I J C T A, 9(40) 2016, pp. 557-562

Detection of Fake Iris by using Frame Difference and Reflection Ratio

Vijay Kumar Sinha, Anuj Kumar Gupta and Ravinder Khanna

ABSTRACT

Most of the work done in the area of Iris recognition systems emphasizes only on matching of the patterns with the stored templates. Security aspects of the system are still unexplored. The available security algorithms provide only some cryptographic solutions that keep the template database in a secret cryptographic form. Some recent works on fake Iris detection has done but they still lacking of efficiently detect whether an iris is real or scanned image / printed image or digital image of high resolution. We successfully worked on these security issues of present iris recognition system and enhanced the detection capabilities of fake iris images.We use natural motion detection algorithm for detection of natural eye movement (Blinking of eyes and left –right movements) and reflection detection algorithm to detect reflection from retina which not occurred in fake scanned images of iris. This enhanced significantly the performance of the system in terms of security and reliability. We successfully attained 99.98% accuracy at 5.2% threshold value at 10.5 cm distance from the Iris scanner. The result is 1.41% improved over the existing Xiaofu method for fake iris detection method. Further our method is able to detect and differentiate between a live and unconscious person which could not detected in the earlier methods. We used 2-D Fourier spectra with iris image quality assessment based upon reflection. Further we used motion detection based upon frame difference of iris images and reflection detection by using Gabor filter algorithm.

Keywords: Iris, Threshold, Enrollment, Encryption

I. INTRODUCTION

In 1949 J.H. Doggart [1] who was a British ophthalmologist wrote that every human has different iris pattern just like fingerprints. In 1953 F.H. Alder [2] proposed that iris unique features of human iris can be used as unique identification of a person. In 1980 L.Flom and A. Safir [3] patented the idea that iris can be used as human identifications. John Daugman [4] who developed the algorithm very first for identification and recognition of person based upon human iris. Although the iris recognition system is a very robust and reliable biometric identification system, but it can be failed by using fake scanned high resolution images of iris or digital images like the finger print biometrics delicacy. A number of efforts has be made by the researchers to overcome this security issue so that delicacy of iris images can be detected and prevented. Adam Czajka, *et al.* [5] proposed a pupil dynamics for iris liveness detection for distinction between live and fake artificial scanned iris images. They used linear and non linear support vector machines to classify the natural reaction and spontaneous oscillations. Xiaofu, *et al.* [6] proposed a new fake iris detection method based upon wavelet packet transform. They used wavelet packet decomposition method based upon wavelet packet transformation.

Eui Chul Lee, *et al.* [7] proposed a method of fake iris detection based on 3d structure of Iris pattern. They used Near Infra Red (NIR) illuminations attached on the left hand sides of iris camera, in which 3-d iris pattern could be shown distinctively. Sung Joo, *et al.* [8] proposed a multi feature based fake iris

* Research Scholar I.K.G. Punjab Technical University, Punjab, India, *E-mail: cecm.cse.vk@gmail.com*

** Professor, CGC-COE, Landran, I.K.G. Punjab Technical University Punjab, India, *E-mail: anuj21@hotmail.com*

*** Dean Research, MMU, Sadopur, Haryana, Punjab, India, *E-mail: ravikh_2006@yahoo.com*

detection method. They measure distinctive physiological multi features like reflection ratios of the iris of the sclera and thickness of the corneoscleral limbus.

Kang Ryoung Park, et al. [9] proposed a fake iris detection method by using Purkinje image. They calculated the theoretical positions and distances between the purkinje images based on the human eye model. B. Sabarigiri, et al. [10] proposed a counter measures against iris direct attacks by using fake images. They also proposed a method for liveness detection based on electroencephalogram (EEG). B. Sabarigiri, et al. [11] proposed fake iris images detection by counter measuring based on EEG. They used to improve the anti-spoofing ability of conservative biometrics based system. Chun-Wei Tan, et al. [12] proposed ocular and iris descriptors for fake iris image detection. They used a spoof detection approach to detect the fake iris images. Xiaofu He, et al. [13] proposed a new fake iris detection method based on wavelet packet transform. They decomposed the wavelet packet and extracted the features values to detect the fake iris images from real iris images. Daksha Yadav, et al.[14] proposed studied the effect of textured contact lenses on iris Recognition system in year 2013. James S. Doyle,et al. [15] proposed detection of textured contact lenses in iris recognition using BSIF Binarized Statistical Image Features in year 2015.

