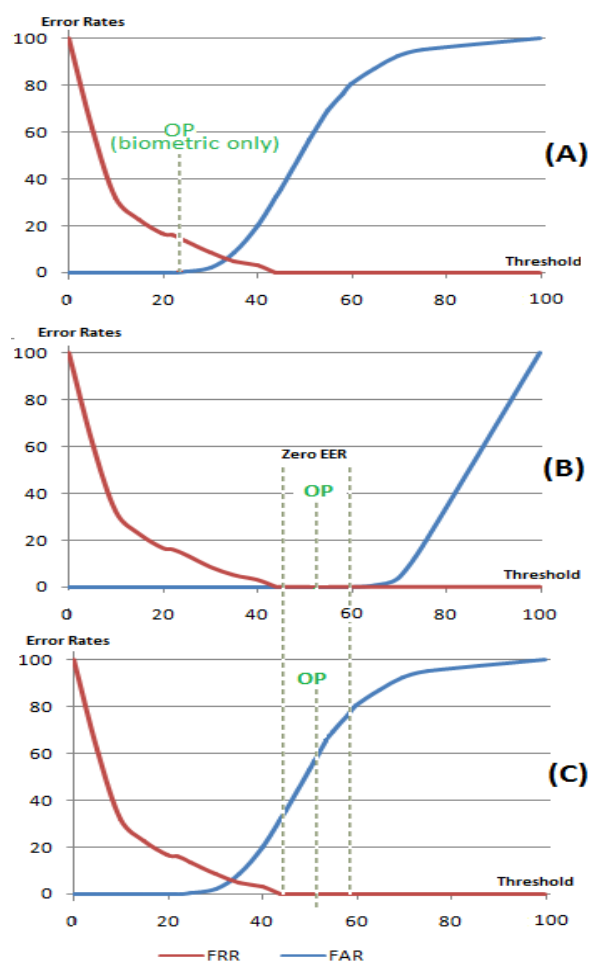


Figure 3. Fingerprint authentication accuracy, FAR% and FRR%, in the three scenarios

3.2 Two-Factor Face Evaluation

For face recognition, we used a wavelet-based recognition scheme, whereby the feature vector representation of a face is the coefficients in a specific frequency subband of wavelet decomposed face image [13]. The low-pass subband LL_3 , which represents the third level resolution approximation of the image, is selected as a feature vector. The first five images per user in the ORL face database were selected to form the gallery set and the remaining images were used for testing.

RP is applied as described briefly in section 2.1 in terms of the matrix equation $y = Ax$ where $A = BxP$, P is a random permutation matrix and B is a block diagonal orthogonal matrix constructed using 2×2 random rotation matrices, see [13]. In case of a stolen key, both impostors and clients use the same orthonormal matrices. Figure 4 shows the charts of the performance of the face authentication system for the three scenarios. For simplicity, we only simulate the case when $A=B$ although in extreme cases B can be estimated.

Here we note that in the second scenario, the two-factor face authentication has a zero (%) EER. However, the true performance in the case of stolen key is $FAR=66.6\%$ ($OP=53$), which is unacceptable from security perspective.

Table 1 provides further details on evaluating two-factor face authentication. The same analysis about the FAR curves in Figure 3 applies equally to the charts in Figure 4. One can notice that selecting an operating point (OP) at threshold 25 in case of biometric only results in $FAR=0.67\%$ at $FRR=21.5\%$ whereas achieving a perfect performance, i.e. 0% EER, based on two factors, requires selecting another operating point in the range $[40..65]$. An OP in the middle of the range that gives 0% ERR is selected, namely $OP=53$. Now, in case of compromised key of two-factor biometric authentication, (Fig. 4 (C)) with $OP=53$ and if the matcher does not know whether the key is stolen key or not, then the FAR is 66.6% which means that an impostor with a stolen key needs less than two attempts on average to be falsely admitted as a genuine user. The fact that 0% EER can be achieved for a rather wide range of OP values means that one can maintain 0% EER (if the key is compromised) by selecting an OP in that range but nearer to that used for the biometric-only case. Even with such a policy that takes into consideration that the transformation key maybe compromised, the assumption of 0% EER results in nearly 25% FAR when the key is actually compromised.

3.3 Two-Factor Iris Evaluation

Iris recognition [21] can be summarized as follows. After localization of the iris in an eye image, the iris image is normalized to a fixed size, and filtered using a bank of Gabor filters. The output is quantized to produce a binary iris code.

