IRIS TEMPLATE PROTECTION USING A DIGITAL MODULATION PARADIGM

Emanuele Maiorana, Patrizio Campisi, Alessandro Neri

Section of Applied Electronics, Department of Engineering, University Roma Tre,
Via Vito Volterra 62, 00146 Roma, Italy

emanuele.maiorana@uniroma3.it, patrizio.campisi@uniroma3.it, alessandro.neri@uniroma3.it

ABSTRACT

Template protection is an issue of paramount importance in the design of biometric recognition systems. In this paper we present a biometric cryptosystem applied to iris biometrics, where template security is guaranteed by means of a framework inspired by the digital modulation paradigm. Specifically, the properties of modulation constellations and turbo codes with soft-decoding are exploited to design a system with high performance in terms of both verification rates and security, even while dealing with a biometrics characterized by a high intra-class variability such as the iris. The effectiveness of the proposed approach is evaluated by performing tests on the Interval subset of the CASIA-IrisV4 database.

Index Terms— iris recognition, biometric template protection, digital modulation, turbo codes

1. INTRODUCTION

In the design of a biometric recognition system, special attention needs to be paid towards the potential security and privacy issues which may arise from the use of the biometric data. In fact biometrics, being limited in number, can be hardly replaced if stolen or copied. Biometric data can also reveal significant information regarding people personality and health, or they can be employed to perform an unauthorized tracking of the enrolled subjects across multiple databases, thus affecting the users' privacy [1].

Many efforts have been therefore devoted to the design of template protection schemes able to properly address the aforementioned concerns [2], [3]. According to the classification in [4], such schemes can be classified into biometric cryptosystems and feature transformation approaches. The former can be further divided into key binding methods, which combine biometric templates with binary keys, or key generation approaches, where cryptographic keys are directly created from biometric data. Feature transformation methods can be classified into salting approaches, whose security relies on the secure storage of an invertible function key, and non-invertible transform methods which apply one-way transformations to the considered biometrics. An ideal template protection scheme should make impossible recovering the original template from the stored one. Moreover, it should be able to generate multiple versions of the same biometrics without leaving the possibility of linking one to the others. Also, it should be able to guarantee a recognition accuracy comparable to an unprotected system [5].

The present paper proposes a biometric cryptosystem designed for protecting iris templates through a general framework inspired by the digital modulation paradigm, introduced by the authors in [6]. Our scheme allows to overcome several limitations of the iris cryptosystems so far proposed, being able to guarantee high performance in terms of both verification rates and security. The paper is organized as follows. The state of the art on iris template protection is reviewed in Section 2, while the proposed iris cryptosystem is described in Section 3, where also the performed security analysis is detailed. The experimental tests performed for evaluating the effectiveness of the proposed scheme are presented in Section 4, and conclusions are eventually given in Section 5.

2. IRIS TEMPLATE PROTECTION

Iris is one of the most investigated and employed biometrics for automatic people recognition, mainly due to the high recognition accuracy it can provide, and to the ease with which it can be acquired [7]. Several iris template protection schemes have been therefore recently proposed [8]. Salting approaches have been for instance presented in [9], where subject-specific transforms are employed to generate cancelable biometrics, as well as in [10], where products between the original templates and secret user-dependent random vectors are exploited for providing security. Several non-invertible transforms applicable to both the image and the feature domain have been proposed in [11], while a non-invertible transform approach based on block re-mapping and image warping has been described in [12]. However, it is in general difficult to quantitatively evaluate the security of the approaches relying on non-invertible transformations. A proper detailed analysis is provided only in few papers, as in [13] where the use of adaptive Bloom filters is proposed for iris template protection, or in [14], where correlation attacks are considered. It is also worth pointing out that the integration of feature transformation methods into cryptographic frameworks may not be straightforward, which is why cryptosystems approaches have typically received a wider attention, and their security has been evaluated in more details. Specifically, the fuzzy commitment (FC) framework [15] has been adopted in [16] and [17], where a combination of Reed-Solomon and Hadamard codes is employed to manage both the background and burst errors which can be encountered when comparing two binary iris codes. The product of two Reed-Muller codes is employed in [18], while a shuffling scheme together with a decoding performed on