Irrespective of all advancements iris recognition system in order to making more secure the hazards of making fool of iris scanner are still a big issue. We can't implement it for critical financial transactions as a password of identification. As one can take a photo of iris by high resolution camera by some distance while taking a photo shoot and later can use the iris images for making scams.

We proposed a new and robust fake iris detection system in which natural blinking of both eyes, natural movements of both eyes and natural reflection of both eyes used as detection of fake iris.[16]

It is difficult to blink a fake scanned iris image like a live human iris. Again it is difficult to move the both iris in the same direction by the fake iris. Similarly it is difficult to reflection of light by fake iris like a real human iris. Our method is able to detect and differentiate between a live and dead or unconscious person by using blinking features of a live person which is not happened in a fake iris images.[17]

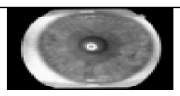
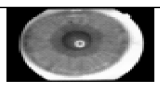
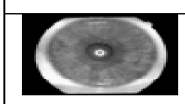
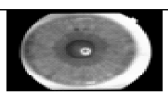
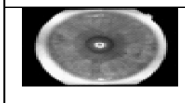
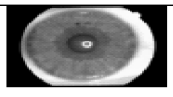
We used 2-D Fourier spectra with iris image quality assessment based upon reflection. Further we used motion detection based upon frame difference of iris images and reflection detection by using Gabor filter algorithm.[18]

II. PROPOSED ALGORITHM

2.1. Proposed Algorithm

Step 1: Start iris diagnosis, Step 2: Capture image, Step 3 :Test Flash Level, Step 4 : If Flash below level detect fake Iris and stop else proceed, Step 5: Test natural movement of Eye ball, Step 6 : If movement of

Table 1
Real Iris Images

Sl No.	Persons	Iris Images (Left Eye)	Iris image (Right Eye)	Distance from iris scanner	Threshold value	Natural Movement of Iris	Result
1	1st			11.6 cm	6.3	Yes	Real Human Iris
2				11.2 cm	6.3	Yes	Real Human Iris
3				10.3 cm	6.3	Yes	Real Human Iris

eye ball is not natural then detect fake iris image and stop else proceed, Step 7 : Conduct Template matching from stored database, Step 8 : Match left Iris with left iris template and right iris with right iris template, Step 9 : If Iris is matching then declare user identified and authorized else declare unidentifiedand unauthorized., Step 10 : Exit iris diagnosis

