Unpredictability Assessment of Biometric Hashing Under Naive and Advanced Threat Conditions

Berkay Topcu and Cagatay Karabat
TUBITAK BILGEM UEKAE
P.O. 74, 41470
Kocaeli, Turkey
Email: {berkay.topcu, cagatay.karabat}@tubitak.gov.tr

Hakan Erdogan
Sabancı University
Orta Mahalle, Tuzla 34956
İstanbul, Turkey
Email: haerdogan@sabanciuniv.edu

***Abstract*—Recent years have witnessed the use of biometric recognition systems in increasing number of applications with the number of users growing at a steady pace. However, security and privacy problems have arisen from this upsurge of interest to biometric systems. Template protection methods solve such security and privacy problems where unpredictability is a crucial goal. Here, we study the unpredictability of biohashing (a transformation-based template protection method) using entropy as a measure. Our novel work outlines a systematic approach for theoretical evaluation of biohashes using estimated entropy which is based on degree of freedom of Binomial distribution. Our experiments demonstrate that biohash unpredictability varies in different threat models where the entropy of a biohash is almost equal to its bit length under the naive scenario and is significantly low in the advanced scenario, implying that the amount of information kept hidden in a biohash is more likely to be predicted.**

I. Introduction

The deployment of biometric authentication systems in real world applications (e.g., electronic identity cards and border control systems with electronic travel documents) has been a common practice in recent years. Although biometric verification or identification enables fast, reliable, and secure electronic authentication, widespread usage of biometrics arises severe security and privacy issues [1], [2], [3]. In the literature, several biometric template protection methods have been proposed (e.g., fuzzy commitment scheme [4] and biohashing [5]) in order to overcome these concerns by securing biometric templates (e.g., face and fingerprint).

Template protection methods can be classified into two classes [6] as biometric cryptosystems (i.e., fuzzy commitment and fuzzy vault [7] and transformation-based methods (i.e., biohashing). The biometric cryptosystems embed in or generate secrets from biometric data and can precisely retrieve these secrets with the use of auxiliary data during verification. On the other hand, transformation-based approaches distort or randomize biometric data with the use of non-invertible functions so that the original data cannot be reconstructed from transformed templates. Biohashing, an emerging biometric template protection method, uses a unique secret key in order to randomize biometric template of each user. Although biohashing methods have become very popular due to their high authentication performance and easy deployment into match-on-card applications, research recently showed that they may suffer from serious security and privacy problems [8], [9].

Comprehensive evaluation of biometric template protection methods can be carried out by theoretically analyzing the underlying methodology and assessing its vulnerabilities under practical attacks. For biometric cryptosystems, there exist some theoretical analyses utilizing information theoretical metrics (e.g., entropy, conditional entropy, and mutual information) or metrics used in cryptanalysis (e.g., min-entropy, average min-entropy, guessing entropy, and conditional guessing entropy) [10]. However, the applicability of these metrics to empirical evaluation and their computation in practice are still unknown and need further investigation. Unfortunately, transformation-based methods lack any such theoretical analysis. From practical point of view, the strength of transformation-based methods is based on the hardness of invertibility of the underlying transformation. In some studies [11], [12], the most reasonable way of measuring difficulty in reconstructing original biometric features via the inversion of biohashes and practical security analysis of biohashes have been explored. Our earlier work, which is currently under review, has also addressed the reconstruction of biometric features from biohashes with a novel use of sparse recovery.

This current work presents the first successful theoretical evaluation of biometric hashing as required for thorough analysis where the unpredictability of biohashes generated by random projection (RP) based biohashing scheme is quantified via estimated entropy. Since a random projection and quantization method is required in our framework, the first study of Teoh [5] among all other recent alternatives [13] was chosen since none has an effect on our entropy estimation method. The amount of information a biohash carries is quantitatively analyzed by measuring the entropy of a biohash obtained from a face image. Furthermore, to assess to what extent a biohash is unpredictable once the secret key of a user is stolen, the difference in the entropy of the original biohash and the entropy of the one created by using the stolen key along with the biometric feature of an arbitrary person is used.

Our second contribution in this work is to estimate entropies using the degree of freedom of Binomial distribution as described by Daugman [14]. Our work demonstrates that Daugman's entropy estimation cannot only be applied to

978-0-9928-6265-7/16/$31.00 ©2016 IEEE

iris but also to other biometric modalities (e.g., face) that are represented with a fixed-length binary string and can be compared via Hamming distance.