978-1-4799-2893-4/14/$31.00 ©2014 IEEE

separated chunks is proposed in [19]. As can be seen, such approaches rely on the use of multiple codes, or exploit specific characteristics of the binary iris template, for providing the error correction capability (ECC) required for dealing with the intra-class variability of the considered biometrics. Unfortunately, in [20] and [21] it has been shown that using combinations of codes may leave the system vulnerable to statistical attacks able to break its security by exploiting the histograms of the stored data. Moreover, in [22] it is observed that a random permutation process shall be applied to the templates to be protected before binding them with codewords, in order to prevent possible decodability attacks affecting users' privacy. Such random permutation alters the patterns of statistic properties of the considered biometrics, thus making it unfeasible to design a code on their basis as in [16]. The storage of user-specific information about the most stable features of a biometric template [23] for reducing the intra-class variability of the employed data should also be avoided, because such additional helper data could expose discriminative information which can aid an attacker in tracking a user across different databases [24]. As detailed in Section 3, in the proposed approach the intra-class variability of iris biometrics is managed without exploiting any specific property of the iris templates or combinations of codes.

3. PROPOSED IRIS CRYPTOSYSTEM

The proposed iris cryptosystem, inspired by the digital *modulation - channel coding - transmission - channel decoding - demodulation* chain of digital data transmission over a noisy channel [25], is depicted in Figure 1. As described in [6], the employed framework represents a generalization of the code-offset approach [26], of which the FC [15] is the most widely known implementation. Specifically, as in a digital communication scenario, a random message $\mathbf{b}$ with k bits is first generated, and then encoded into an n-bit string to provide resilience against the errors which may affect the transmitted data. Turbo codes may be employed for such task, due to their capability of approaching the theoretical maximum code rate for a given noise level [27]. It is worth remarking that a high code rate k/n is of primary importance for a biometric cryptosystem, being its security against brute-force attacks dependent on the length k of the binary key $\mathbf{b}$ [4]. The encoded string is then modulated into s symbols of a constellation with L points, being $s = \frac{n}{\log_2 L}$, thus generating a codeword $\mathbf{c}$ represented through s complex symbols, $\mathbf{c} \in C \subset \mathbb{C}^s$, with C representing the considered code. The channel through which the message is sent is represented by the binding operation $\mathbf{v} = f(\mathbf{x}, \mathbf{c}) \in \mathbb{C}^s$, which combines the considered codeword with the biometric template $\mathbf{x}$. The operator f has to be defined in accordance with the employed constellation and in such a way that a function g, which allows performing $\mathbf{c} = g(\mathbf{x}, \mathbf{v})$, exists. The potentially corrupted codeword $\tilde{\mathbf{c}} = g(\tilde{\mathbf{x}}, \mathbf{v}) \in \mathbb{C}^s$ is generated through this latter operator, depending on a fresh biometrics $\tilde{\mathbf{x}}$ acquired during recognition. A joint demodulation and decoding process can be then applied to $\tilde{\mathbf{c}}$ to obtain $\tilde{\mathbf{b}}$. The hashed versions of $\mathbf{b}$ and $\tilde{\mathbf{b}}$ are then compared to determine the outcome of the verification process. With respect to the FC approach, the employed framework offers a wider choice for selecting the function binding the biometrics $\mathbf{x}$ with the message $\mathbf{b}$. The domains of $\mathbf{x}$ and $\mathbf{c}$ may also not be the same, thus resulting in more flexibility when determining the system operating conditions. Moreover, it permits to exploit soft-decoding to improve the recognition performance of the considered protected schemes. The following sections describe in detail each step of the proposed cryptosystem.

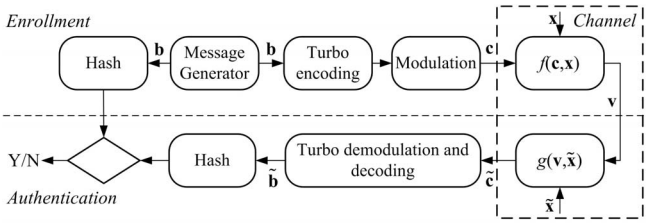

Fig. 1. Proposed iris cryptosystem.

