Int. J. Advance Soft Compu. Appl, Vol. 11, No. 1, March 2019
ISSN 2074-8523

The Construction of Confidence Bits to Improve Protected Iris Recognition System

Tong-Yuen Chai, Bok-Min Goi, and Yong-Haur Tay

Lee Kong Chian Faculty of Engineering and Science, Universiti Tunku Abdul Rahman, Bandar Sg. Long
e-mail: chaity@utar.edu.my
Lee Kong Chian Faculty of Engineering and Science, Universiti Tunku Abdul Rahman, Bandar Sg. Long
e-mail: goibm@utar.edu.my
Lee Kong Chian Faculty of Engineering and Science, Universiti Tunku Abdul Rahman, Bandar Sg. Long

Abstract

This paper discussed about a recent iris template protection scheme named Indexing-First-One hashing (IFO). IFO hashing is originally inspired by the concept of min-hashing while integrating Hadamard product and modulo threshold function to increase the complexity in reconstruction by adversary. It possesses strong security shield against major security and privacy attacks. However, similar to other template protection schemes, it degrades the recognition performance of biometrics system. In this paper, we propose a confidence mask based method into biometric system to overcome the performance degradation experienced by IFO template protection scheme. The newly proposed biometric framework shows promising improvement of 22% and 17% in recognition accuracy for CASIA iris database v1 andv3-interval respectively with lower equal error rate being reported.

Keywords: *iris recognition, template protection, collision matching scheme, confidence mask.*

1 Introduction

Biometrics system has been rapidly implemented in our daily lives. Possessing with superior advantages in terms of efficiency and convenience, biometrics system is gradually replacing traditional security systems such as lock & key and other password-based system. However, with the rapid development of biometrics

system, another security threat had been issued which is biometric template security. Biometric template protection is a very hot research topic as with the mature of biometrics recognition technology, security serve as a very important part in a complete optimum biometrics system. This is because unlike traditional lock-and-key and password-based security systems where the token of access (keys, passwords) can be easily replaceable, most of the human biometrics (fingerprints, human iris) are stable and will not vary along human age. Therefore, if our biometric information is compromised, it is impossible for us to replace our raw biometric template and eventually it will lead us to life-time security crisis.

Biometric template protection scheme serves as a protection step where it will alter the biometric template via random projection, matrix rearrangement and combination of matrix with secret keys to produce a hashed matrix which is hard to reconstruct back to the original biometric template. The protected template will be saved in the database instead of the unprotected original template. The matching stage will also carry out in the transformed domain therefore there is no raw biometric template being exposed to the potential threat of compromise. There are two major requirements in order to achieve a good biometric template protection which are i) Irreversibility, where it is computational infeasible for wrongdoer to reconstruct the original biometric template from the protected hashed template and ii) Unlinkability, where different version of protection biometric templates can be generated using the same biometric template while cross-matching will not be successful among the different versions of protected biometric template. On top of the requirement stated above, biometric template protection scheme needs to be able to maintain the recognition performance and other important performance parameters such as hashed-code size (storage purpose) and processing speed compared to the unprotected biometric template.

However, there is still a challenge in searching the optimum state between performance and security. Some biometric template protection schemes do preserve the system performance but it leaves some security doubt while other schemes provide stronger and complex biometric template protection in exchange of recognition performance. In this paper, indexing-first-one hashing scheme [10] will be used in our experiment as the template protection since it is proven strong in security aspect to protect biometric feature. By implementing Hadamard product and modulo threshold function, huge amount of biometric information will be lost in the transformation process which increases the difficulty of template reconstruction. Besides, modulo threshold function increases the number of guessing during reconstruction due to its many-to-one mapping nature. On top of that, this method has been proven to survive from several major privacy attacks such as attack with record multiplicity (ARM). Therefore, it is a very good case study with the outstanding overall performance as well as high inherent security strength.