We conducted experiments in a face verification set-up considering two different threat scenarios. Our results showed that the entropy of a biohash is almost equal to its bit length when the secret key of each user is kept safe. However, in the advanced threat scenario where the secret key of a user is compromised, the discriminative effect of the random projection is lost and the entropy of the biohash is limited to the entropy of the biometric feature. This is consistent with the study of Adler *et al*. [15] which shows that the biometric information for a person could be calculated by the relative entropy between the feature distributions of that person and the population (practically measured to be approximately 40 bits).

The second section of this paper describes the random projection-based biometric hashing scheme and the third section outlines the proposed entropy prediction method for biohashes. Experimental results are discussed in the fourth section and finally conclusions are given.

II. BioHashing

Biometric hashing (simply biohashing) schemes are simple yet powerful biometric template protection methods [5], [16], [17], [18], [19], [20]. Biohash is a binary and pseudo-random representation of a biometric template and biometric hashing schemes perform an automatic verification of a user based on his biohash (a binary string). Two inputs of a biometric hashing scheme are: i) biometric template and ii) user specific secret key. A biometric feature vector is transformed into another space using a pseudo-random set of vectors which are generated from the user's secret key. Then, the result is binarized to produce a pseudo-random bit-string which is called the biohash. The random projection matrix is unique and specific to each user and it can be stored in a USB token or a smartcard. In a practical system, a user specific random matrix is calculated using a seed (a user specific secret key) that is stored in a USB token or a smartcard microprocessor through a pseudo random number generator. The seed is the same with that used during the enrollment of a user and is different among different users and different applications [5]. This allows revocability of the subject's biohash in case it is compromised. Also, the same biometric trait of a subject can be used in different biometric recognition systems without constituting privacy threat as two biohashes of the same person with different keys are unlinkable.

A. Enrollment Stage

The first stage in a biometric recognition system is the enrollment stage in which a user is introduced to the system for the first time. His biometric record is captured and converted to a reference biometric template which will be compared to a fresh sample at the authentication stage. This biometric template can be stored either in a central database or a smart card that will be in possession of the user.

a) Random Projection: In the first step, a pseudo random projection (RP) matrix, $\mathbf{R} \in \mathrm{R}^{\ell \times k}$, is generated to transform the PCA coefficient vectors. The RP matrix elements are independent and identically distributed (*i.i.d*) and generated from a Gaussian distribution with zero mean and unit variance by using a Pseudo Random Number Generator (PRNG) with a seed derived from the user's secret key. The RP matrix projects the PCA coefficients onto an ℓ-dimensional space:

$$\mathbf{z} = \mathbf{R}\mathbf{x}, \tag{1}$$

where $\mathbf{z} \in \mathrm{R}^{\ell \times 1}$ is an intermediate biohash vector.

b) Quantization: In this step, elements of the intermediate biohash vector $\mathbf{z}$ are binarized with respect to a threshold:

$$\mathbf{b}(k) = \begin{cases} 1, & \mathbf{z}(k) \geq \beta, \\ 0, & \text{otherwise}, \end{cases} \tag{2}$$

where $\mathbf{b} \in \{0,1\}^{\ell}$ denotes the biohash vector of the user and β denotes the quantization threshold which can be 0 (sign operator) or the mean value of the intermediate biohash vector $\mathbf{z}$, depending on the system design.

After enrollment, biometric hashes are stored in a database or in a smart card.

B. Authentication Stage

At this stage, a claimer sends his biometric features $\tilde{\mathbf{x}}$ and secret key to the system. The system computes the claimer's test biometric hash vector by using the same procedures in the enrollment phase. The user is authenticated when the Hamming distance between $\mathbf{b}_{enroll}$ (which denotes the biohash of the user generated at the enrollment stage) and $\mathbf{b}_{auth}$ (which denotes the biohash of the user generated at the authentication stage) is below a pre-determined distance threshold ϵ as follows:

$$\sum_{k=1}^{n} \mathbf{b}_{enroll}(k) \oplus \mathbf{b}_{auth}(k) \leq \epsilon \tag{3}$$

where $\oplus$ denotes the binary XOR (exclusive OR) operator.

