Iris Recognition: Existing Methods and Open Issues

Sajida Kalsoom
Department of Computer Science
COMSATS Institute of Information Technology
Islamabad, Pakistan
Email: sajida.kalsoom@comsats.edu.pk

Sheikh Ziauddin
Department of Computer Science
COMSATS Institute of Information Technology
Islamabad, Pakistan
Email: sheikh.ziauddin@comsats.edu.pk

***Abstract*—Biometric authentication uses unique physical or behavioural patterns in humans to identify individuals. Though biometric is generally considered most reliable, stable and unique among all entity authentication means, it is not as stable and unique as is usually conceived. In this paper, we highlight the issues with current state-of-the-art iris-based biometric authentication systems. This survey covers the review of existing iris recognition methods with a focus on enumerating the open issues that must be addressed in order to be more confident in the performance, security and privacy aspects of iris-based biometric systems.**

***Keywords*-Pattern recognition; biometric authentication; iris recognition; template security**

I. Introduction

With the increase in use of biometrics for human identification, control shifts to identifying the factors that affect the performance of biometric authentication systems. Biometric authentication systems use behavioural or physical characteristics to authenticate a user. These systems have become more reliable sources of authentication as compared to the traditional means like passwords or hardware tokens such as smart cards. Reliability of biometric authentication systems lies in the fact that, unlike passwords and smart cards, biometrics cannot easily be forged, shared, compromised or forgotten. Biometric is considered to be highly unique among all human population. Genetically, same identities including twins and irises of left and right eye of the same person represent different iris patterns [8]. Another important property of biometric is its stability [23][24][25][34]. In this paper, we will critically analyse these claims by showing counter-examples from other researchers' work. These will be discussed in the problems and open issues section in detail.

The rest of the paper is organized as follows. Section II provides an overview of existing iris recognition methods. Section III presents issues, problems and challenges associated with template security and recognition performance. The paper is concluded in Section IV.

II. Iris Recognition

Iris recognition is considered as one of the most reliable biometric authentication technique [9][19][35][37]. An iris recognition system captures human eye image using a near infrared iris sensor which passes through three steps to be transformed into an iris template. These three steps are iris segmentation, iris normalization and iris feature encoding. The iris segmentation procedure segments the annular iris region from the entire eye image. First, it finds the inner and outer boundaries (the iris-pupil and iris-sclera boundaries) of the iris, then it marks the region of the annular iris ring that is not visible due to eyelids and eyelashes. The iris normalization procedure transforms the segmented iris region into a fixed size to cater for variations in iris sizes among different eye images. The feature encoding procedure extracts the most distinguishing features from normalized iris images and typically encodes the result as a binary string.

Recognition involves either verification or identification. Verification is one to one comparison where claim of an identity is verified, e.g., an employee of an office. On the contrary, identification is one to many comparison where an identity is watched against an entire database, e.g., a criminal surveillance system. In the verification step, the recognition time captured image is compared with the image taken at the enrolment time. The comparison is mostly done by calculating the Hamming distance where a value of 0 represents a perfect match and a value of 1 represents perfect non-match.

This paper is not primarily a survey on iris recognition techniques, but is to identify performance and security related issues with existing techniques. So, we will briefly describe just a couple of representative systems, followed by a table, reproduced from [5], providing a comparative analysis of a number of state-of-the-art iris recognition systems.

The most famous iris biometric system is due to Daugman [7][8]. In Daugman's system, iris segmentation is performed by using the following optimization:

$$\max_{(r,x_0,y_0)} \left| G_\sigma(r) * \frac{\partial}{\partial r} \oint_{C(s;r,x_0,y_0)} \frac{I(x,y)}{2\pi r}\, ds \right|,$$

where r and (x_0, y_0) are candidates for the radius and center of the iris, $G_\sigma(r)$ is the one-dimensional Gaussian with standard deviation σ, $*$ is the convolution operator, $C(s; r, x_0, y_0)$ is the circular closed curve with center (x_0, y_0) and radius r, parameterized by s, and $I(\cdot, \cdot)$ is the input eye image. Noise due to eyelids occlusion is avoided by restricting ds to the nearly vertical regions. The above optimization is performed twice to find both iris and pupil circles. For template generation, Daugman uses phase information of the image. After detecting the iris boundaries and removing the irrelevant region, 2D