2 Related Work

Iris recognition was first proposed by John Daugman [1], in his article, he pointed out that human iris is a good alternative for automatic biometric recognition compared to fingerprint which often exposed to environment and easily wound. The author used a phase-quadrature 2-D Gabor wavelets demodulation process to extract the segmented iris features followed by a quadrant quantization to produce the iris code. During comparison stage, iris code is compared using a Boolean Exclusive-OR while masked (AND) with mask bit and hamming distance is used to calculate the final matching result. Another feature extraction method is studied in [2] where the author developed an efficient algorithm for iris recognition by characterizing key local variations. By using dyadic wavelet transformation, local sharp variation point which represented the characteristic of the iris will be record as iris features.

Global iris bits stabilization with the combination of localized Zernike moments phase-based encoding stage is used in [3] to develop a more accurate and noise-resistant iris recognition system which can be used for both NIR and visible eye iris sample under less-cooperative circumstances. In [4], the author used another method of multiple signature method to divide human iris into six regions to solve the noise effect of iris recognition. The author stated that the separation method comes from the initial studies of the locations of some most common types of noise such as reflection of light, iris obstruction often locate on the upper/lower and boundary of the iris respectively. The method is able to minimize the effect of each type of noise by comparing the iris code separately. The same idea is studied in [5] where unlinkable multi-biometric iris cryptosystem based on fuzzy vault scheme is generated by combining left and right portion from two irises from the same person to improve the recognition performance. The combined processed set of feature values goes into key-binding stage where the values are bounded with a secret polynomial to create final protected iris template.

The concept of cancelable biometric template protection is firstly introduced by Ratha et al. [6], by applying non-invertible geometric transformations which are block permutation and feature folding to the biometric template. Other than that, as an extension to his work, he has proven that surface folding transformation outperformed others in fingerprint biometric [7]. Random Projections method is used in [8] to generate cancelable iris template that mitigates the effect of outliers in iris template. Cancelable biometrics based on Bloom filters is introduced by Rathgeb et al. [9] to generate un-invertible cancelable biometric template, the scheme uses binary to decimal transformation followed by index remapping strategy to achieve irreversibility. Random permutation matrix can also be used in conjunction with bloom filter to achieve unlinkability across all versions of the generated cancelable biometric template. Indexing-first-one (IFO) hashing is introduced by Y.L. Lai et al. [10] to generate irreversible iris template. With the implementation of two additional methods which are P-order Hadamard Product

and Modulo Threshold function, IFO hashing is able to create a strong security protection against numerous privacy attacks such as single-hash attack, multi-hash attack etc. In his later work in [11], IFO hashing is coupled with bloom filter methodology to solve the pre-alignment issue of iris biometric due to iris rotation and tilted iris acquisition. By implementing bloom filtering, the system is able to offer higher recognition performance compared to the conventional IFO hashing without pre-alignment.

In [12], fragile bits technique is used to improve the performance of iris processing and matching system. The author weighted every corresponding encoded bit with a probability value to indicate the level of confidence of the respective bit. By training through several intra-class samples, iris bit with higher consistency will be less frequent to flip and vice versa. If the flipping drops over a preset threshold, the bit will be categorized as fragile bit which will be ignored during the matching stage. Bit Reliability-driven template matching is proposed in [13] where the author adopts the topology of fragile bits in their developed approach. Instead of requiring multiple samples from the same class to generate initial reliability weight mask, the reliability mask will eventually updates every successful iris authentication.

In [14], the author achieved cancelable iris biometrics using block re-mapping and image warping. However, it is observable that the matching performance dropped after implementing the cancelable biometric template protection approach. Other than that, the degradation of performance is also shown in another article [10]. On top of that, the security aspect of this method is considered low as the iris code can be easily reconstructed given that the attacker obtains parameters of the transformations. In [15], although the author stated that there is little to no degradation in terms of performance accuracy, 6 out of 10 iris samples for each class are used to extract the consistent bit vector during enrollment. The training sample exceeds 50% of the total samples of each class which leads to problem when limited number of biometric templates is available due to privacy issue. Random row wise offset is applied to the iris code and random pairs of iris code row will be combined by using different operations such as AND, XOR or XNOR to achieve cancelable iris biometric [16]. In this method, original pixel intensities or bit strings will be “damaged” so the raw biometric cannot be recovered. However, performance degradation is also observed as a result of the protection for better security.

