Protecting Biometric Templates with Image Watermarking Techniques

Nikos Komninos and Tassos Dimitriou

Athens Information Technology,
GR-19002 Peania Attiki, Greece
{nkom, tdim}@ait.edu.gr

Abstract. Biometric templates are subject to modifications for identity fraud especially when they are stored in databases. In this paper, a new approach to protecting biometric templates with image watermarking techniques is proposed. The novelty of this approach is that we have combined lattice and block-wise image watermarking techniques to maintain image quality along with cryptographic techniques to embed fingerprint templates into facial images and vice-versa. Thus, protecting them from being modified.

Keywords: Biometric templates, fingerprints, face pictures, authentication, watermarking.

1 Introduction

Visual based biometric systems use feature extraction algorithms to extract the discriminant information that is invariant to as many variations embedded in the raw data (e.g. scaling, translation, rotation) as possible. Template-based methods crop a particular subimage (the template) from the original sensory image, and extract features from the template by applying global-level processing, without a priori knowledge of the object's structural properties. Compared to geometric feature extraction algorithms, image template approaches need to locate far fewer points to obtain a correct template. For example, in the probabilistic decision-based neural network (PDBNN) face recognition system, only two points (left and right eyes) need to be located to extract a facial recognition template. An early comparison between the two types of feature extraction methods was made by Brunelli and Poggio [1]. They found the template approach to be faster and able to generate more accurate recognition results than the geometric approach.

In practice, there is not always a perfect match between templates and individuals. One speaks of a false positive if the biometric recognition system says 'yes', but the answer should be 'no'. A false negative works the other way round: the system says 'no', where it should be a 'yes'. One of the main challenges with biometric systems is to minimise the rates of both false positives and of false negatives. In theory one is inclined to keep the false positives low, but in practical situations it often works the other way round: people that operate these systems dislike false negatives, because they slow down the process and result in extra work and people complaining.

A potential protection approach of biometric templates is feasible with image watermarking techniques in visual-based biometric systems. Watermarking techniques attempt to protect the copyrights of any digital medium by embedding a unique pattern or message within the original information. The embedding method involves the use of a number of different authentication, encryption and hash algorithms and protocols to achieve the validity and copy protection of the particular message.

One of the most important requirements of watermarking is the perceptual transparency between the original work and the watermarked. Especially for images that objective metrics are widely used [6]. The watermark message may have a higher or lower level of perceptibility, meaning that there is a greater or lesser likelihood that a given observer will perceive the difference.

In this paper, we apply watermarking techniques to biometric templates to overcome serious cases of identity theft. In particular, we embed a person's fingerprint template into his facial image with the form of a cryptographic encoder that utilizes encryption algorithms, hash functions and digital signatures. Once the facial image has been watermarked, it can be stored in public databases without risking an identity modification or fabrication.

Following this introduction, the paper is organized as follows. Section 2 presents current work that combine watermarking and biometrics techniques. Section 3 discusses the requirements for efficient watermarking and briefly describes lattice and block-wise embedding methods and how these can be used along with cryptographic techniques to protect biometric templates. Section 4 evaluates the performance and the efficiency of the two embedding methods, through simulation tests. Section 5 concludes with remarks and comments on the open issues in watermarking and biometric templates.

2 Related Work

Current research efforts in combining watermarking techniques and visual-based biometric systems follow a hierarchical approach, with the most explored area being that of biometrics. Watermarking techniques on the other hand have been explored less in conjunction with biometrics templates. Despite the fact that several attempts of combining watermarking techniques and biometric systems have already been proposed.

In Lucilla et al. [5], a technique for the authentication of ID cardholders is presented, which combines dynamic signature verification with hologram watermarks. Two biometric features are already integral parts of ID cards for *manual* verification: the user's face and signature. This technique embeds dynamic features of the cardholder's signature into the personal data printed on the ID card, thereby facilitating automated user authentication based on the embedded information. Any modification of the image can also be detected and will further disallow the biometric verification of the forger.

Jain and Uludag [2] worked with hiding fingerprint minutiae in images. For this purpose, they considered two application scenarios: A set of fingerprint minutiae is

transferred as the watermark of an arbitrary image and a face image is watermarked with fingerprint minutiae. In the first scenario, the fingerprint minutiae are transferred via a non-secure channel hidden in an arbitrary image. Before being embedded into the host image, the fingerprint minutiae are encrypted, which further increases the security of the data. The produced image is sent through the insecure communication channel. In the end, the image is received and the fingerprint minutiae are extracted, decrypted and ready for any further processing.