III. Entropy Prediction for Biohashing

The entropy of a random variable measures it uncertainty. In other words, it is a measure of the average amount of information required to describe a random variable. An important theoretical measure for biometric template protection methods is the entropy loss or mutual information (defined as the difference between unconditional and conditional entropies) [21]:

$$I(B;K) = H(B) - H(B|K), \tag{4}$$

where $H(B)$ is the entropy of biohash B and $H(B|K)$ is the conditional entropy of B where the corresponding secret key K is known (i.e., stolen by an adversary). In [6], the entropy of a biometric template is defined as the measure of the number of different identities that are distinguishable by a biometric system and it is a powerful indicator of its unpredictability. However, theoretical estimation methods are required to assess

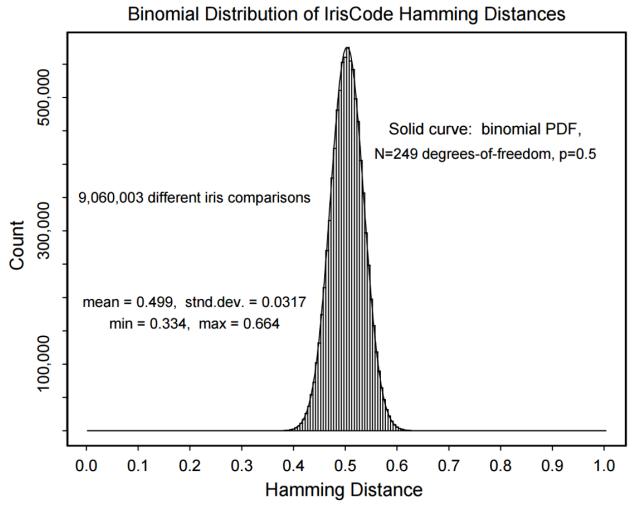

Fig. 1. Distribution of Hamming distances of interclass comparisons for iris phase codes [14]

the entropy of a biohash since how to calculate that entropy is not immediately clear. One approach is to compute the bit-wise entropy of a biohash where the entropy of each bit location is calculated using a large database of biohashes [22]. Since this approach assumes that the bits of a biohash are independent and identically distributed, the predicted entropy is overestimated.

A. Daugman's Entropy Estimation

Daugman proposed a method for estimating the entropy of iris phase codes [14]. Iris phase codes, bit strings of length 2048, are compared using the normalized Hamming distance and the ratio of the number of disagreeing bits to the number of total bits are used to assess the degree of dissimilarity between two bit strings. A low dissimilarity ratio between two iris codes are accepted as belonging to the same eye whereas as from different eyes if it is close to 0.5.

Comparing bits corresponds to a Bernoulli trial and a binomial distribution is the distribution of the sum of n Bernoulli trials, each with the same probability. By observing the interclass distance distribution over a large iris database, Daugman concluded that the distribution of the normalized Hamming distances between iris codes are normalized binomial with an observed mean of 0.499. Correlated Bernoulli trials reduce the effective number of trials but the output is still binomially distributed [23]. In iris phase codes, only a small number of bits are mutually independent, therefore the effective number of bits is not 2048 (number of bits in a phase code) but 249 and this corresponds to the entropy of an iris phase code [14]. In Fig. 1, the observed distribution is plotted against the theoretical binomial (solid curve), which shows the close fit between them.

B. Entropy of Biometric Hashing

Biohashes are bit strings as iris codes and are compared via Hamming distance during authentication. In this work, we utilize these similarities between biohashes and iris codes. We use the same methodology of fitting a binomial distribution to imposter distance data and to calculate the entropy of biohashes via the degree of freedom in the corresponding binomial distribution. A binomial distribution is fit to the obtained inter-class distances (i.e., imposter comparisons) as follows. Using the imposter comparisons between biohashes of different subjects, the observed mean of the normalized Hamming distances (μ_d) and observed standard deviation (σ_d) are calculated from data. This corresponds to a binomial distribution with $N_b = \mu_d(1-\mu_d)/\sigma_d^2$. The theoretical binomial distribution has the functional form:

$$f(m) = \frac{N_b!}{m!(N_b-m)!}\mu_d^m(1-\mu_d)^{(N-m)}, \qquad (5)$$

where m/N_b ($m = 1, \ldots, N_b$) is the outcome fraction of N_b Bernoulli trials, for our case, it is the Hamming distance for imposter matches. The number N_b (degree of freedom) of the binomial distribution is the predicted entropy of biohashes.

IV. Experiments and Results

We implement the entropy estimation method described on a face verification set-up considering two different threat scenarios. The naive threat model assumes that an adversary has very limited information about the system and he can only perform a brute force attack using an arbitrary face information and a random secret key. In the advanced threat model, essential details of the algorithms, properties of biometric data as well as the secret keys of users are assumed to be known by the attacker. So, the attacker can create biohashes using any face image and the secret key of the user that he tries to impersonate.