3 Problem Formulations

In this paper, the degradation in performance due to the nature of biometric template protection schemes has been highlighted in earlier section. To the best of our knowledge, there is no literature that looks into this severe problem to date. Thus, we have proposed a simple and fast method to improve the recognition

performance. This can be done in two stages. First, the constructions of confidence mask which involves training samples. Next, collision matching scheme is proposed to match the query biometric template across the confidence masks.

The proposed method in this paper with the construction of confidence mask and collision matching scheme are newly developed and novel in terms of contribution. Biometric template protection is essential to protect the privacy of the users and restore the confidence of public on the future implementation of biometrics systems. However, most of the biometric template protection schemes available are designed to lose and distort information in order to fulfill the requirement on irreversibility and unlinkability. This inevitability degrades the recognition performance of biometrics systems after going through template protection scheme. In this work, we believe that we are among the first to highlight this drawback and propose a trainable method which is not only able to work on the protected/transformed biometric features in hashed domain but also able to further improve the recognition accuracy of biometrics system which has been degraded earlier by template protection scheme.

4 The Proposed Method

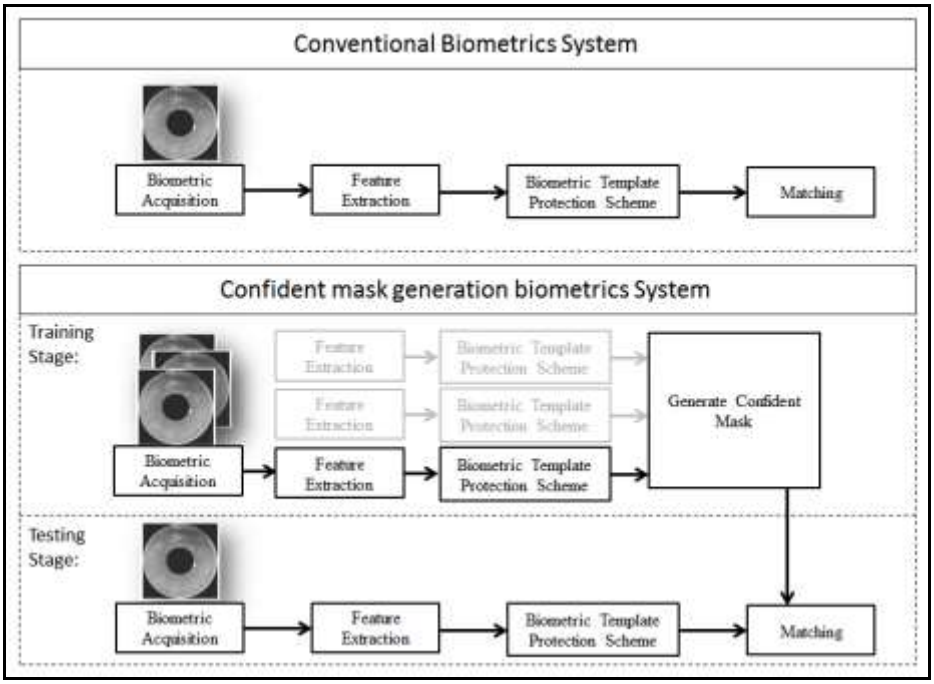

Fig. 1. Overview of the design for the proposed biometrics system

Figure 1 shows the comparison between a conventional biometrics system and our proposed framework, confidence mask based biometrics system. In conventional

biometrics system, after the acquisition stage, the raw biometrics features will undergo features extraction process to extract as much useful information from the biometrics. After that, the extracted biometric features will through biometric template protection (BTP) scheme to transform into protected biometric template. Finally, the protected biometric template will proceed into matching stage where the protected template will match with another query sample which went through the similar process. Differing from the conventional biometrics system, our proposed framework can be categorized into 2 stages, training stage and testing stage. In training stage, multiple biometric samples from the same personnel can be used to generate the confidence mask. As we can observe, our method is able to work directly in the hashed domain. In testing stage, the query template will first undergo the same feature extraction and BTP process. However, a proposed collision matching scheme will be conducted between the query template and the confidence mask to generate a matching score. This additional step has proven to improve the recognition performance of protected iris recognition system in Section 5.