In our experiments, the first image of each eye in the CASIA database is used as a template, and the remaining 6 are used for testing. In our experiments, the password-based shuffling described in Sec. 2.2 has been applied on iris codes, and the performance of the

corresponding two-factor authentication scheme is evaluated for two scenarios: secure and compromised shuffling key.

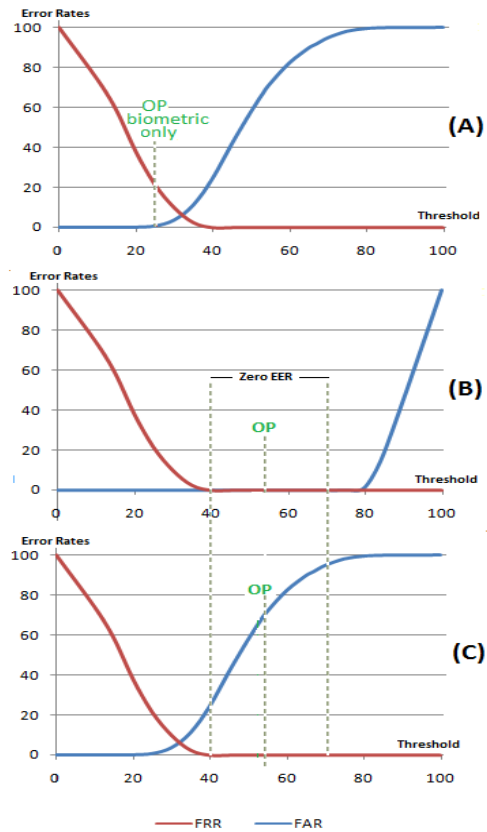


Figure 4. Face authentication accuracy, FAR% and FRR%, in the three scenarios

Table 1. Face authentication accuracy in the 3 scenarios

Decision Threshold	A		B		C	
	FAR	FRR	FAR	FRR	FAR	FRR
25	0.67	21.5	0	21.5	0.67	21.5
	Single-Factor OP				NOT the right OP	
30	3.62	10	0	10	3.62	10
40	24.44	0	0	0	24.44	0
53	66.69	0	0	0	66.69	0
			Two-Factor Operating point			
70	94.79	0	0	0	94.79	0
80	99.44	0	1.49	0	99.44	0

It can be seen from Figure 5 that the operation point (OP) that gives the best performance for the biometric only authentication scheme results in $FAR=0.1\%$ & $FRR=9.55\%$ (Fig.5 (A)) whereas the OP that gives the best performance for the multi-factor biometric

authentication scheme results in FAR=0.1% & FRR=2.66% (Fig.5 (B)).

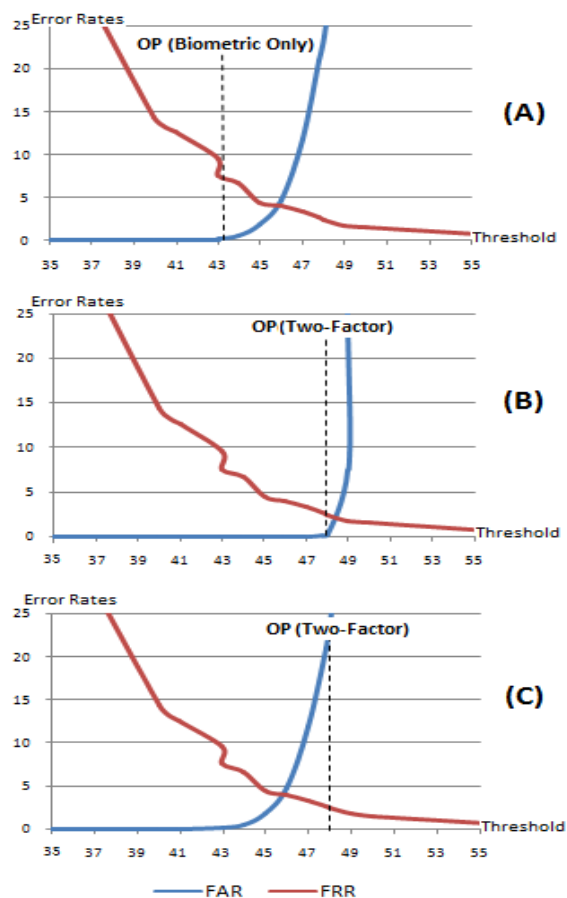


Figure 5. Iris authentication accuracy in the 3 scenarios

Again there is a noticeable difference between the two OP thresholds. This means that *scenario B* has better authentication accuracy than *scenario A*. However, in the event of compromised keys in *scenario C* (Fig.5 (C)), the FAR is 21% which is unacceptable from security perspectives. Further details are presented in Table 2.