A. Experimental Setup and Database

In our experiments, we use the BioSecure-ds2 [24] face database. It consists of 210 users, equally balanced by gender. 8 standard camera acquisitions per person (captured in two separate sessions) are used in our experiments. PCA coefficients extracted from detected face images are used for matching. The faces are automatically detected using Viola-Jones face detector [25] and resized to 64×64 pixels. In order to normalize a gray-scale face image, its mean intensity value is extracted from each pixel and each pixel is divided by its standard deviation.

1024-dimensional PCA coefficients are calculated for all 8 samples of 210 subjects (a total of 1680 (210×8) face images). PCA training is done using the first session images only. Applying the standard biohashing procedure, a bit-string is created through inner product between the pseudo-random number and 1024-dimensional PCA coefficients and quantization of the resulting vector using a predefined threshold. One can obtain a bit-string of any length according to the memory and security requirements of the system. In order to demonstrate that the accuracy of the entropy analysis does not depend on biohash length, we experiment with three test lengths, namely 128, 256 and 512.

TABLE I
MEAN VALUE, STANDARD DEVIATIONS, AND DEGREES OF FREEDOM FOR DIFFERENT BIT LENGTHS UNDER BOTH SCENARIOS

	Bit Length	Mean (μ_d)	Standard Deviation (σ_d)	Degree of Freedom (N_b)
Naive Model	128	0.5000	0.0443	127
	256	0.4997	0.0313	254
	512	0.5001	0.0223	504
Advanced Threat Model	128	0.3653	0.0862	31
	256	0.3685	0.0792	37
	512	0.3836	0.0761	40

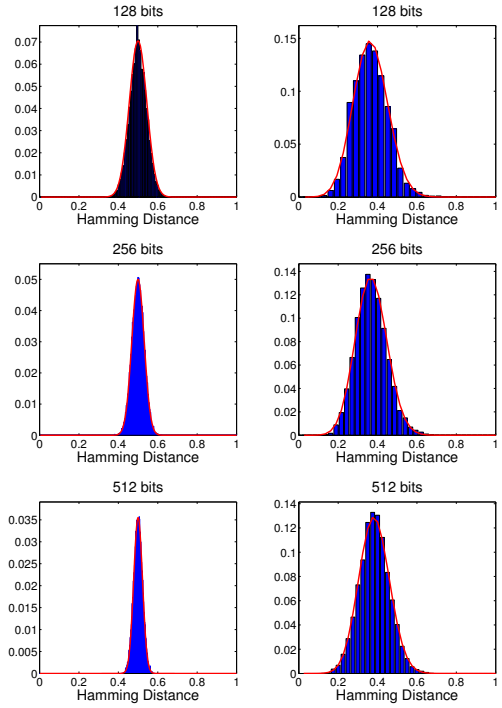

Fig. 2. Distribution of Hamming distances of interclass comparisons of biohashes with various lengths and different threat models - first column: naive threat model and second column: advanced threat model

B. Entropy Prediction Under Naive Threat Model

In our verification setting, all possible combinations of matching genuine pairs are used and the first sample of each subject is chosen for imposter matches (5880 ($210 \times 8 \times 7/2$) genuine comparisons and 21945 ($210 \times 209/2$) imposter comparisons). For imposter comparisons, the observed mean Hamming distance with standard deviation and the degree of freedom of its corresponding binomial distribution for each test length are given in Table I.

The figures in the first column of Fig. 2 illustrate the distribution of imposter distances under the naive threat model for biohashes with three test lengths. The histogram of the interclass comparison distribution (shown in blue) forms a perfect binomial distribution with parameters $\mu_d = 0.5001$, $\sigma_d = 0.0223$, and $N_b = 504$ (for 512 bits) as shown by the solid red line. The small difference between the actual bit length and the predicted entropy is due to database artifacts and it is expected that as the number of imposter comparisons gets higher, the ratio estimated entropy in bits/bit length would reach 1.

C. Entropy Prediction Under Advanced Threat Model

In the advanced threat model, the adversary is assumed to have full knowledge of the system and the secret keys of all users. The same experimental set-up of the naive model is used in order to predict the entropy of biohashes. For a biohash of a valid system user, an imposter biohash is created using the secret key of that user and a biometric template of an arbitrary user. Thus, unlike the naive model, interclass distances are calculated between two biohashes that are created using the same secret key for different users. The graphs in the second column of Fig. 2 illustrate the distribution of imposter distances for biohashes with various lengths. The observed mean of the distribution deviates from 0.5 and gets closer to the observed mean of genuine comparisons as the imposter distances get smaller. Since the distribution of genuine results is not involved in the entropy estimation, it is not discussed here. Thus, the comparison of genuine templates is not presented here for brevity.