 ISBN: 978-1-61208-221-9

Gabor wavelets is applied on normalized iris image to the iris template. For comparison of iris templates, Hamming distance metric is used. Most of the subsequent work on iris recognition, follows Daugman's approach of using Hamming distance for template matching

After Daugman's iris recognition system, one of the most important and popular systems is due to Wildes [38][39]. For iris segmentation, Wildes first detects edges in the eye image and then applies a circular Hough transform to find circular pupil and iris boundaries. Much of the subsequent work on iris segmentation follows Wildes approach where a common variation is the usage of a coarse-to-fine strategy. For template generation, Wildes uses Laplacian of Gaussian filter applied at multiple scales to extract unique information from iris texture. His system uses normalized correlation between the templates for template matching at verification time.

As mentioned above, most of the subsequent work in iris recognition follows the above-mentioned seminal approaches. Most work on iris segmentation is a variation and enhancement of Wildes' approach, while most feature extraction schemes are variations on Daugman's wavelet-based approach. A very nice detailed survey of iris recognition techniques is due to [5]. Table I (reproduced from [5]) provides a quick comparison of recognition results for some of the important iris recognition techniques. The interested reader is referred to [5] for a detailed study of existing iris recognition techniques.

TABLE I
COMPARISON OF THE MOST CITED IRIS RECOGNITION TECHNIQUES [5]

First Author, Year	Database Size	Results
Alim, 2004	Not given	96.17%
Jang, 2004	1694 images including 160 w/glasses and 11 w/contact lenses	99.1%
Krichen, 2004	700 visible-light images	FAR/FRR: 0%/0.57%
Liu, 2005	4249 images	97.08%
Ma, 2002	1088 images	99.85%, FAR/FRR: 0.1%/0.83%
Ma, 2003	2255 images	99.43%, FAR/FRR: 0.1%/0.97%
Ma, 2004	2255 images	99.60%, EER: 0.29%
Ma, 2004	2255 images	100%, EER: 0.07%
Monro, 2007	2156 CASIA images and 2955 U. of Bath images	100%
Proenca, 2007	800 ICE images	EER: 1.03%
Rossant, 2005	149 images	100%
Rydgren, 2004	82 images	100%
Sanchez-Reillo, 2001	200+ images	98.3%, EER: 3.6%
Son, 2004	1200 images, (600 used for training)	99.4%
Sun, 2004	2255 images	100%
Takano, 2004	Images from 10 people	FAR/FRR: 0%/26%
Thornton, 2006	CMU database, 2000+ images	EER: 0.23%
Thornton, 2007	CMU database, 2000+ images	EER: 0.39%
Tisse, 2002	300+ images	FAR/FRR: 0%/11%
Yu, 2006	1016 images	99.74%

III. PROBLEMS AND OPEN ISSUES

We categorize issues of iris recognition systems in two broad classes namely those related to iris template security and those associated with iris recognition performance. Details are as follows.

A. Iris Template Security

As biometric is an integral part of human body, loss of one's biometric corresponds to loss of his/her identity. Therefore, security of biometric templates is one of the most important concerns in any biometric authentication system. In literature, we found four types of biometric systems which are described below along with related issues and challenges.

1) Traditional Biometric Systems: These are the conventional systems [7][25][38] which store users' templates in clear form to verify the identity. A template is generated at enrolment time, stored in the database without encryption/hashing and compared with the corresponding verification template at the verification time. As the template is used and stored in plaintext, a compromise of database has severe security and privacy implications. There are scenarios where users use the same biometrics for multiple applications or different organizations share data among themselves for their users. In such scenarios, cross-matching becomes feasible for tracking individual users [27][30][31].