Table 2. Iris authentication accuracy in the 3 scenarios

Decision Threshold	A		B		C	
	FAR	FRR	FAR	FRR	FAR	FRR
43	0.10	9.55	0	9.55	0.10	9.55
	Single-Factor OP		NOT the right OP			
45	1.79	4.44	0	4.44	1.79	4.44
47.8	21.01	2.66	0.10	2.66	21.01	2.66
			Two-Factor Operating point			
50	60.48	1.55	51.80	1.55	60.48	1.55

4. Accuracy vs. Security

The biased evaluation of the performance of two-factor biometric authentication means that simulating the case of insecure keys is done at operating point(s) whose values are completely different from the operating point(s) in case of secure key. Table 3 summarizes some results that were reported in the literature, and includes the correct evaluation at the end. It can be clearly noticed that apart from our results, excellent authentication accuracy was reported when keys are assumed to be secure, whereas stolen key scenario was either not simulated or an authentication accuracy equal or close to the case of biometric only was reported. Moreover, one can see that achieving zero (%)EER results in high FAR 56.6%, 66.6%, and 21% in case of stolen transformation keys using fingerprint, face, and iris biometric respectively. These results highlight serious security implications for the two-factor biometric systems.

UBTs typically have no (or a very slight) effect on intra-class variations while it significantly increases inter-class variations. As it can be noticed from Figures 3, 4, and 5, the FRR line remains the same in the three scenarios. However, the FAR line in the three Figures is shifted to the right in the secure keys scenario, (scenario B), to offer better separation between clients and impostors which results in better authentication accuracy whereas in the stolen keys scenario, (scenario C), the FAR is shifted back to its original state when no transformation is applied.

Two-factor biometric authentication results in a trade-off between accuracy and security. Enhancing the accuracy in case of secure keys two-factor authentications (decreasing FRR) requires shifting the OP of a single-factor authentication to the right (i.e. relaxing the decision threshold), which results in a high FAR if user-based key is compromised. Thus, aiming at zero (%) or near zero (%) EER in secure keys scenario compromises the security of the two-factor biometric authentication system when the transformation key is stolen.

This situation could be improved by appropriate choice of the OP that takes into account reasonable assumptions on the possibility of key theft. Figure 6 illustrates the trade-off between accuracy and security in two-factor authentication systems: (A) two-factor fingerprint (B) two-factor face authentication. One can notice that enhancing the accuracy of two-factor authentication, i.e. decreasing FRR, requires shifting the operating point of a single-factor, i.e. biometric only, authentication to the right. However, accuracy enhancement in case of secure keys two-factor

authentications results in much higher FAR if user-based key is compromised. Thus, aiming at perfect accuracy, 0% EER, in secure keys scenario compromises the security of the two-factor biometric authentication system when the transformation key is known to the attacker.

Table 3. Authentication results reported in the literature in addition to our evaluation in the three scenarios

Ref	Trait	Biometric only	Two-Factor (secure)	Two-Factor (insecure)
[6]	Fingerprint	EER=5.66	EER = 0	N/A
[7]	Iris	EER=3.2	EER = 0	EER =4.6
[8]	Fingerprint	FAR≈1 at FRR=7	EER = 0	FAR≈1 at FRR=7
[9]	Face	EER = 15.63	EER = 0	EER = 16.21
[10]	Palm	EER =2.75	EER = 0	N/A
[11]	Face	EER= 7.19	EER =0	EER = 7.19
This paper	Fingerprint	FAR=0.1 at FRR=16	EER =0	FAR= 56.6 at FRR=0
	Face	FAR=0.67at FRR=21.5	EER =0	FAR= 66.6 at FRR=0
	Iris	FAR=0.1 at FRR=9.55	FAR=0.1 at FRR=2.66	FAR= 21 at FRR=2.66

It can be seen from figure 6 that the probability of an imposter with a stolen key being falsely accepted grows significantly when the operating point is shifted to the right to enhance the accuracy of two-factor biometric authentication. Hence, there is a need for a strategy to select the appropriate OP and maintain optimal performance without unreasonable assumption on the security of the non-biometric factor(s). In the next section, we discuss ways of enhancing the performance of MFBA schemes and propose a strategy for OP value selection,

5. Improving MFBA Robustness

5.1. Challenge and response approach.

The incorporation of a Challenge and Response (C&R) step into authentication schemes certainly improves the security of the authentication in that it prevents replay attacks. Here we describe such a step for the case where the UBT is a random projection as described in section 2.1.