In the second scenario, a face scan is watermarked with fingerprint minutiae data and the result is encoded in a smart card. For the authentication of a user, the image is retrieved from the smart card, the fingerprint minutiae are extracted from it and they are compared to the minutiae obtained from the user online. The user is authenticated based on the two fingerprint minutiae data sets and the face image.

Jain et al. [3] have presented a fingerprint image watermarking method that can embed facial information into host fingerprint images. The considered application scenario in this case is as follows: The fingerprint image of a person is watermarked with face information of the same person and stored on a smart card. At an access control site, the fingerprint of the user is sensed and compared with the one stored on the smart card. After the fingerprint matching has successfully been completed, the facial information can be extracted from the fingerprint image on the smart card and can be used for further authentication purposes.

3 Combining Image Watermarking Techniques with Visual Based Biometric Systems

Visual-based biometric systems use feature extraction techniques to collect unique facial patterns and create biometric templates. However, biometric templates are subject to fraud especially in passport cloning and illegal immigration. Image watermarking techniques along with cryptographic primitives can be used to verify the authenticity of a person and also detect any modification to biometric templates when these are securely stored.

Biometric templates of a fingerprint and a face scan can be hashed and encrypted with cryptographic algorithms and then embedded into an image. For example, with the use of hash functions and encryption methods, the owner of a facial image can embed his/her template. The recipient can extract it by decrypting it and therefore can verify that the received image was the one intended by the sender. Encrypting and hashing watermarked information can guarantee the authentication of the owner and the image itself since the purpose of watermarks is two-fold: (i) they can be used to determine ownership, and (ii) they can be used to detect tampering.

There are two necessary features that all watermarks must possess [7]. First, all watermarks should be detectable. In order to determine ownership, it is imperative that one be able to recover the watermark. Second, watermarks must be robust to various types of processing of the signal (i.e. cropping, filtering, translation, compression, etc.). If the watermark is not robust, it serves little purpose, as ownership will be lost upon processing. Another important requirement for watermarks is the perceptual transparency between the original work and the

watermarked; and for images objective metrics are widely used. The watermarked message may have a higher or lower level of perceptibility, meaning that there is a greater or lesser likelihood that a given observer will perceive the difference. The ideal is to be as imperceptible as possible and it is required to develop models that are used to compare two different versions of the works and evaluate any alterations. Evaluating the perceptibility of the watermarks can be done with distortion metrics.

These distortion metrics do not exploit the properties of the human visual system but they provide reliable results. Also, there is an objective criterion that relies on the sensitivity of the eye and is called *Watson* perceptual distance. It is also known as just noticeable differences and consists of a sensitivity function, two masking components based on luminance, contrast masking, and a pooling component. Table I gives the metrics that are used more often.

Table I. Quality Measurements

		Mean Square Error (MSE)	$MSE = \frac{1}{MN} \sum_{m,n} \left(I_{m,n} - \tilde{I}_{m,n}\right)^2$
Signal to Noise Ratio (SNR)	$SNR = \sum_{m,n} I_{m,n}^2 / \sum_{m,n} \left(I_{m,n} - \tilde{I}_{m,n}\right)^2$	Normalized Cross Correlation (NC)	$NC = \sum_{m,n} I_{m,n}\tilde{I}_{m,n} / \sum_{m,n} I_{m,n}^2$
Peak Signal to Noise Ratio (PSNR)	$PSNR = MN \max I_{m,n}^2 / \sum_{m,n} \left(I_{m,n} - \tilde{I}_{m,n}\right)^2$	Correlation Quality (CQ)	$CQ = \sum_{m,n} I_{m,n}\tilde{I}_{m,n} / \sum_{m,n} I_{m,n}$
Image Fidelity (IF)	$IF = 1 - \sum_{m,n} \left(I_{m,n} - \tilde{I}_{m,n}\right)^2 / \sum_{m,n} I_{m,n}^2$	Watson Distance (WD)	$D_{wat}(c_0, c_w) = \left(\sum_{i,j,k} \lvert d[i,j,k] \rvert^4 \right)^{1/4}$

There are plenty of image watermarking techniques available in the literature but we have combined ***lattice*** and semi-fragile, or ***block-wise***, embedding methods to take advantage of their unique features. Briefly, the lattice watermarking system embeds only one bit per 256 pixels in an image. Each bit is encoded using the trellis code and produces a sequence of four bits. The trellis coding is a convolution code and the number of states is 2^3=8 with possible outputs 2^4=16. After the encoding procedure, the bits need to be embedded in 256 pixels which means that each of the four bits is embedded in 256/4=64 pixels [6].