This effect is also evident in the results given in Table I. As compared to the naive model, the degree of freedom is much lower than the actual bit length and the predicted entropy decreases dramatically for all biohash lengths. For example, the entropy drops from 504 to 40 for biohashes of length 512. We argue that our results in naive and advanced scenarios are generalizable when the database is large and representative enough. For all biohash lengths, the estimated entropy in this threat model is between 31 and 40 bits which is consistent with the face entropy of 40 bits reported in [15].

V. CONCLUSION

Existing theoretical evaluations of biometric protection methods cannot be used for assessing biohashing methods. In this work, we have described a systematic approach to quantify the unpredictability of random projection-based biohashing scheme by using entropy as a measure. Since feature extraction and feature normalization methods are not in our scope, we have focused only on quantitative evaluation of random projection and quantization steps. We have estimated the entropy of a biohash in terms of bits via the degree of freedom of binomial distribution under two predefined threat

models [10]. Our experiments in a face verification setup have demonstrated that the entropy of a biohash is almost equal to its bit-length as expected when there is no attack against the system (the naive threat model). On the other hand, the entropy and hence the unpredictability of biohashes decrease when the attacker knows the secret key of the user that he tries to impersonate (the advanced threat model). Thus, the amount of information kept secret in a biohash becomes more likely to be predicted in such cases.

Potential future research directions on entropy of biohashes can be summarized as follows. Novel random projection methods should be studied in order to decrease the entropy loss between the naive and advanced threat models. In addition, other applicable privacy and security metrics could be investigated, such as the mutual information of hashes of different users (i.e., the entropy of one hash conditional to another hash). One other possible research direction would be to study the suitability of universal entropy estimators (e.g., Coron's or Maurer's [26] or Kraskov's [27]) to biohashes.

ACKNOWLEDGMENT

This work has been performed by the BEAT project 7^{th} Framework Research Programme of the European Union (EU), grant agreement number: 284989. The authors would like to thank the EU for the financial support and the partners within the consortium for a fruitful collaboration. For more information about the BEAT consortium please visit http://www.beat-eu.org.

REFERENCES

[1] T. Ignatenko and F. M. J. Willems, "Information leakage in fuzzy commitment schemes." *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 2, pp. 337–348, 2010.

[2] S. Prabhakar, S. Pankanti, and A. K. Jain, "Biometric recognition: Security and privacy concerns," *IEEE Security & Privacy*, vol. 1, no. 2, pp. 33–42, 2003.

[3] N. K. Ratha, J. H. Connell, and R. M. Bolle, "An analysis of minutiae matching strength," in *Proceedings of the Third International Conference on Audio- and Video-Based Biometric Person Authentication*. London, UK: Springer-Verlag, 2001, pp. 223–228.

[4] A. Juels and M. Wattenberg, "A fuzzy commitment scheme," in *Proceedings of the 6th ACM Conference on Computer and Communications Security*, ser. CCS '99. New York, NY, USA: ACM, 1999, pp. 28–36.

[5] D. N. C. Ling, A. T. B. Jin, and A. Goh, "Biometric hash: high-confidence face recognition." *IEEE Transactions on Circuits Systems for Video Technology*, vol. 16, no. 6, pp. 771–775, 2006.

[6] A. K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," *EURASIP Journal on Advances in Signal Processing*, vol. 2008, pp. 113:1–113:17, Jan. 2008.

[7] U. Uludag, S. Pankanti, and A. K. Jain, "Fuzzy vault for fingerprints," in *Audio- and Video-Based Biometric Person Authentication*, ser. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2005, vol. 3546, pp. 310–319.

[8] B. Yang, C. Busch, P. Bours, and D. Gafurov, "Robust minutiae hash for fingerprint template protection." in *Media Forensics and Security*, ser. SPIE Proceedings, vol. 7541. SPIE, 2010, p. 75410.

[9] K. Kummel, C. Vielhauer, T. Scheidat, D. Franke, and J. Dittmann, "Handwriting biometric hash attack: A genetic algorithm with user interaction for raw data reconstruction." in *Communications and Multimedia Security*, ser. Lecture Notes in Computer Science, vol. 6109. Springer, 2010, pp. 178–190.