Given a fresh n-dimensional biometric feature vector X, and an nxn orthonormal random projection A which we can assume that it has been selected at the enrollment stage. If b is an n-dimensional random blinding vector generated by the server (i.e. the authenticator side) and sent to the client, over a secure channel, as a challenge then the formula:

$$Y = AX + b$$

can be sent by the client to the server for matching which incorporates the transformed fresh template with the response. Since b is a random vector generated during the authentication session then it is expected to provide a prevention mechanism against replay attack. However, b needs to be selected in a sensible manner so that it significantly changes the matching scores, otherwise it may result in reduced accuracy. In a previous set of experiments we found that the best choice for $b = [b_1, b_2, \dots, b_n]$ where

$$b_i \in [\min(X) \max(X)], \quad i=1, \dots, n.$$

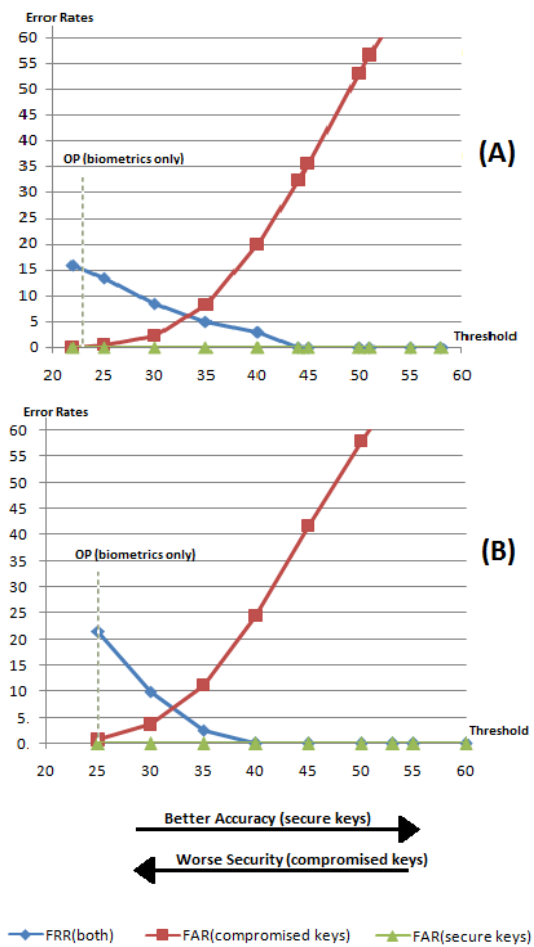


Figure 6. The trade-off between accuracy and security (A) two-factor fingerprint (B) two-factor face authentication

5.2. Partial compromise of UBT key

Here, we propose a strategy for the selection of an appropriate OP that relies on evaluating performance in a number of scenarios where impostors have varying

degrees of knowledge of the non-biometric factor. The proposed strategy addresses the following question: what if an imposter manages to guess part of the transformation key? The answer obviously depends on the transformation type. For illustration purposes, random projection based face authentication is selected as a case study, using both schemes: with and without the C&R step. Note that, these two schemes can be linked to the same matrix equation:

$$Y = O X + b$$

where $b = 0$ means no C and R.

Figure 7A shows two-factor face authentication accuracy in terms of equal error rates in the two cases: b is a zero vector and b is a non-zero vector when {10%, 20%,...,100%} of the transformation key being compromised. It can be seen that when a random projection [13] is used to produce a two-factor biometric representation of a user, a zero error rate can be achieved even when 52% and 90% of the transformation keys being compromised where b is a zero and a non-zero vector respectively.