The *block-wise method* involves the basic properties of the JPEG compression where DCT domain takes place. Four bits are embedded in the high-frequency DCT of each 8x8 (64 pixels) block in the image and not in the low-frequency in order to avoid any visual differences that would lead to unacceptably poor fidelity. By using the block-wise method, the image can host 16 times more information than lattice. Specifically 28 coefficients are used which means that each bit is embedded in seven coefficients. The seven coefficients that host one bit are chosen randomly according to a seed number and thus, each coefficient is involved in only one bit [6].

By combing the two methods, we can exploit their advantages particularly, in circumstances where both the quality and the ability to notice the corrupted blocks is essential. In an image, the part that is likely to be illegally altered is watermarked with the block-wise method while the rest of the image is watermarked with the lattice method. In a facial image, for example, the areas of the eyes, mouth and jaw can be

used to embed the fingerprint template. The round area of the face can be used to embed additional information, such as the name and/or address of the person shown in the photo with the lattice method. If an adversary changes for example the color of the eyes or some characteristics of the face (e.g. adding a moustache) the combined algorithm is able to determinate the modified pixels. This is achieved by comparing the extracted message with the original.

The combination of the two embedding methods is implemented in a *cryptographic encoder-decoder*. The authority that wishes to protect a face or fingerprint photo, extracts the biometric template(s) of that person and along with a short description and a unique feature of the image are inserted in a hash function and the result is encrypted with a 1024-bit secret key. The signature, together with the short and the extracted unique description, is embedded with the lattice method while the biometric template is embedded with the block-wise algorithm. As a unique description we have used the sum of the pixel values of the four blocks in the corners. The Secure Hash Algorithm (SHA) and the Rivest, Shamir, Aldeman (RSA) [8] have been used to hash and sign the fingerprint template, short and unique descriptions. The design of the encoder is illustrated in Fig. 1a.

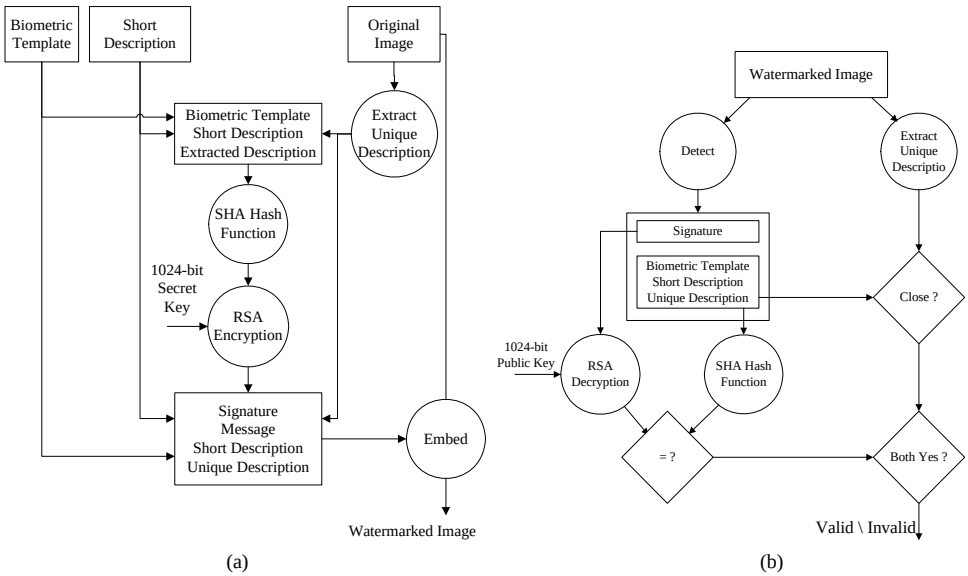


Fig. 1. Cryptographic Encoder / Decoder

From the watermarked version of the image, at the decoder's side, the signature, the short and unique descriptions are extracted with the lattice method while the biometric template is extracted with the block-wise algorithm. Then, the unique description is compared with the extracted one. Thus, the first step is to verify whether the unique descriptions match. In the case of the watermark being copied and embedded in another image, the extracted description will not be the same. This is due to the fact that the pixel values of the image have been slightly changed to host

the watermark, the extracted description cannot be exactly the same, but can be very close. Therefore, some upper and lower boundaries have been determined for this step of verification.