3.1. Iris Template Extraction

Iris biometrics is processed according to the classic approach described in [28]. Specifically, iris segmentation is first performed to extract the iris information from the original eye image. A normalization process is then required to obtain a rectangular iris representation with fixed dimensions $I \times J$ indicated as *rubber sheet*, where I provides the angular resolution, while J represents the radial resolution. The normalized iris texture is then processed by means of Gabor filters, and an image $G[i, j]$, with $i = 1, \ldots, I$, $j = 1, \ldots, J$, is then obtained by retaining only the phase information of the filtered complex image, while discarding the amplitude component. In more details, the code made available in [29] is employed to segment, normalize, and filter the irises thus generating phase images $G[i, j]$ with resolution $I \times J = 240 \times 20$.

In order to partially reduce the intra-class variability of the employed templates, a user-independent mask is then estimated. Such approach is justified by the consideration that the regions of an iris code are not equally useful [30]. Having indicated with $\mathcal{U}$ a training database employed for estimating such mask, and with $G_l^{(u)}[i, j]$ the phase image originated from the l-th iris image acquired from a user $u \in \mathcal{U}$, the proposed user independent mask $D[i, j]$ is computed as:

$$D[i, j] = \sum_{u,l,h} \min_t \left\{ G_l^{(u)}[i, j] - G_h^{(u)}[i - t, j] \right\}. \quad (1)$$

Basically, (1) compares any possible couple of phase templates belonging to the same user u, retaining only the difference resulting from the best match obtained by shifting the test template with respect to the reference one. It thus computes a map of the pixels providing the lowest distances for all the users in U. An example of $D[i, j]$, computed over $|\mathcal{U}| = 66$ classes of right irises taken from the Interval subset of the CASIA-IrisV4 database [31], is given in Figure 2. As it can be seen, the areas where the greatest difference between the templates belonging to the same person occur, represented

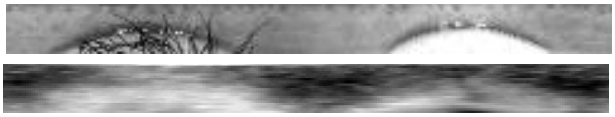

Fig. 2. Examples of a *rubber sheet* containing occlusions (above), and of the user independent mask $D[i,j]$ (below).

with brighter pixels, are those where it is more common to encounter occlusions due to eyelids, and should therefore be discarded. The desired iris template to be protected $\mathbf{x}$ is then obtained for each user by selecting from $G[i,j]$ only the s positions having the lowest values in $D[i,j]$.

It is worth pointing out that, during the recognition phase, several attempts of recovering the original message $\mathbf{b}$ have to be performed, each time applying a cyclic scrolling to the acquired template $\tilde{G}[i,j]$ before selecting the best positions according to $D[i,j]$, for generating $\tilde{\mathbf{x}}$.

3.2. Channel Modeling: Binding Operators

As already described, in the considered digital modulation paradigm the channel is composed by the operations performed by the binding function f and by its inverse g, which have to be selected according to the employed constellation. In the proposed implementation we resort to a PSK modulation, where a codeword $\mathbf{c}$ can be represented through s symbols, each belonging to a set of L points lying on the unit circle in the complex domain. By its definition, the considered biometric template $\mathbf{x}$ is given by a set of coefficients each lying in the $[-\pi,\pi)$ interval. Such interval can be (circularly) uniformly decomposed into D parts, according to the set of values $\mathcal{D}=\{\frac{\pi}{D}+\frac{2\pi}{D}d\}$, with $d=\left[-\frac{D}{2},-\frac{D}{2}+1,\ldots,\frac{D}{2}-1\right]$. A vector $\boldsymbol{\varphi}$ is then generated by mapping each phase coefficient in $\mathbf{x}$ to the closest value in $\mathcal{D}$. The binding operators can be therefore defined as

$$\mathbf{v}=f(\mathbf{x},\mathbf{c})=\mathbf{c}\cdot e^{i\boldsymbol{\varphi}};\;\; \tilde{\mathbf{c}}=g(\mathbf{v},\tilde{\mathbf{x}})=\mathbf{v}\cdot e^{-i\tilde{\boldsymbol{\varphi}}}, \quad (2)$$