2) Biometric Key Release: These are the systems where biometrics along with cryptographic keys are used for authentication and communication [32]. The effort lies in using biometric templates effectively to release cryptographic keys in a secure manner. Modern cryptographic keys are uniformly random and large in size, therefore it is not feasible for users to memorize them. In biometric key release systems, cryptographic keys are stored at some location and are released using biometric information of the user. When user inputs his/her biometric, cryptographic key is released for use in any security protocol. This way, the key would be released only to the authorized users.

Though these systems use biometric information effectively for cryptographic key storage and release, there are certain issues which are not addressed by these systems. First, though these systems secure cryptographic key using biometric template, the template itself still remains unprotected. This leads to all security and privacy issues discussed earlier. Second, these systems fail to provide revocability of biometric templates meaning that if it is known that biometric template of a

 ISBN: 978-1-61208-221-9

particular user has been compromised, it is not feasible for him/her to change his/her secret in contrast to password or hardware token-based systems.

3) Cancelable Biometrics: Cancelable biometric systems apply some transformation on the biometric template to secure the template [6][21][33][42]. The idea is that, instead of directly storing the template, a function is applied on the template and the output of that function (transformed template) is stored in the database. The transformation function must be non-invertible so that a compromised transformed template cannot be translated to the original template. The major advantage of cancelable biometric systems is that even if the transformed template is compromised, the original template still remains secure. In addition, the secret can easily be revoked by applying a different transformation to the original template resulting in a new transformed template. Moreover, a user can have different transformed templates for different applications he/she is using hence making cross-matching infeasible for any potential attacker.

Finding a suitable transformation function can be quite tricky in cancelable biometric systems. Standard non-invertible transformation functions (such as one-way cryptographic hash functions) do not work with biometric data due to intra-class variability of biometric data. Therefore, in most cases, transformation is user-dependent, i.e., user either has to remember a password/pin or to carry a token which stores the transformation parameters. This puts an extra burden on the user and effectively converts the system into two-factor authentication scheme. It is also desirable to observe user specific key to check the strength of user-provided secret.

4) Biometric Key Generation: In such systems, biometric template and cryptographic key are bind together [11][14][20][22][26][41]. Cryptographic key can either be generated directly from biometric template [14][20][22][41] or by using standard cryptographic techniques [11][26]. In former case, generated key is not uniform and hence may not be strong enough for use in many cryptographic protocols. In biometric key generation systems, neither biometric template nor cryptographic key is stored in cleartext. Instead, a value obtained by binding these two secrets is stored such that it is not feasible to get any of the two secrets from this bound value.

Though last three non-traditional systems described above are quite effective in resolving template security related issues in biometric recognition systems, in most cases, recognition performance is affected. In addition, speed of these systems is always slower as compared to conventional iris recognition systems. Moreover, most of these systems do not perform well with noisy iris image datasets. Due to all these issues, we can conclude that a reliable and efficient solution to solve template security related issues is yet to be achieved.

B. Iris Recognition Performance

An iris recognition system is considered ideal when match and non-match distributions do not overlap each other. There are a few factors which may lead to a significant drop in accuracy of iris recognition systems. These are detailed as follows.

1) Dilation: One of the important but often ignored factor is pupil dilation. Due to dilation effects, we have varying size of pupil, which results in decreased recognition performance. Dilation may occur due to many factors such as drugs, sunglasses, light illumination, etc.

Experimental studies are presented by Hollingsworth et al. identifying the effects of pupil dilation on iris recognition performance [15][16]. To produce dilation, they used ambient light for controlled intervals of time. Degree of dilation was measured by taking the fraction of pupil and iris radius. They conducted two experiments, one to find out the effects of dilation of same degree (between two templates to be matched) and second with varying dilation. Their findings indicate that 1) If both images have same but high pupil dilation, this results in lower recognition performance as compared to images with no dilation. 2) If images have different amount of pupil dilation, this results in further increasing of False Reject Rate (FRR).