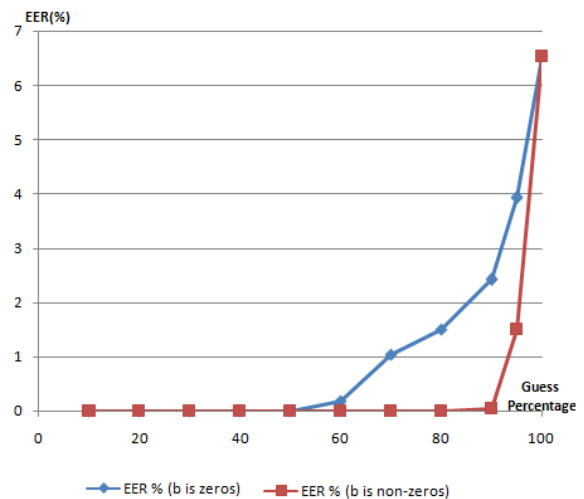
Figure 7 B and C depict the False Acceptance Rates, and the False Rejection Rates in two cases: b is a zero and non zero vector respectively. The graphs show that guessing the second factor (i.e. the transformation key O) has no effect on FRR. However, FAR is severely affected by compromised keys. The larger the guessed percentage of the key, the smaller the margin between FAR and FRR. It can be seen from these charts that the appropriate choice of the OP for improved accuracy does not compromise the security of the MFBA system even when 80% (resp. 90%) of the transformation key is guessed by an imposter in the case of $b=0$ (resp. $b \neq 0$). These results demonstrate that analyzing accuracy under varying level of MFBA compromised keys can shed light on the security of the system without creating unpleasant consequences.

6. Conclusion

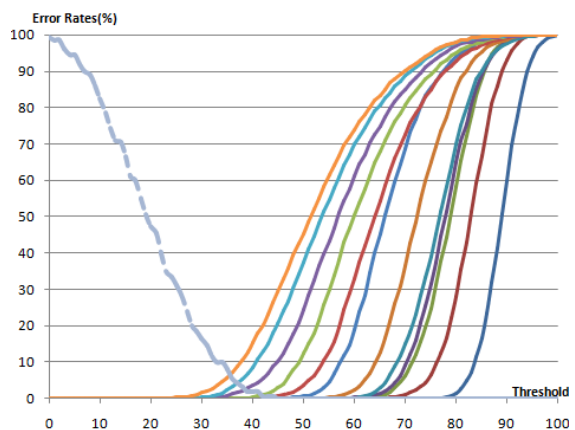
In this paper we have investigated the trade-off between high accuracy and security of two-factor biometric authentication schemes for three commonly used biometric traits. We have demonstrated that the conventional wisdom that in the case of compromised key(s), the accuracy of two-factor authentication drops but remains close to the accuracy of the biometric-only scheme is based on a false and biased assumption. Furthermore, this paper showed by experiments conducted on fingerprint, iris, and face biometrics that if a two-factor biometric system is configured to yield a zero or near zero EER, the probability of an impostor with a stolen transformation

key being falsely accepted will be markedly high. Consequently, setting a two-factor biometric authentication system to achieve zero EER introduces a serious lapse in security in the case of stolen keys where the FAR reaches unacceptable levels.

We have demonstrated that when the system is unaware of the key being stolen, the FAR increases rapidly from zero to 21%, 56.6% and 66.69% for iris, fingerprint, and iris respectively. Finally, we have described and tested two techniques that can be combined to greatly reduce the effect of stolen keys on accuracy, when the system is not aware of the theft. The first technique is the incorporation of a challenge and response at the authentication stage, while the other is an approach to analyse accuracy under the assumption of partially compromised transformation keys.



(A)



(B)

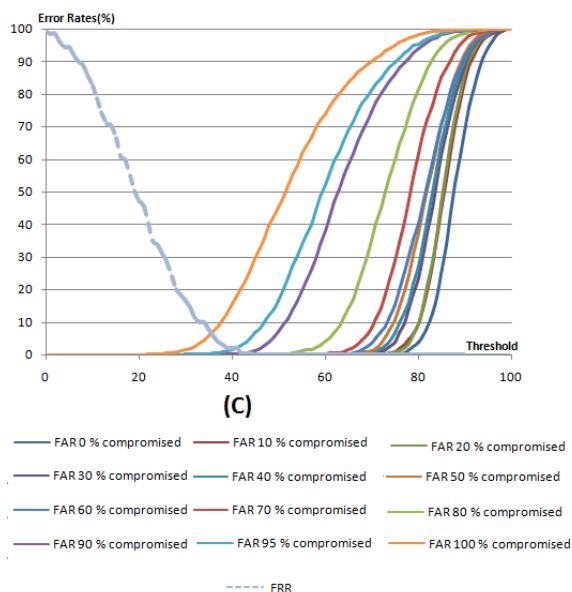


Figure 7. Partial compromising of transformation keys of random projection $Y= OX+b$ where 10%, 20%,..., 100% of the transformation key is guessed. A) Equal Error Rates (EER %) in two setups: b is zero vector, and b is non-zero vector, B) False Acceptance Rates (FARs) and False Rejection Rates (FRRs) of two-factor face authentication where b is a zero vector, and C) FARs and FRRs of two-factor face authentication where b is a non-zero vector.