The next step is to decrypt the signature using the 1024-bit RSA public key and retrieve the hash value. The biometric template, short and unique descriptions that have been extracted, is again the input to the hash function. The obtained hash value is then compared with the one decrypted from the signature. The third step of the decoder is to verify whether the decrypted hash value matches exactly with the one calculated by the decoder. If both hash values and unique descriptions are valid, the authentication process is successful. The whole design of the decoder is presented in Fig. 1b.

4 Experimental Results

In order to evaluate the performance and the efficiency of the embedding methods, excessive tests have taken place. A number of cases have been considered each with a different variable parameter. A grayscale bitmap image with 300x300 (Fig. 2a) resolution has been used for the experiments. The difference between the original and the watermarked image was evaluated by the ideal values of the original image that are presented in Table II.

Table II. Ideal Values of the test Image

Quality Measurements	Ideal Values	Quality Measurements	Ideal Values
MSE	0	NC	1
SNR (dB)	97	CQ	129.923
PSNR (dB)	104	Watson Distance	0
IF	100		

Cases have also been considered once again each with a different variable parameter, independent of lattice and block-wise methods in order to maintain image quality. When combined image watermarking is performed, a small part of the image is watermarked with the block-wise method and the rest is watermarked with the lattice method. We assume that the most vulnerable to illegal modifications, is the small part. The biometric template is embedded in the small part while the short and extracted descriptions are embedded in the large part of the image. The experimental tests of the quality measurements were performed using: only lattice; only block-wise; combined block-wise and lattice.

It was found that the lattice method achieves better results than the block-wise and expected that the produced result values of the combined case would be in between the values of those produced by the two methods. Particularly, in the case of the lattice algorithm the maximum number of the embedded bit can be 351 (one bit per 256 pixels). The formulas that are used to evaluate the differences between two images are presented in Table I. The tests were executed using a range of values for

the parameter in order to conclude what the best values are. The parameters are the embedding strength (β) and the lattice spacing (α). The range of the α value was from 0.35 to 5.33 and the range of β from 0.7 to 1.1. The incensement steps for a was 0.02 and for β 0.1.

The measurement values for the lattice method are very close to the ideal ones. More specifically, the direction towards zero is achieved using low values of α in the case of MSE. If at the same time the value of β that is used is low, the MSE is decreased even further. In the case of SNR and PSNR, the result values are higher when the parameters α and β are low. The image fidelity (IF), which is defined as a percentage of how identical the images are, the value of 100% is considered to be the optimum and as can be noticed from Table III, the results are very close to this. Utilizing the NC and the CQ quality measurements, it is observed that their measurements are closer to the ideal ones (Table II), as the values of α and β are decreased. The above observations are also justified from the Watson measurement which is based on luminance, contrast, and pooling masking.

Table III. Results From Lattice, Block-Wise and Combined Embedding Methods

alpha(a)=0.93, beta(β)=1.0, alpha(a)=0.1	**Lattice alpha(a), beta(β)**	**Block-Wise alpha(a)**	**Combined alpha(a),beta(β) alpha(a)**
MSE	0.353	1.428	0.389
SNR	47.13	39.33	45.14
PSNR	53.27	45.29	52.52
IF	99.969	99.983	99.966
NC	0.99999	0.99992	0.99994
CQ	129.925	129.916	129.922
Watson-Distance	31.436	58.262	32.453

(a)

alpha(a)=1.53, beta(β)=0.8, alpha(a) =0.2	**Lattice alpha(a), beta(β)**	**Block-Wise alpha(a)**	**Combined alpha(a),beta(β), alpha(a)**
MSE	0.545	4.951	0.72
SNR	43.18	33.62	41.97
PSNR	50.77	41.18	49.55
IF	99.9952	99.9563	99.9936
NC	0.99998	0.99985	0.99998
CQ	129.921	129.903	129.921
Watson-Distance	48.901	157.506	49.136

(b)

Therefore, it could be suggested that the optimum parameter values are those that give the best results. They could even be the zero values. But at the decoder's side not all the bits are extracted correctly. Specifically when using low values of α and β, the decoder is not able to get the correct embedded bits. In conclusion it can be said that a trade-off between the quality results and the decoder's result is necessary in order to determine the optimum values. From the tests we concluded that suggested values could be $\alpha \approx 1.53$ and $\beta = 0.8$ (Table IIIb).