Effects of pupil dilation on iris recognition performance have been studied by other researchers also [4][10][29]. Rakshit and Monro [29] have used eye drops to achieve the effects of dilation. For their experiments, they collected images before and after 5, 10 and 15 minutes of instilling of drops. In most cases, due to the instillation of drops, pupil lost its shape and they used their shape-description method to generate accurate normalized images. Their experiments also showed a decrease in recognition performance due to iris dilation. They also observed that, with the increase in time, dilation is increased leading to an increase in FRR. Dhir et al. [10] later extended their study with 15 subjects as compared to 11 in [29]. They found the same results namely dilation results in poor performance and false reject rate increases with increase in dilation which in turn increases with time after eye drops have been administered.

Bowyer et al. [4] categorized iris images in three classes based on amount of pupil dilation namely *small, medium* and *large*. For experiments with varying amount of dilation, their results show that the larger the difference in dilation ratio, the more the chances of false non-match. For experiments with same amount of dilation, their findings indicate that increasing the degree of dilation, increases the false match and false non-match.

From the above studies, it can safely be concluded that it is not that difficult to deceive iris recognition systems which is contrary to the popular belief in research community. Pupil dilation not only affects the recognition performance but an intruder can easily deceive the system by just wearing sunglasses or by using eye drops. Pupil dilation factor should be incorporated in iris recognition systems to increase confidence in recognition results.

2) Lenses: Around the world, approximately 125 million people use contact lenses. Therefore, iris recognition systems should be flexible enough to accommodate these large number of people. Designers of iris recognition algorithms claim that

 ISBN: 978-1-61208-221-9

recognition performance of their systems is not affected by the use of contact lenses[1][8][28][40]. But, recently, Baker et al. [2] come up with a study showing that every type of lens negatively affects iris recognition performance. They used a dataset containing 51 subjects with contact lens and 64 without lenses. After visual inspection of iris images, they categorized lenses into four categories. First category includes lenses that are visible but have no effects on the iris. Second category includes images that result in light or dark outline around iris and sclera. Third category includes lenses with large artefacts on the iris that are mainly due to written logo/number or misfit lens. Fourth category is one having subjects with hard lenses.

They conducted two experiments. First experiment compares results of contact lenses and non-contact lenses subjects while the second experiment compares results of different categories of contact lenses. In first experiment, false reject rate for subjects with lenses is 9.42% and 0.719% for subjects without contact lenses. This shows that contact lenses have a severely adverse effect on iris recognition accuracy. The second experiment showed that second category is the one with the lowest FRR of 3.9% whereas fourth category has highest FRR of 45.44%. Category one and three have also shown high false reject rates of 10.64% and 14.37%, respectively. As is clear from results, lenses of all types affect the verification results little or more depending on the type.

Baker et al. [3] later conducted a larger study on the effects of lenses. They used three different systems for iris recognition namely IrisBEE, VeriEye and CMU. They also categorised lenses in four types. The results show that false reject rate for subjects with lenses is much higher than that for subject without lenses. In addition, category four of hard lenses showed worst recognition results among all lens types for all three iris recognition systems.

Bowyer et al. [4] conducted a similar study to evaluate iris recognition performance among subjects wearing contact lenses. Their findings are that false non-match score was almost same for contact lens and non-contact lens groups while false match score was 0.27% for non-contact lens group and 5.64% for contact lens group showing a significant drop in recognition accuracy. From the above reported studies and results, the effects of the contact lenses are apparent on recognition performance. All types of lenses result in performance degradation so there is need to introduce techniques that can handle such scenarios to strengthen iris biometric systems.

3) Twins: In [17][18], Hollingworth et. al presented studies identifying the texture similarities between irises of twins. Their work is in contrast to the previous work which focuses on identifying the differences between genetically same identities. To conduct their experiments, they collected the data on twins day festival Twinburg in Ohio in August 2009.

They also collected the data from unrelated people to do comparative analysis. At first step, they performed biometric system testing and their findings are same as those of the old researchers, i.e., for iris biometric system, irises of twins are more or like similar as those belonging to unrelated people. At the second step, they performed user testing to identify similarities between irises of twins.