4.1 Biometric Template Protection Scheme

The main contribution of this project is mainly taken place after the feature extraction and template protection stages in a biometric system. A typical method to extract a representation of iris texture called iris code [1]. Therefore, iris code has been used as the standardized input in our experiments. First, the iris code will undergo a state-of-the-art iris template protection scheme called indexing-first-one (IFO) hashing [11]. This process is mainly used to protect the biometric template by transforming the extracted biometric features into another form of matrix which it is hard for the adversary to reconstruct the original biometric features. IFO provides not only non-invertibility but also cancelable transformation for biometric features. The methodology of IFO hashing is shown in the Figure 2.

IFO is a row-wise function where firstly, the matrix will first undergo several random permutations. Then, huge amount of information is expected to lose by multiplying all the permuted matrices through logic AND function. This is to prevent easy reconstruction of iris code while part of the noisy bits can be excluded. After that, only first K columns of the code are selected while anything beyond K columns are all deleted. The index with the first ‘1’ along the code within the selected K columns will be recorded down. Lastly, the recorded integer value will undergo a modulo threshold function. This function induces a many-to-one mapping which further strengthen the non-invertibility properties and increases the security complexity of the biometric template protection scheme.

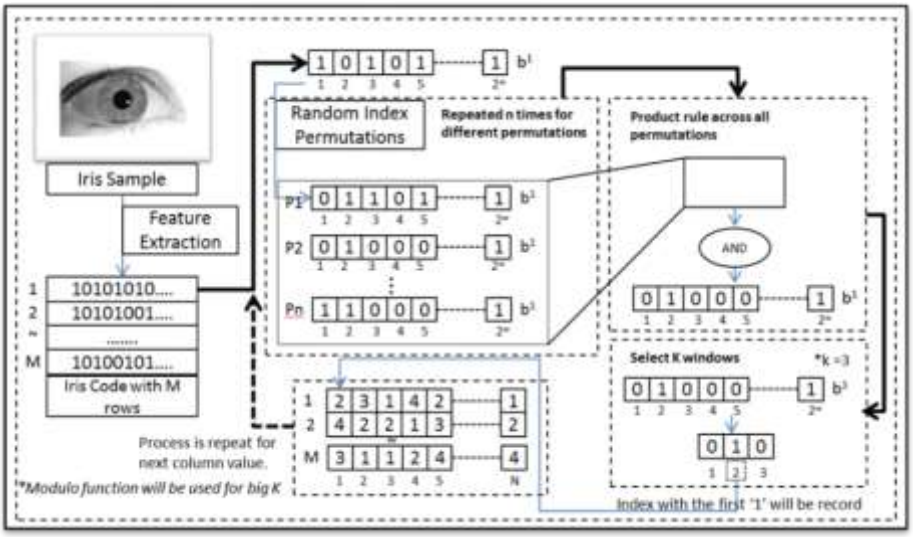

Fig. 2. Overview of the design for Indexing-First-One hashing scheme

This biometric template protection scheme is proved to be effective dealing with several attacks such as single-hash attack, multi-hash attack, pre-image attack, etc. due to its transform complexity. It will simply take took much efforts in reconstructing of the biometric template as there is not enough information on the protected template for template reconstruction. Other than that, this scheme also fulfilled the standard requirements of biometric template protection which are irreversibility where it is not feasible for the protected template to reconstruct back to the previous unprotected biometric template and unlinkability where different version of protected template can be constructed using the same biometric template and cross-matching cannot be done among the different versions of protected template.

4.2 THE GENERATION OF CONFIDENCE MASK

Previous research has indicated a decrease in False Rejection Rate (FRR) by several orders of magnitude through masking out fragile bits. As a result, this algorithm slightly increases the separation between the match and non-match distributions. However, we do not aim to address the difference between fragile bits and our proposed method here. In this paper, we propose a different approach by constructing a confidence mask instead. The main focus of this work is to improve the recognition performance of the protected biometric templates, in another words, to mitigate the effect of degradation introduced by template protection scheme.