where $\boldsymbol{\varphi}$ is obtained from $\mathbf{x}$ during the enrollment stage, and $\tilde{\boldsymbol{\varphi}}$ from $\tilde{\mathbf{x}}$ in the authentication stage. The binding therefore generates an offset $\mathbf{v}$ whose elements do not lie on the original constellation points yet remaining on the unitary complex circle, while the reconstruction operator tries to revert such displacement. In order to not reduce the number of possible constellation points from which each symbol in the offset $\mathbf{v}$ maight have been originated, D has to be greater than L, with $D=L\cdot 2^l$ in the proposed implementation, where $l\in\mathbb{N}_0$ being $\mathbb{N}_0$ the set of non-negative integers. The proposed quantization is performed for allowing a proper analysis of the system security in Section 3.3, and for evaluating the increase in ECC due to the use of soft-decoding in turbo decoders [27] in Section 4. It is in fact worth pointing out that the use of turbo codes has been already suggested within the framework of FC in [32] and [33], yet in both cases they have been employed in hard decoding modality. The digital modulation paradigm here employed allows performing soft decoding through a joint demodulation and decoding process [27], thus increasing the ECC of the considered turbo codes and improving the achievable recognition performance.

3.3. Security analysis

As mentioned in Section 2, the security of biometric cryptosystems has been analyzed with a greater detail than that dedicated to feature transformation methods. For instance, a deep analysis on the security and privacy leakage of FC is given in [32]. Consistently to such approach, the security of the proposed framework could not be expressed only by the entropy $H(\mathbf{b})=k$, representing the effort required by a brute-force attack for breaking the system. Conversely, the conditional entropy $H(\mathbf{b}|\mathbf{v})$, giving the uncertainty about the message $\mathbf{b}$ once the helper data $\mathbf{v}$ has been made publicly available, has to be taken into account for assessing the system security against statistical attacks which could exploit the knowledge of the employed biometric characteristics. Also the conditional entropy $H(\mathbf{x}|\mathbf{v})$, or its equivalent $H(\boldsymbol{\varphi}|\mathbf{v})$ for our scheme, should be estimated for evaluating the privacy of the proposed system [34], [35]. As remarked in [36], such analysis is often omitted due to the difficulty in properly estimating the required entropies in practical scenarios.

Nonetheless, it can be observed that, in the employed framework, $H(\mathbf{b}|\mathbf{v})=H(\boldsymbol{\varphi}|\mathbf{v})$, due to the fact that once $\mathbf{v}$ is known, the knowledge of $\boldsymbol{\varphi}$ provides $\mathbf{b}$, as well as knowing $\mathbf{b}$ reveals also the biometric information $\boldsymbol{\varphi}$. Moreover, $\mathbf{b}$ can be retrieved once k bits out of n of its encoded version are known [34], which is equivalent to knowing any $z=\frac{k}{\log_2 L}$ coefficients of $\boldsymbol{\varphi}$, given (2). The security of the considered system can be therefore evaluated by observing that $H(\mathbf{b}|\mathbf{v})=\min_{Z\in\mathcal{Z}}\{H(\boldsymbol{\varphi}^Z|\mathbf{v})\}$, being $\boldsymbol{\varphi}^Z$ a string generated from $\boldsymbol{\varphi}$ by selecting only z coefficients out of the available s ones, with $\mathcal{Z}$ being the ensemble of all possible sets Z of z coefficients, $Z\subset\{1,\ldots,s\}$. As in [6], it is therefore possible to practically compute $H(\boldsymbol{\varphi}^Z|\mathbf{v})$ over real data by resorting to an approximation based on second-order dependency trees [37], which assumes that the probability $P(\boldsymbol{\varphi}^Z)$ can be expressed as:

$$\hat{P}(\boldsymbol{\varphi}^Z)=\prod_{i=1}^{z}P(\varphi^Z_{u_i}|\varphi^Z_{t(u_i)}),\; 1\le t(u_i)<u_i, \quad (3)$$

where $\mathbf{u}=\{u_i\}$, $1\le i\le z$, is a permutation of the indexes $[1,2,\ldots,z]$, $t(u_1)=u_1$, and $P(\varphi^Z_{u_1}|\varphi^Z_{t(u_1)})=P(\varphi^Z_{u_1})$. Given the assumption in (3), the conditional entropy $H(\mathbf{b}|\mathbf{v})$ can be therefore approximated as

$$\hat{H}(\mathbf{b}|\mathbf{v})=\min_{Z\in\mathcal{Z}}\left\{\min_{\{\mathbf{u}\}}\sum_{i=1}^{z}\left\{H(\varphi^Z_{u_i},\varphi^Z_{t(u_i)}|\mathbf{v})-H(\varphi^Z_{t(u_i)}|\mathbf{v})\right\}\right\}, \quad (4)$$

and can be practically computed as in [6], through the application of a minimum spanning algorithm for directed trees [38]. The results of the performed analysis, reported in Section 4, therefore describe the actual security of the proposed iris cryptosystem against statistical attacks in a practical implementation, with respect to the selection of the system parameters L and D.

