International Journal of Information Processing, 8(4), 23-34, 2014
ISSN : 0973-8215
IK International Publishing House Pvt. Ltd., New Delhi, India

Protection of Iris Image using Secret Sharing Schemes

Maroti Deshmukh[a], Munaga V N K Prasad[b]

[a]Assistant Professor, Department of Computer Science and Engineering, National Institute of Technology, Uttarakhand-246174, India. Email: marotideshmukh100@gmail.com

[b]Associate professor, Institute for Development and Research in Banking Technology, Hyderabad-500046, India. Email: mvnkprasad@idrbt.ac.in

Preserving the iris image has become of prime importance since due to security threats iris image may be modified. To overcome this issue visual cryptography scheme can be applied to secure the iris image. In this paper a study of (k, n) visual secret sharing (VSS) for binary images and (n, n) VSS for binary and grayscale images has been done for iris authentication. In case of (k, n) VSS n shares are created and at least k or more than k shares are required to reveal the information. For (n, n) VSS n shares are created and all n shares are needed to reveal the information. A correlation technique is used for the decision of acceptance or rejection of superimposed images and to authenticate the user.

Keywords : Correlation, Normalization, Segmentation, Visual Secret Sharing.

1. INTRODUCTION

An iris biometric system is used to authenticate an individual using iris textural patterns. The most promising and significant feature in the eye image is iris. Iris is in the form of circular ring that contains many unique characteristics such as ridges, rings, zigzag, collarette, crypts, furrows, corona, arching ligaments, freckles *etc.*,.[1]-[5]. These patterns in the iris are unique to each individual. Inside the iris, there is a central dark circle known as pupil.

A biometric method has significant advantages over traditional password authentication systems. Traditional security systems depend on knowledge (*e.g.,* passwords and the personal identification numbers) and tokens (*e.g.,* keys and identity cards) which could be shared, lost or hacked [5,6]. The iris has unique features and a very complex structure.

A typical iris recognition system includes four steps: image acquisition, preprocessing, feature extraction and matching [7–9]. In image acquisition high quality eye images are captured with user cooperation. Preprocessing consists of three steps: segmentation, normalization and enhancement. The performance of iris recognition system is mainly dependent on the accuracy of iris segmentation. Iris segmentation is the process of locating the iris region in an acquired input eye image. Normalization is the process of converting annular region to rectangular *i.e.,* Cartesian to polar coordinate system. The normalized iris is enhance using contrast enhancement techniques. After enhancement, normalized iris features are extracted using Gabor filter. Matching can be done using hamming distance.

Image processing techniques can be applied to extract the unique iris patterns from the acquired image of an eye and generate biometric template, which can be stored in the iris database. The iris biometric template contains a mathematical representation of unique texture information stored in the iris, and allows comparisons to be made between individuals. When a user wishes to be identified by an iris recognition system, first it capture the eye image, and then iris region template is created. This template is then compared with the other templates stored in a database. If matching

Table 6
Correlation Between Secret Image (S) and Stacked Image (R) for (k, n), (n, n) and $(2, 2)$ VSS Scheme with $k = 2$ and $n = 4$

Stacked shares (R)	**Tzung-Her Chen [24]**	**Kai Hsiang Tsao [25]**	**Bhaskar Mondal [4]**	**Daoshun Wang [3]**	**Kafri Keren [15]**
R_1, R_2	0.5889	0.0138	-0.0045	0.0012	**1.0000**
R_1, R_3	0.5932	0.0061	0.0027	0.0122	-
R_1, R_4	0.5913	-0.0075	-0.0197	0.0063	-
R_2, R_3	0.5874	0.0044	0.0098	0.0075	-
R_2, R_4	0.5855	-0.0101	-0.0104	0.0027	-
R_3, R_4	0.5898	0.0039	-0.0023	-0.0096	-
R_1, R_2, R_3	0.7849	-0.0018	0.0035	0.0027	-
R_1, R_2, R_4	0.7829	-0.0015	-0.0017	0.0052	-
R_1, R_3, R_4	0.7874	0.0039	0.0078	0.0057	-
R_2, R_3, R_4	0.7814	0.0052	0.0012	-0.0086	-
R_1, R_2, R_3, R_4	**1.0000**	**1.0000**	**1.000**	**1.0000**	-

11. Shah Samir and Ross Arun. Iris Segmentation using Geodesic Active Contours, *IEEE Transactions on Information Forensics and Security*, 4(4):824–836, 2009.
12. Li Yung-Hui and Savvides Marios. An Automatic Iris Occlusion Estimation Method based on High-Dimensional Density Estimation, *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 35(4):784–796, 2013.
13. Radman Abduljalil, Jumari Kasmiran and Zainal Nasharuddin. Fast and Reliable Iris Segmentation Algorithm, *IET Image Processing*, 7(1):42–49, 2013.
14. Naor Moni and Shamir Adi. Visual Cryptography, *Advances in CryptologyEUROCRYPT'94*, pages 1–12, 1995.
15. Kafri Oded and Keren Eliezer. Encryption of Pictures and Shapes by Random Grids, *Optics letters*, 12(6):377–379, 1987.
16. Guo Teng, Liu Feng and Wu ChuanKun. K out of K Extended Visual Cryptography Scheme by Random Grids, *Signal Processing*, 94:90–101, 2014.
17. Chen Tzung-Her and Tsao Kai-Hsiang. Threshold Visual Secret Sharing by Random Grids, *Journal of Systems and Software*, 84(7):1197–1208, 2011.
18. Shyu, Shyong Jian. Image Encryption by Random Grids, *Pattern Recognition*, 40(3):1014–1031, 2007.
19. Wang Ran-Zan, Lan Yung-Ching, Lee Yeuan-Kuen, Huang Shih-Yu, Shyu Shyong-Jian and Chia Tsorng-Lin. Incrementing Visual Cryptography using Random Grids, *Optics Communications*, 283(21):4242–4249, 2010.
20. Ross Arun and Othman Asem. Visual Cryptography for Biometric Privacy, *IEEE transactions on information forensics and security*, 6(1):70–81, 2011.
21. Revenkar PS, Anjum Anisa and Gandhare WZ. Secure Iris Authentication using Visual Cryptography, *arXiv preprint arXiv:1004.1748*, 2010.
22. Mehrotra Hunny, Sa Pankaj K and Majhi Banshidhar. Fast Segmentation and Adaptive SURF Descriptor for Iris Recognition, *Mathematical and Computer Modelling*, 58(1):132–146, 2013.
23. Daugman John. How Iris Recognition Works, *IEEE Transactions on Circuits and Systems for Video Technology*, 14(1):21–30, 2004.
24. Chen Tzung-Her, Lee Yao-Sheng, Huang Wei-Lun, Juan Justie Su-Tzu, Chen Ying-Yu and Li Ming-Jheng. Quality-Adaptive Visual Secret Sharing by Random Grids, *Journal of Systems and Software*, 86(5):1267–1274, 2013.
25. Chen Tzung-Her and Tsao Kai-Hsiang. Visual Secret Sharing by Random Grids Revisited, *Pattern Recognition*, 42(9):2203–2217, 2009.

Maroti Deshmukh is currently the Assistant Professor, National Institute of Technology, Uttarakhand. He obtained his Bachelor of Technology from SGGSIET Nanaded. He received his Master of Technology in Information Technology from University of Hyderabad, Hyderabad.

Munaga V N K Prasad is a Associate Professor, Institute for Development and Research in Banking Technology, Hyderabad, India. During the past 15 years of his service at the Institute he has over 80 research publications in refereed International Journals and Conference Proceedings.