Since the concern is on the recognition performance and degradation, the generation of confidence mask will begin after the hashing of biometric template protection scheme, in this case, IFO-hashing. At this stage, the hashed code will be separated into 2 categories which are training samples and testing samples. Training samples are randomly selected to generate the confidence mask while testing samples are selected to validate the result. In typical cases, excessive number of training samples is not recommended as this might lead to arguable result due to the biased training condition. Therefore, the maximum training samples used in our experiment will not exceed 50% of the total number of samples of each respective class. For example, if the total number of samples is 7, maximum training samples allowed will be 3.

We take two randomly selected hashed codes, A and B (training samples) as shown in Figure 3. Collision matching is proposed to cross-match each and every element between the two training samples. Collision matching is the collision formulation to calculate element-wise similarity across multiple training samples. In our proposed design, a zero matrix with the same size as the hashed code will first be constructed. If the element's value of hashed code A same as the element of hashed code B at location (x, y), then it will flip the respective bit location to '1' from its initial value. The overview of our proposed collision matching is shown at Figure 3 below.

Our proposed collision matching scheme can then be repeatedly applied between all possible pairs of training samples. All the results of the collision matching obtained will be fused via logic AND operation to produce the final confidence mask. The confidence mask indicates bit location among the feature matrix which is deemed to be either with confidence ('1') or no confidence ('0'). In order to be defined as confidence bit, all paired training samples need to have the same value on particular location to create a matched collision. If this condition is not fulfilled, the particular bit will be categorized under no confidence. This indicates that the variation of values being observed among all paired training samples on particular bit locations could be potentially affected by noise.

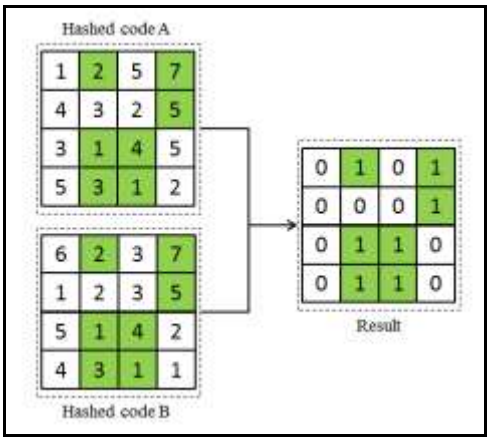

Fig. 3. Collision matching scheme

4.3 MATCHING SCORE

After the generation of confidence mask, the final stage is the matching part. In this part, collision matching will be conducted against a confidence matrix consisting the confidence masks for all classes. The final matching score can be calculated as follows,

$$Matching\ score = \frac{sum(match\ score==1)}{sum(confident\ mask==1)} \quad (1)$$

The matching score indicates the number of collided confidence bits of the confidence mask when a query protected biometric template is given.

5 RESULTS AND DISCUSSION

In this experiment, we have adopted two databases, CASIA v1 [17] and CASIA v3-interval [18] to verify the performance of our proposed algorithm. In CASIA v1 database, there are 756 eye images from 108 different classes (each class contains 7 eye images) whereas CASIA v3-interval contains 396 different left and right eyes and a total of 2639 eye images. In this experiment, the entire database of CASIA v1 database is used while the left eye images from CASIA v3-interval are chosen to form a subset database which contains a total of 124 classes and 7 eye images for each class which is adequate to achieve the objective of this project. Therefore, a total of 1624 (756+868) eye images are being adopted in this project. It is important to mention that the number of CASIA v3-interval database used in this project is the same as the database used by the state-of-the-art in iris template protection, Lai et al. [11] for the ease of benchmarking.

In [11], the best result obtained was 0.69% equal error rate (EER) compared to the best result 1.00% EER from conventional bit-shifting matching on Hamming Distance. In this project, our proposed method has achieved the best EER of 0.54% as shown in Table I. This shows a performance improvement of 22% from 0.69% EER reported by the state of-the-art. On top of that, performance improvement of 17% is also reported in CASIA v1 database. This result has indicated that the proposed method can be effectively implemented into different databases. Besides that, the ability of the proposed method to improve the performance of protected biometric template (IFO hashed iris template in this case) has been verified since inevitably performance will usually degrade after going through template protection scheme.