[10] X. Zhou, "Privacy and security assessment of biometric template protection," *IT - Information Technology*, vol. 54, no. 4, pp. 197–200, 2012.

[11] Y. C. Feng, M. Lim, and P. C. Yuen, "Masquerade attack on transform-based binary-template protection based on perceptron learning," *Pattern Recognition*, vol. 47, no. 9, pp. 3019–3033, 2014.

[12] A. Nagar, K. Nandakumar, and A. K. Jain, "Biometric template transformation: a security analysis," in *Media Forensics and Security*, 2010, p. 75410.

[13] P. Boufounos and S. Rane, "Secure binary embeddings for privacy preserving nearest neighbors," in *Proceedings of the IEEE Workshop on Information Forensics and Security (WIFS)*, 2011, pp. 1–6.

[14] J. Daugman, "The importance of being random: statistical principles of iris recognition." *Pattern Recognition*, vol. 36, no. 2, pp. 279–291, 2003.

[15] A. Adler, R. Youmaran, and S. Loyka, "Towards a measure of biometric information," in *Proceedings of the Canadian Conference on Electrical and Computer Engineering*, May 2006, pp. 210–213.

[16] Z. Bai and D. Hatzinakos, "LBP-based biometric hashing scheme for human authentication," in *Proceedings of the 11th International Conference on Control Automation Robotics Vision*, Dec. 2010, pp. 1842 –1847.

[17] C. Karabat and H. Erdogan, "A cancelable biometric hashing for secure biometric verification system," in *Proceedings of the Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, 2009, pp. 1082–1085.

[18] R. Lumini and L. Nanni, "An improved biohashing for human authentication," *Pattern Recognition*, vol. 40, pp. 1057–1065, 2006.

[19] C. Rathgeb and A. Uhl, "Iris-biometric hash generation for biometric database indexing," in *Proceedings of the 20th International Conference on Pattern Recognition*, 2010, pp. 2848–2851.

[20] Y. Wai Kuan, A. B. Teoh, and D. C. Ngo, "Secure hashing of dynamic hand signatures using wavelet-fourier compression with biophasor mixing and 2N discretization," *EURASIP Journal on Advances in Signal Processing*, vol. 2007, no. 1, pp. 32–32, 2007.

[21] J. D. Golic and M. Baltatu, "Entropy analysis and new constructions of biometric key generation systems." *IEEE Transactions on Information Theory*, vol. 54, no. 5, pp. 2026–2040, 2008.

[22] C. Karabat and B. Topcu, "How to assess privacy preservation capability of biohashing methods?: Privacy metrics," in *Proceedings of the IEEE 22nd Signal Processing and Communications Applications Conference*, April 2014, pp. 2217–2220.

[23] R. Viveros, K. Balasubramanian, and N. Balakrishnan, "Binomial and negative binomial analogues under correlated Bernoulli trials," *The American Statistician*, vol. 48, no. 3, pp. 243–247, 1994.

[24] J. Ortega-Garcia, J. Fierrez, F. Alonso-Fernandez, J. Galbally, M. Freire, J. Gonzalez-Rodriguez, C. Garcia-Mateo, J.-L. Alba-Castro, E. Gonzalez-Agulla, E. Otero-Muras, S. Garcia-Salicetti, L. Allano, B. Ly-Van, B. Dorizzi, J. Kittler, T. Bourlai, N. Poh, F. Deravi, M. Ng, M. Fairhurst, J. Hennebert, A. Humm, M. Tistarelli, L. Brodo, J. Richiardi, A. Drygajlo, H. Ganster, F. Sukno, S.-K. Pavani, A. Frangi, L. Akarun, and A. Savran, "The multiscenario multi-environment biosecure multimodal database (BMDB)," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 32, no. 6, pp. 1097–1111, June 2010.

[25] P. Viola and M. J. Jones, "Robust real-time face detection," *International Journal on Computer Vision*, vol. 57, no. 2, pp. 137–154, May 2004.

[26] J.-S. Coron and D. Naccache, "An accurate evaluation of Maurer's universal test," in *Selected Areas in Cryptography*, ser. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 1999, vol. 1556, pp. 57–71.

[27] A. Kraskov, H. Stögbauer, and P. Grassberger, "Estimating mutual information." *Physical Review. E, Statistical, Nonlinear, and Soft Matter Physics*, vol. 69, no. 6 Pt 2, Jun. 2004.