They conducted two user studies. First, where only irises of subjects are presented to respond to the queries and second where periocular images are displayed to the user to respond to the queries. On the iris image experiments, the average success score is 81.3% and for periocular queries success score is 76.5%. Their findings indicate that there are similarities between the irises of genetically same users which can be visually identified, but current biometric systems do not identify them. It is required to explore further and establish techniques so that biometric systems may utilize this visual similarity between genetically similar irises for the benefit of performance enhancement.

4) Time Variability: Human iris is considered stable over time [23][24][25][34]; but, a recent study by Gonzalez et al. [36] shows results which contradict what has been demonstrated so far. For their experimental evaluation, Gonzalez et al. used BioSecurId [12] and BioSec [13] baseline datasets. The former dataset consist of 254 individuals (8128 images) captured in four different sessions and later has 200 subjects (3200 images) captured in two different sessions, both splitted by a time span of one to four weeks. Results show that errors rate is increased in inter-session experiments compared with the intra-session ones. Their finding indicates that, as the lapse time between enrolment and comparison is increased, false accept rate remains unaffected but false reject rate is increased up to more than twice. Bowyer et al. [4] conducted a similar research to find the effect of time variability on recognition performance. Their recognition results also showed that as the time between enrolment and verification increases, false reject rate of the system also increases though that increase is less significant than that reported by Gonzalez et al. Although, research results show that time variability affects verification performance but to be more confident in extent of this effect, more research with large datasets is desirable.

5) Cataract Surgery: In [10] Dhir et al. and [29] Rakshit et al. identified the effects of cataract surgery on recognition performance. In [29], they collected the images of 3 patients before and after two weeks of cataract surgery. The results of pre and post surgery images comparison shows that cataract surgery does not affect recognition performance. Later on, Dhir et al. [10] did similar experiments with 15 subjects and found same results. Although the study is significant, but as the dataset was not large, there is need to do more experiments on larger datasets to explore the effects.

6) System Portability: To check system portability related issues, Bowyer et al. [4] performed experiments on a set of iris images acquired using different sensors namely LG 2200 and LG 4400. Experiments show false reject rate is higher when both images (enrolment and verification) are from different sensors compared with the results where both images are from the same sensor. The study is done on limited dataset and only using IrisBEE software. There are chances that results may be affected differently by different software and hardware. A larger research is needed to explore effect of different sensors on iris recognition performance.

 ISBN: 978-1-61208-221-9

IV. Conclusion and Future Work

This review paper summarizes the issues and challenges with current iris biometric systems. In particular, we discussed security and performance related issues. We have shown that many popular beliefs about security, reliability, stability and performance of iris recognition systems are not correct and need to be revisited. The issues raised in this survey should be addressed in order to be more confident in working of iris recognition systems. In the future, we plan to explore the security and privacy concerns facing other biometric systems. This could lead to a design of multi-biometric system that overcomes the weaknesses of one by the strength of other biometric.

References

[1] J. Ali and A. Hassanien. An iris recognition system to enhance e-security environment based on wavelet theory. *AMO-Advanced Modeling and Optimization*, 5(2):93–104, 2003.

[2] S. Baker, A. Hentz, K. Bowyer, and P. Flynn. Contact lenses: Handle with care for iris recognition. In *International Conference on Biometrics: Theory, Applications, and Systems (BTAS)*, pages 1–8, 2009.

[3] S. Baker, A. Hentz, K. Bowyer, and P. Flynn. Degradation of iris recognition performance due to non-cosmetic prescription contact lenses. *Computer Vision and Image Understanding*, 114:1030–044, 2010.

[4] K. Bowyer, S. Baker, A. Hentz, K. Hollingsworth, T. Peters, and P. Flynn. Factors that degrade the match distribution in iris biometrics. *Identity in the Information Society*, 2(3):327–343, 2009.