Similarly, in the case of the block-wise method, the tests were executed for the same image in order to be comparable with those of the lattice method. One major difference is the number of bits that are embedded. Since the method embeds four bits

in every 64 pixels and the image has 90000 pixels in total, the number of bits can be hosted in 5625. The size of the information that can be watermarked is significantly higher and in fact is 16 times greater than the size in the lattice method. Therefore, before even executing the test, it is expected that the results will not be as good. The information in the block-wise method is much more, which means that the alterations in the image will produce worse values in the quality measurements.

The observation of the results proves what is being stated in the beginning. The values of the quality measurements are not as good in comparison with those of the lattice method since the measurement of the MSE is higher than the ideal value, which is zero. The values of the SNR and PSNR, which are widely used, show that as the value of the parameter alpha (a) is increased, the result becomes worse. In the case of the IF, NC, and CQ, the measurements seem to be distant from the ideal values as alpha (a) takes higher values. The same conclusion can be phrased for the perceptual distance given by the Watson model, where the results are worse as the value of alpha (a) is increased.

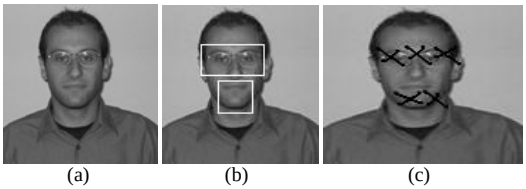
It seems that as the value of alpha is increased, the watermarked image has poorer fidelity. So the optimum value of the parameter should perhaps possibly be a small one e.g. 0.01. However, it seems that values below 0.05 do not allow the decoder to get the right message. The chosen value of alpha depends on how sensitive the user wants the method to be in order to locate the corrupted bits and mark the corresponding blocks. Higher values increase the sensitivity but at the same time the quality of the image is reduced. So it is again necessary to make a trade-off between the results and the sensitivity. A possible suggested value could be a ≈ 0.2 (Table IIIb).

Indeed the results were not as good as those of the lattice method but they were better than those of the block-wise method. In Table III some result values of the combination are given in order to compare them with those of the two methods when they are applied individually. Table III justifies that the combination produces quality measurements between the two methods. Table IV presents the maximum number of bits that can be hosted in the image using the two embedding methods and a combination of them.

Table IV. Maximum Number of Embedded Bits

	Lattice	**Block-Wise**	**Combined**
Max Embedded Bits	351	5625	2752

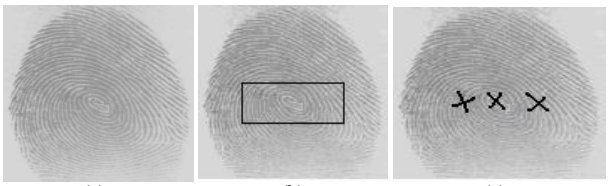
The last test was to verify that in case somebody modifies the block-wise part of the image, which is the biometric template, the decoder realizes the modification, informs the authority that the authentication application failed and outputs a file with the modified blocks marked. The part that is likely to be illegally altered is the eyes or jaw and the biometric template(s) of the facial and/or fingerprint images which are embedded with the block-wise method (Fig. 2b). In the watermarked version the distance between the eyes was changed and this image was inserted in the decoder in order to verify its authenticity. The authentication process failed and a marked image was produced (Fig. 2c). By observing the last image it is clear that the decoder has successfully located the modified blocks.



(a) (b) (c)

Fig. 2. Original Image (a), Watermarked Image (a), Marked Image (c)

Throughout the paper we have considered the case where a fingerprint and/or facial template is embedded into a facial image. That does not mean that a facial image cannot be embedded with our method into a fingerprint image, which is illustrated in Fig. 3. Similar to Fig. 2, Fig. 3a is the original image, Fig. 3b is the watermarked and Fig. 3c is the marked image generated by our testbed.