Table 1: Performance of proposed method

Training Sample		1	2	3
Equal Error Rate (%)	CASIA v1	5.81	4.80	5.01
	CASIA v3-interval	0.71	0.54	0.80

From the result tabulated above, the best result with lowest EER of 0.54% is reported with only 2 training samples are being used for confidence matrix generation. The performance worsens when increasing the training samples further. This is because when the training sample increases, the number of confidence bits '1' in the confidence mask will reduce. This happens due to the principle that all training samples need to be identical (all '0' or all '1') on the same bit location in order to generate the final confidence bit '1'. Therefore, although the confidence level on that particular bit location could be higher, the requirement in our proposed method is rigid and will only generate confidence bit if it is '1' at the same location in all training samples.

In the experiment using the CASIA v1 database, the best result with lowest EER of 4.80% is achieved by using only 2 training samples to generate the respective confidence matrix. However, it is reasonable to deem that the number of training samples needed to generate optimum confidence mask or lowest EER lies on the image quality of a specific database. As explained above, the training process is a highly bit-independent process as the same bit location across all training samples need to be identical in order to generate the final confidence bit '1'. As we increase our training samples, the confidence level of confidence matrix generated will also increase. However, this will also exaggerate the influence of noise in the process of generating confidence matrix. For example, if 5 training samples are used to generate confidence matrix instead of 2 and if 1 out of 5 training samples consists of noise, it might greatly alter the outcome of the confidence matrix. As a conclusion, the number of training samples needed to generate the optimum confidence matrix is heavily dependent on the overall image quality of the adopted database.

Table 2: Performance benchmarking for state-of-the-arts

Method		Equal Error Rate (%)
Block remapping	[14]	1.30
Bio-encoding	[19]	6.27
Adaptive bloom filter	[9]	1.14
Bin-combo	[16]	4.41
Alignment-free IFO	[11]	0.69
Alignment-free IFO with Confidence Mask		0.54

From Table 2, iris recognition performance of the state-of-the-art biometric template protection methods are shown in terms of equal error rate. All of the results in Table II are obtained by using the same database. Although different number of iris samples are used between different methods, it should not affect the qualities of iris samples and the EER much. Therefore, benchmarking can be done reasonably. Most of the methods shown suffered from different degree of degradation except for adaptive bloom filter [9] where the method increased the performance accuracy by 0.05%. However, alignment-free IFO [11] has the lowest equal error rate, 0.69% among all the benchmarking methods. Therefore, this method is adopted as the template protection method in this experiment. As a result, substantial amount of performance improvement has been achieved as the proposed method successfully reduces the EER to 0.54%.

6 CONCLUSION

In this work, we have proposed a method with confidence mask generation and collision matching scheme to improve the performance accuracy of iris templates under protected domain (hashed codes) as our main contribution. Confidence mask generation serves as a solution to reduce the performance degradation due to the nature of biometric template transformation in order to protect the template. The degradation has been seen as a tradeoff in order to have higher security on biometric template. Our proposed method aims to give a new insight for the potential development of protected biometric recognition system besides improving its recognition performance. On the other hand, further development on the confidence mask generation will be carried out with the purpose of finding the optimum method to recover the degradation effect caused by biometric template protection schemes. More databases and experiments will be conducted in future as the extension of this study.

ACKNOWLEDGEMENTS
The authors gratefully acknowledge the support from Fundamental Research Grant Schemes FRGS/1/2016/ICT02/UTAR/03/1 for this research.

References

[1] Daugman, John. (2009). How iris recognition works. *The essential guide to image processing*, 715-739.

[2] Ma, L., Tan, T., Wang, Y., & Zhang, D. (2004). Efficient iris recognition by characterizing key local variations. *IEEE Transactions on Image processing*, *13*(6), 739-750.

[3] Tan, Chun-Wei, & Ajay Kumar. (2014). Accurate iris recognition at a distance using stabilized iris encoding and Zernike moments phase features. *IEEE Transactions on Image Processing, 23*(9), 3962-3974.