7. References

- [1] A. Adler, Vulnerabilities in biometric encryption systems. 2005. Proc. of Audio and Video-Based Biometric Authentication. Vol. 3546, pp. 1611-3349.
- [2] R. Cappelli, A. Lumini, D. Maio, and D. Maltoni. 2007. Fingerprint Image Reconstruction from Standard Templates. Pattern Analysis and Machine Intelligence. Vol. 29(7), pp. 1489-1503.
- [3] A. Teoh, D. Ngo, A. Goh. BioHashing: two factor authentication featuring fingerprint data and tokenised random number. Pattern Recognition. Vol. 37(11), pp. 2245-2255, 2004.
- [4] L. Alessandra and L. Nanni, "Empirical tests on BioHashing", Neurocomputing, pp. 2390-2395, 2006.
- [5] Anil K. Jain, K. Nandakumar, and A. Nagar, "Biometric Template Security", EURASIP Journal on Advances in Signal Processing. pp. 1-17, 2008.
- [6] Andrew B. J. Teoh, Kar-Ann Toh, and WK. Yip, " 2^N Discretisation of BioPhasor in Cancellable Biometrics. Advances in Biometrics", pp. 435-444, 2007.
- [7] A. Teoh, M. Goh, and D. Ngo, "PalmHashing: a novel approach for dual-factor authentication", Pattern Analysis & Applications. Vol. 7(3), pp. 255-268, 2004.
- [8] Y. Wang and K. Plataniotis, "Face based biometric authentication with changeable and privacy preservable templates", Biometrics Symposium, pp. 1-6, 2007.
- [9] A. Konga, K. Cheung, D. Zhang, M. Kamel, and J. You, "An analysis of BioHashing and its variants. Pattern Recognition", Vol. 39, pp. 1359-1368, 2006.
- [10] A. Konga, K. Cheung, D. Zhang, M. Kamel, J. You., "Revealing the Secret of FaceHashing", Advances in Biometrics, pp. 106-112, 2006.
- [11] Christian Rathgeb and Andreas Uhl, "Two-Factor Authentication or How to Potentially Counterfeit Experimental Results in Biometric Systems", Proc. of the 7th International Conference of Image Analysis and Recognition (ICIAR-2010), pp.296-305, 2010.
- [12] Y C Feng, Pong C Yuen and Anil K Jain, "A Hybrid Approach for Face Template Protection", Proc. SPIE, Vol. 6944, p.p. 694408, 2008.
- [13] H. Al-Assam, H. Sellahewa, and S.A. Jassim, "Lightweight approach for biometric template protection", Proc. SPIE. Vol. 7351, p.p. 73510, 2009.
- [14] S. Kanade, D. Camara, B. Dorizzi, "Three factor scheme for biometric-based cryptographic key regeneration using iris", Biometrics Symposium, pp. 59-64, 2008.
- [15] H. Al-Assam, H. Sellahewa, and S.A. Jassim, "Multi-factor biometrics for authentication: a false sense of security", Proc. of the 12th ACM workshop on Multimedia and security, p.p. 81-88, 2010.
- [16] A. Jain, S. Prabhakar, L. Hong, and S. Pankanti., "Filterbank-Based Fingerprint Matching", IEEE Trans. Image Processing. Vol. 9(5), pp. 846-859, 2000.
- [17] D Maltoni, D Maio, AK Jain, S Prabhakar, "Handbook of fingerprint recognition 2nd Edition", 2009.
- [18] Harter, F.S. Samaria, "Parameterisation of a stochastic model for human face identification", Proc. 2nd IEEE workshop Applications of Computer Vision, 1994.
- [19] Chinese Academy of Sciences. Institute of Automation CASIA Iris Image Database: <http://www.cbsr.ia.ac.cn>. (Access date: 6 May 2009)
- [20] S Jassim, H Al-Assam, H Sellahewa, "Improving performance and security of biometrics using efficient and stable random projection techniques", Image and Signal Processing and Analysis, pp. 556 – 561, 2009.
- [21] J. Daugman, "How iris recognition works". Proc. of Int. Conference on Image Processing, Vol. 1, 2002.