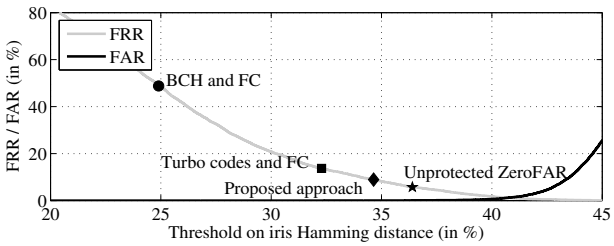

Fig. 3. Recognition in unprotected and protected systems

4. EXPERIMENTAL RESULTS

The proposed iris cryptosystem is tested over the Iris-Interval subset of the CASIA-IrisV4 database [31], containing right and left irises of 249 subjects, for a total of 395 classes. As described in Section 3.1, 66 classes are employed to estimate the user-independent mask $D[i,j]$, while the remaining 329 classes are employed for performance evaluation. More in detail, in our experiments we consider 2002 irises out of the available 2251 ones: the images which the module in [29] fails to properly segment are excluded, in order to prevent the estimated performance being dependent on the employed implementation of the segmentation module. The False Recognition Rate (FRR) is therefore evaluated over 13490 comparisons among irises belonging to the same class, and the False Acceptance Rate (FAR) is estimated over 25100 comparisons among irises of different classes.

Figure 3 reports the performance of a standard unprotected system based on [28], where iris templates are obtained by binarizing each phase value in $G[i,j]$ with two bits according to its corresponding quadrant, thus generating templates with $2{*}I{*}J$ bits. User-dependent masks are employed for discarding the regions where eyelids, eyelashes, specular reflections or other artifacts are encountered. The Equal Error Rate (EER) is at 1.31%. In order to verify the effectiveness of the proposed scheme, the behavior of a protected system based on this binary representation, and using the FC to provide the desired security, is first reported in Table 1. Specifically, the user-independent mask $D[i,j]$ is applied to the computed phase images $G[i,j]$ for selecting $s = 2048$ coefficients, each of which is binarized with 2 bits as in an unprotected system. The binary templates are then bind with either BCH or Turbo codes, for comparing the performance achievable by exploiting the ECC of both coding schemes. As can be seen, BCH codes do not provide enough ECC to manage the intra-class variability of the considered iris templates, thus resulting in high FRR and low security, with regard to both brute-force and statistical attacks. Unacceptable results, with FRR above 40%, are also obtained when using the coding scheme in [16] with Hadamard/Reed-Solomon codes, if a random permutation process is applied to the binary iris templates to prevent decodability attacks [22], thus enlightening the significative dependence of such coding scheme on typical iris error patterns. It is also worth remarking that the employed iris data are characterized by an intra-class variability much greater than those employed in [16], where the mean intra-class Hamming distance between templates belonging to the same iris is equal to 0.127 with a standard deviation equal to 0.058, with respect to values for the the same measures equal to 0.251 and 0.058 for the dataset here considered.

BCH codes				Turbo Codes			
FRR	FAR	$H(\mathbf{b})$	$\hat{H}(\mathbf{b}\|\mathbf{v})$	FRR	FAR	$H(\mathbf{b})$	$\hat{H}(\mathbf{b}\|\mathbf{v})$
48.8	0.0	13	5.7	13.7	0.0	268	117.7
53.7	0.0	31	13.9	13.8	0.0	310	140.4
60.4	0.0	47	20.7	13.9	0.0	368	163.5
71.3	0.0	71	31.2	14.3	0.0	450	200.4

Table 1. Verification (in %) and security (in bits) performance for a FC approach with BCH or turbo codes, with $s = 2048$.