(a) (b) (c)

Fig. 3. Original Image (a), Watermarked Image (a), Marked Image (c)

The potential danger with sensitive databases containing biometric identifiers, such as facial, fingerprint images and templates, is that they are likely to be attacked by hackers or criminals. Watermarking the information in these databases can allow the integrity of the contents to be verified. Another danger is that this critical data can be attacked while it is being transmitted. For example, a third party could intercept this data and maliciously alter the data before re-transmitting it to its final destination. The transmission problem is even more critical in cellular and wireless channels. The channels themselves are quite noisy and can degrade the signal quality.

Additionally, data transmitted through wireless channels is far from secure as they are omni-directional, and as such can be eavesdropped with relative ease. The growth of the wireless market and e-commerce applications for PDAs requires a robust cryptographic method for data security. There are compact solid state sensors already available in the market, which can capture fingerprints or faces for the purpose of identity verification. These devices can also be easily attached to PDAs and other hand-held cellular devices for use in identification and verification.

Considering all the noise and distortion in cellular channels, our combined watermarking technique along with the cryptographic encoder/decoder will mainly work in smudging, compression and filtering. Our cryptographic encoder/decoder will only fail when noise and distortion is detected in the sensitive areas of the images that have been embedded with the block-wise algorithm. If our watermarked image is transferred in a noisy channel, then we need to reduce the amount of information inserted with the block-wise method to have a high rate of success.

5 Conclusion

Watermarking biometric data is of growing importance as more robust methods of verification and authentication are being used. Biometrics provides the necessary unique characteristics but their validity must be ensured. This can be guaranteed to an extent by watermarks. Unfortunately, they cannot provide a foolproof solution especially when the transmission of data is involved. A receiver can not always determine whether or not he has received the correct data without the sender giving access to critical information (i.e., the watermark).

In this paper we have presented a cryptographic encoder/decoder that digitally signs biometric templates, which are embedded with combined lattice and block-wise image watermarking techniques into an image. Combining image watermarking techniques with cryptographic primitives enables us to protect biometric templates that have been generated by a visual-based biometric system without any distortion of the image. Since biometric templates are essential tools for authenticating people, it is necessary to protect them for possible alterations and fabrications in conjunction with their biometric image(s) when these are stored in private/public databases.

Image watermarking techniques in conjunction with cryptographic primitives provide a powerful tool to authenticate an image, its biometric template and any additional information that is considered important according to a particular application. In the passport-based scenario, for example, the photograph and the private information (i.e. name/address) of an individual can be protected with the proposed approach. Our results showed that we can combine watermarking techniques to securely embed private information in a biometric image without fading it out.

References

1. R. Brunelli and T. Poggio, "Face recognition: features versus templates", *IEEE Trans. On Pattern Analysis and Machine Intelligence*, 15:1042-1052, 1993
2. Anil K. Jain, Umut Uludag, "Hiding Fingerprint Minutiae in Images", *In Proc. Automatic Identification Advanced Technologies (AutoID)*, pp. 97-102, New York, March 14-15, 2002
3. Anil K. Jain, Umut Uludag, Rein-Lien Hsu, "Hiding a face in a fingerprint image", *In Proc. International Conference on Pattern Recognition (ICPR)*, Canada, August 11-15, 2002
4. S. Y. Kung, M. W. Mak, S. H. Lin, *Biometric Authentication: A Machine Learning Approach*, Prentice Hall Information and System Sciences Series, 2005
5. C. F. Lucilla, M. Astrid, F. Markus, V. Claus, S. Ralf, D. Edward J., "Biometric Authentication for ID cards with hologram watermarks", *In Proc. Security and Watermarking of Multimedia Contents SPIE'02*, Volume 4675, pp. 629-640, 2002
6. F. Peticolas, R. Anderson, and M.Kuhn, "Information hiding – a survey", In IEEE Proceedings, Vol: 87, No: 7, 1999, Page(s): 1062-1078
7. P. H. W. Wong, O. C. Au, and Y. M. Yueng, "Novel blind watermarking technique for images", IEEE Trans. On Circuits and Systems for Video Technology, 13(8):813-830, 2003
8. F. Hao, R. Anderson, J. Daugman, "Combining Crypto with Biometrics Effectively", *IEEE Transaction on Computers*, Vol. 55, No. 9, 2006, Page(s): 1081-1088