[4] Kumar, M. Rajeev, M. Dilsath Fathima, K. Kiruthika, & M. S. Saravanan. (2013). Non-cooperative iris recognition: A novel approach for segmentation and fake identification. *Journal of Computer Science, 9*(9), 1241.

[5] Rathgeb, Christian, Benjamin Tams, Johannes Wagner, & Christoph Busch. (2016). Unlinkable improved multi-biometric iris fuzzy vault. *EURASIP Journal on Information Security 2016, 1,* 26.

[6] Ratha, Nalini K., Jonathan H. Connell, & Ruud M. Bolle. (2001). Enhancing security and privacy in biometrics-based authentication systems. *IBM systems Journa,l 40*(3), 614-634.

[7] Ratha, Nalini K., Sharat Chikkerur, Jonathan H. Connell, & Ruud M. Bolle. (2007). Generating cancelable fingerprint templates. *IEEE Transactions on pattern analysis and machine intelligence 29, 4*, 561-572.

[8] Pillai, Jaishanker K., Vishal M. Patel, Rama Chellappa, & Nalini K. Ratha. (2011). Secure and robust iris recognition using random projections and sparse representations. *IEEE transactions on pattern analysis and machine intelligence 33, 9*, 1877-1893.

[9] Rathgeb, Christian, Frank Breitinger, & Christoph Busch. (2013). Alignment-free cancelable iris biometric templates based on adaptive bloom filters. In *Biometrics (ICB), 2013 International Conference on* (pp. 1-8). IEEE.

[10] Lai, Yen-Lung, Zhe Jin, Andrew Beng Jin Teoh, Bok-Min Goi, Wun-She Yap, Tong-Yuen Chai, & Christian Rathgeb. (2017). Cancellable iris template generation based on Indexing-First-One hashing. *Pattern Recognition 64*, 105-117.

[11] Lai, Yen-Lung, Bok-Min Goi, & Tong-Yuen Chai. (2017). Alignment-free indexing-first-one hashing with bloom filter integration. In *Intelligence and Security Informatics (ISI), 2017 IEEE International Conference on* (pp. 78-82). IEEE.

[12] Hollingsworth, Karen P., Kevin W. Bowyer, & Patrick J. Flynn. (2004). Using fragile bit coincidence to improve iris recognition. In *Biometrics: Theory, Applications, and Systems, 2009. BTAS'09. IEEE 3rd International Conference on* (pp. 1-6). IEEE.

[13] Rathgeb, Christian, & Andreas Uhl. (2010). Bit reliability-driven template matching in iris recognition. In *Image and Video Technology (PSIVT), 2010 Fourth Pacific-Rim Symposium on* (pp. 70-75). IEEE.

[14] Hämmerle-Uhl, Jutta, Elias Pschernig, & Andreas Uhl. (2009). Cancelable iris biometrics using block re-mapping and image warping. In *International Conference on Information Security* (pp. 135-142). *Springer, Berlin, Heidelberg*.

[15] Ouda Osama, Norimichi Tsumura, & Toshiya Nakaguchi. (2010). Tokenless cancelable biometrics scheme for protecting iris codes. In *Pattern Recognition (ICPR), 2010 20th International Conference on* (pp. 882-885). IEEE.

[16] Zuo, Jinyu, Nalini K. Ratha, & Jonathan H. Connell. (2008). Cancelable iris biometric. In *Pattern Recognition, 2008. ICPR 2008. 19th International Conference on* (pp. 1-4). IEEE.

[17] Chinese Academy of Sciences. [Online] CASIA v1 Iris Image Database, http://biometrics.idealtest.org/dbDetailForUser.do?id=1 , 2003.

[18] Biometric ideal test. [Online]. CASIA v3 Iris Image Database, Available: http://www.cbsr.ia.ac.cn/Database.htm.

[19] Ouda Osama, Norimichi Tsumura, & Toshiya Nakaguchi. (2011). On the security of bioencoding based cancelable biometrics. *IEICE TRANSACTIONS on Information and Systems*, *94*(9), 1768-1777.