[5] K. Bowyer, K. Hollingsworth, and P. Flynn. Image understanding for iris biometrics: A survey. *Computer Vision and Image Understanding*, 110(2):281–307, 2008.

[6] J. Bringer, H. Chabanne, and B. Kindarji. The best of both worlds: Applying secure sketches to cancelable biometrics. *Science of Computer Programming*, 74(1-2):43–51, 2008.

[7] J. Daugman. High confidence visual recognition of persons by a test of statistical independence. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 15(11):1148–1161, 1993.

[8] J. Daugman. How iris recognition works. *IEEE Transactions on Circuits and Systems for Video Technology*, 14(1):21–30, 2004.

[9] S. Dhavale. Robust iris recognition based on statistical properties of walsh hadamard transform domain. *International Journal of Computer Science*, 9, 2012.

[10] L. Dhir, N. Habib, D. Monro, and S. Rakshit. Effect of cataract surgery and pupil dilation on iris pattern recognition for personal authentication. *Eye*, 24(6):1006–1010, 2009.

[11] H. Feng and C. Wah. Private key generation from on-line handwritten signatures. *Information Management & Computer Security*, 10(4):159–164, 2002.

[12] J. Fierrez, J. Galbally, J. Ortega-Garcia, M. Freire, F. Alonso-Fernandez, D. Ramos, D. Toledano, J. Gonzalez-Rodriguez, J. Siguenza, J. Garrido-Salas, et al. BiosecurID: a multimodal biometric database. *Pattern Analysis & Applications*, 13(2):235–246, 2010.

[13] J. Fierrez, J. Ortega-Garcia, D. Toledano, and J. Gonzalez-Rodriguez. Biosec baseline corpus: A multimodal biometric database. *Pattern Recognition*, 40(4):1389–1392, 2007.

[14] F. Hao, R. Anderson, and J. Daugman. Combining cryptography with biometrics effectively. *University of Cambridge Computer Laboratory, Tech. Rep*, 2005.

[15] K. Hollingsworth, K. Bowyer, and P. Flynn. The importance of small pupils: a study of how pupil dilation affects iris biometrics. In *2nd IEEE International Conference on Biometrics: Theory, Applications and Systems, 2008. BTAS 2008.*, pages 1–6. IEEE, 2008.

[16] K. Hollingsworth, K. Bowyer, and P. Flynn. Pupil dilation degrades iris biometric performance. *Computer Vision and Image Understanding*, 113(1):150–157, 2009.

[17] K. Hollingsworth, K. Bowyer, and P. Flynn. Similarity of iris texture between identical twins. In *IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, pages 22–29. IEEE, 2010.

[18] K. Hollingsworth, K. Bowyer, S. Lagree, S. Fenker, and P. Flynn. Genetically identical irises have texture similarity that is not detected by iris biometrics. *Computer Vision and Image Understanding*, pages 1493–1502, 2011.

[19] M. Hosseini, B. Araabi, and H. Soltanian-Zadeh. Pigment melanin: pattern for iris recognition. *IEEE Transactions on Instrumentation and Measurement*, 59(4):792–804, 2010.

[20] S. Kanade, D. Camara, E. Krichen, D. Petrovska-Delacrétaz, and B. Dorizzi. Three factor scheme for biometric-based cryptographic key regeneration using iris. In *Biometrics Symposium, 2008. BSYM'08*, pages 59–64. IEEE, 2008.

[21] S. Kanade, D. Petrovska-Delacrétaz, and B. Dorizzi. Cancelable iris biometrics and using error correcting codes to reduce variability in biometric data. In *Computer Vision and Pattern Recognition, 2009. CVPR 2009. IEEE Conference on*, pages 120–127. IEEE, 2009.

[22] Y. Lee, K. Bae, S. Lee, K. Park, and J. Kim. Biometric key binding: Fuzzy vault based on iris images. In *2nd International Conference on Biometrics*, pages 800–808. Springer, 2007.