It can be observed that the performance reported in Table 1 for turbo codes can be considered as a particular case, with $L = D = 4$, of the protection framework here proposed. The capability of the proposed approach in improving the recognition accuracy, thanks to the higher ECC allowed by the use of modulation constellation and soft-decoding in turbo codes, is shown in Table 2. Both a Binary PSK (BPSK) and Quaternary PSK (QPSK) constellations, respectively with $L = 2$ and $L = 4$, are considered for different values od D. From the reported results it is therefore possible to observe that the proposed iris cryptosystem is able to reach significative verification performance while guaranteeing proper security even when dealing with iris data characterized by a high intra-class variability. In order to show the improvement in recognition accuracy available with the proposed approach, the best FRR achievable at ZeroFAR for protected systems using BCH and turbo codes in a FC scheme, and turbo codes according to the proposed framework, are reported in Figure 3, superimposed on the FRR of the unprotected system.

5. CONCLUSIONS

An iris cryptosystem inspired by the digital modulation paradigm has been presented in this paper. Thanks to the properties of modulation constellations and turbo codes soft-decoding, acceptable recognition rates can be reached even dealing when data with significant intra-class variability, while guaranteeing proper security against both brute-force and statistical attacks.

rate	D	$L=2$				$L=4$			
k/n		FRR	FAR	$H(\mathbf{b})$	$\hat{H}(\mathbf{b}\|\mathbf{v})$	FRR	FAR	$H(\mathbf{b})$	$\hat{H}(\mathbf{b}\|\mathbf{v})$
1/15	2	13.4	0.01	132	67.4	-	-	268	-
	4	4.84	0.05		18.6	13.6	0.00		117.7
	8	3.00	0.26		11.6	**8.92**	**0.00**		46.7
1/13	2	17.9	0.01	152	81.4	-	-	310	-
	4	6.61	0.03		21.7	18.2	0.00		140.4
	8	4.12	0.20		13.2	11.4	0.00		53.1
1/11	2	21.8	0.00	180	89.7	-	-	368	-
	4	8.37	0.01		24.2	22.8	0.00		163.5
	8	5.24	0.13		14.4	13.9	0.00		60.2
1/9	2	29.7	0.00	222	104.3	-	-	450	-
	4	10.1	0.00		28.5	27.4	0.00		200.4
	8	6.36	0.07		16.6	16.4	0.00		73.5

Table 2. Verification (in %) and security (in bits) performance for the proposed cryptosystem, with $s = 2048$.

6. REFERENCES

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

[2] T. Kevenaar P. Tuyls, B. Skoric, Ed., *Security with Noisy Data Privacy Biometrics, Secure Key Storage and Anti-Counterfeiting*, SPRINGER, 2007.

[3] P. Campisi, Ed., *Security and Privacy in Biometrics*, SPRINGER, 2013.

[4] A.K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," *EURASIP Journal on Advances in Signal Processing, Special Issue on Biometrics*, 2008.

[5] P. Campisi, E. Maiorana, M. Gonzalez, and A. Neri, "Adaptive and distributed cryptography for signature biometrics protection," in *Proceedings of SPIE 6505*, 2007.

[6] E. Maiorana, D. Blasi, and P. Campisi, "Biometric template protection using turbo codes and modulation constellations," in *IEEE WIFS*, 2012.

[7] W. Dong, Z. Sun, and T. Tan, "A design of iris recognition system at a distance," in *IEEE CCPR*, 2009.

[8] P. Campisi, E. Maiorana, and A. Neri, "Iris template protection," in *Encyclopedia of Biometrics, Stan Z. Li editor, Springer*, 2009.

[9] O. Ouda, N. Tsumura, and T. Nakaguchi, "Tokenless cancelable biometrics scheme for protecting iris codes," in *IEEE ICPR*, 2010.

[10] S.C. Chong, A.T.B. Jin, and D.N.C. Ling., "High security iris verification system based on random secret integration," *Computer Vision and Image Understanding*, vol. 102, no. 2, pp. 169–177, 2006.

[11] J. Zuo, N.K. Ratha, and J.H. Connel, "Cancelable iris biometric," in *IEEE ICPR*, 2008.

[12] J. Haammerle-Uhl, E. Pschernig, and A. Uhl, "Cancelable iris biometrics using block re-mapping and image warping," in *ISC*, 2009.

[13] C. Rathgeb, F. Breitinger, and C. Busch, "Alignment-free cancelable iris biometric templates based on adaptive bloom filters," in *IEEE ICB*, 2013.

[14] O. Ouda, N. Tsumura, and T. Nakaguchi, "Securing bioencoded iriscodes against correlation attacks," in *IEEE ICC*, 2011.

[15] A. Juels and M. Wattenberg, "A fuzzy commitment scheme," in *ACM Conf. on Computer and Communication Security*, 1999.

[16] F. Hao, R. Anderson, and J. Daugman, "Combining crypto with biometrics effectively," *IEEE Transactions on Computers*, vol. 55, no. 9, pp. 1081–1088, 2006.

[17] C. Rathgeb and A. Uhl, "Systematic construction of iris-based fuzzy commitment schemes," in *IEEE ICB*, 2009.

[18] J. Bringer, H. Chabanne, G. Cohen, B. Kindarji, and G. Zemor, "Optimal iris fuzzy sketches," in *IEEE BTAS*, 2007.

[19] S. Kanade, D. Petrovska-Delacretaz, and B. Dorizzi, "Cancelable iris biometrics and using error correcting codes to reduce variability in biometric data," in *IEEE CVPR*, 2009.

[20] A. Stoianov, T. Kevenaar, and M. Van der Veen, "Security issues of biometric encryption," in *IEEE TIC-STH Symp. on Information Assurance, Biometric Security and Business Continuity*, 2009.

[21] C. Rathgeb and A. Uhl, "Statistical attack against iris-biometric fuzzy commitment schemes," in *IEEE CVPR*, 2011.

[22] E. J. C. Kelkboom, J. Breebaart, T. A. M. Kevenaar, I. Buhan, and R. N. J. Veldhuis, "Preventing the decodability attack based cross-matching in a fuzzy commitment scheme," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 1, pp. 107–121, 2011.

[23] E. Maiorana and P. Campisi, "Fuzzy commitment for function based signature template protection," *IEEE Signal Processing Letters*, vol. 17, no. 3, pp. 249–252, 2010.

[24] Q. Li, M. Guo, and E.-C. Chang, "Fuzzy extractors for asymmetric biometric representation," in *IEEE CVPR*, 2008.

[25] J. Proakis, *Digital communications*, McGraw Hill, 2001.

[26] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," in *EUROCRYPT*, 2004.

[27] C. Berrou and A. Glavieux, "Near optimum error correcting coding and decoding: Turbo-codes," *IEEE Transactions on Communications*, vol. 44, no. 10, pp. 1261–1271, Oct. 1996.

[28] J. Daugman, "How iris recognition works," *IEEE Trans. on Circuits and Systems for Video Technology*, vol. 14, no. 1, pp. 21–30, 2004.

[29] L. Masek and P. Kovesi, "Matlab source code for a biometric identification system based on iris patterns," School of Computer Science and Software Engineering, University of Western Australia, 2003.

[30] K. P. Hollingsworth, K. W. Bowyer, and P. J. Flynn, "The best bits in an iris code," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 31, no. 6, pp. 964–973, June 2009.

[31] Chinese Academy of Sciences (CASIA), "Casia-IrisV4 database," `http://www.cbsr.ia.ac.cn/china/IrisDatabasesCH.asp`.

[32] T. Ignatenko and F. Willems, "On information leakage in fuzzy commitment," in *SPIE Media Forensics and Security II*, 2010.

[33] K. Nandakumar, "A fingerprint cryptosystem based on minutiae phase spectrum," in *IEEE WIFS*, 2010.

[34] X. Zhou, A. Kuijper, R. Veldhuis, and C. Busch, "Quantifying privacy and security of biometric fuzzy commitment," in *IEEE IJCB*, 2011.

[35] L. Lai, S.W. Ho, and H. Vincent Poor, "Privacy-security trade-off in biometric security systems Part I: Single uses case," *IEEE TIFS*, vol. 6, no. 1, pp. 122–139, 2011.

[36] X. Zhou and C. Busch, "Measuring privacy and security of iris fuzzy commitment," in *IEEE ICCST*, 2012.

[37] C. Chow and C. Liu, "Approximating discrete probability distributions with dependence trees," *IEEE Transactions on Information Theory*, vol. 14, pp. 462–467, 1968.

[38] J. Edmonds, "Optimum branchings," *Journal of Research of the National Bureau of Standurds*, vol. 71, pp. 233–240, 1967.