[23] I. Maghiros, Y. Punie, S. Delaitre, E. Lignos, C. Rodriguez, M. Ulbrich, and M. Cabrera. Biometrics at the frontiers: Assessing the impact on society. *Institute for Prospective Technological Studies, Technical Report EUR*, 21585, 2005.

[24] K. Miyazawa, K. Ito, T. Aoki, K. Kobayashi, and H. Nakajima. An effective approach for iris recognition using phase-based image matching. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 30(10):1741–1756, 2008.

[25] D. Monro, S. Rakshit, and D. Zhang. DCT-based iris recognition. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 29(4):586–595, 2007.

[26] F. Monrose, M. Reiter, Q. Li, and S. Wetzel. Cryptographic key generation from voice. In *Security and Privacy, 2001. S&P 2001. Proceedings. 2001 IEEE Symposium on*, pages 202–213. IEEE, 2001.

[27] K. Nandakumar, A. Jain, and S. Pankanti. Fingerprint-based fuzzy vault: Implementation and performance. *IEEE Transactions on Information Forensics and Security*, 2(4):744–757, 2007.

[28] M. Negin, T. Chmielewski Jr, M. Salganicoff, U. von Seelen, P. Venetainer, and G. Zhang. An iris biometric system for public and personal use. *Computer*, 33(2):70–75, 2000.

[29] S. Rakshit and D. Monro. Medical conditions: Effect on iris recognition. In *Multimedia Signal Processing, 2007. MMSP 2007. IEEE 9th Workshop on*, pages 357–360. IEEE, 2007.

[30] N. Ratha, S. Chikkerur, J. Connell, and R. Bolle. Generating cancelable fingerprint templates. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, 29(4):561–572, April 2007.

[31] N. Ratha, J. Connell, R. Bolle, and S. Chikkerur. Cancelable biometrics: A case study in fingerprints. In *Pattern Recognition, 2006. ICPR 2006. 18th International Conference on*, volume 4, pages 370–373, 2006.

[32] O. Song, A. Teoh, and D. Ngo. Application-specific key release scheme from biometrics. *International Journal of Network Security*, 6(2):127–133, 2008.

[33] A. Teoh and C. Yuang. Cancelable biometrics realization with multispace random projections. *Systems, Man, and Cybernetics, Part B: Cybernetics, IEEE Transactions on*, 37(5):1096–1106, 2007.

[34] J. Thornton, M. Savvides, and V. Kumar. A Bayesian approach to deformed pattern matching of iris images. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 29(4):596–606, 2007.

[35] J. Thornton, M. Savvides, and B. Vijayakumar. Robust iris recognition using advanced correlation techniques. *Image Analysis and Recognition*, pages 1098–1105, 2005.

[36] P. Tome-Gonzalez, F. Alonso-Fernandez, and J. Ortega-Garcia. On the effects of time variability in iris recognition. In *IEEE International Conference on Biometrics: Theory, Applications and Systems, (BTAS)*, pages 1–6. IEEE, 2008.

[37] Z. Wang, Q. Han, and C. Busch. A novel iris location algorithm. *International Journal of Pattern Recognitionand Artificial Intelligence*, 23(1):59, 2009.

[38] R. Wildes. Iris recognition: An emerging biometric technology. *PIEEE*, 85(9):1348–1363, September 1997.

[39] R. Wildes, J. Asmuth, G. Green, S. Hsu, R. Kolczynski, J. Matey, and S. McBride. A machine-vision system for iris recognition. *Machine Vision and Applications*, 9(1):1–8, 1996.

[40] G. Williams. Iris recognition technology. *IEEE Aerospace and Electronic Systems Magazine*, 12(4):23–29, 1997.

 ISBN: 978-1-61208-221-9

[41] S. Ziauddin and M. Dailey. Robust iris verification for key management. *Pattern Recognition Letters*, 31(9):926–935, 2010.
[42] J. Zuo, N. Ratha, and J. Connell. Cancelable iris biometric. In *Pattern Recognition, 2008. ICPR 2008. 19th International Conference on*, pages 1–4. IEEE, 2008.

 ISBN: 978-1-61208-221-9