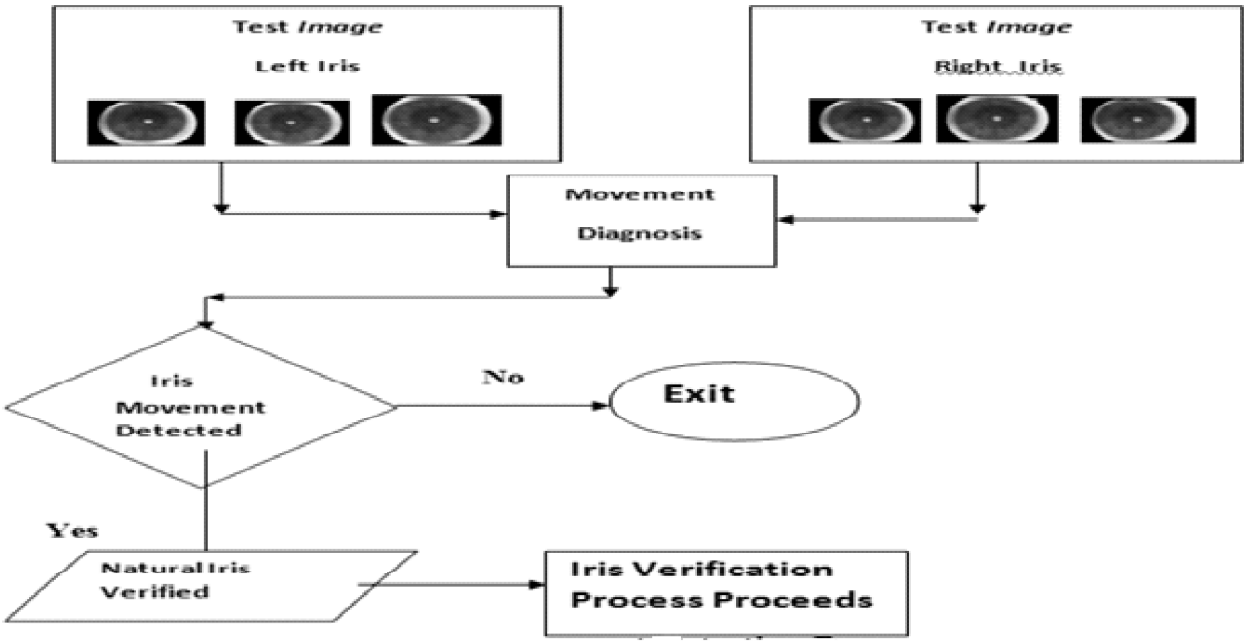


Figure 1: Iris Movement Detection Process

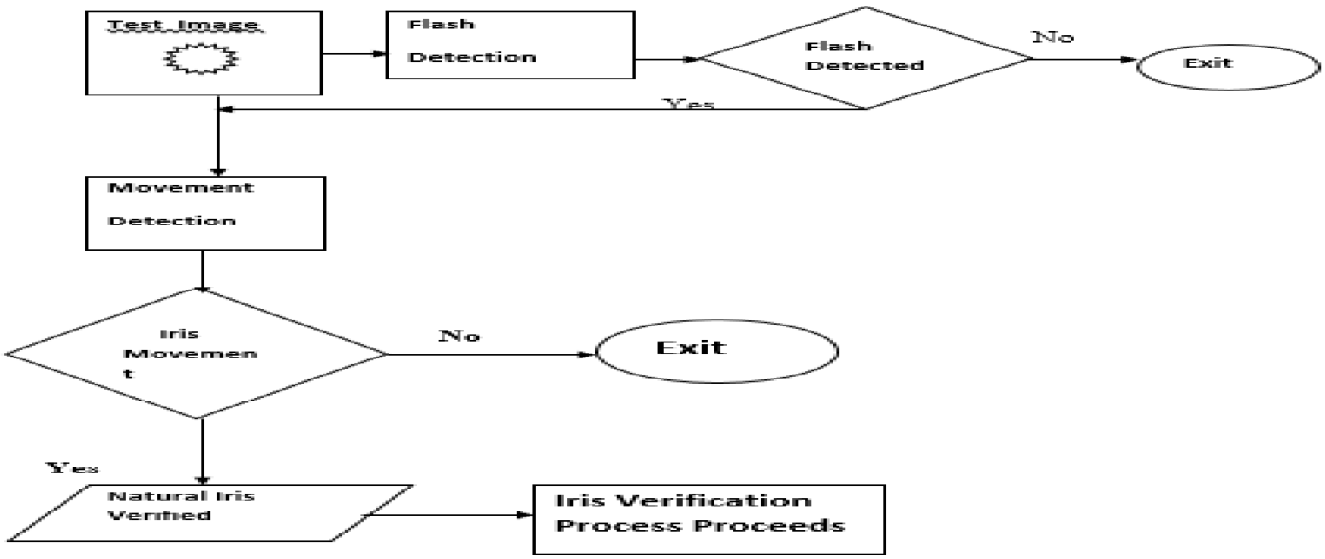


Figure 3: Iris Flash Detection and Movement Detection Process

2.2. Iris Verification Process

The next stage is the verification / identification process of the target person. After iris verification process will continue. For this, I propose to take iris samples of volunteers (randomly from those whose iris images are stored in the database as well as those whose iris images are not in the database).

Verification is proposed to be carried out in the following steps:

Firstly we conduct tests for the natural iris verification.

If iris lecture detected natural then we go for next step i.e. movement detection for a natural iris by using difference algorithm and threshold filters.

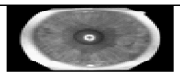
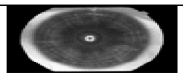
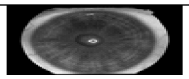
After movement verification process we proceed for the next iris verification process.

For this we repeat all the steps of iris enrollment process as described above i.e. : Iris Segmentation, Iris Normalization, Feature Extraction, Iris Template Generation, RS Decoding, Template Matching by using Hamming Distance and Weighted Euclidian Distance. This would be the template of the target person.

This template of the target person is then matched with the stored template in the database for verification / identification process.

Finally iris is declared matched if all the specified criteria are met otherwise declared not matched or false iris.

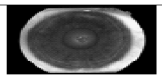
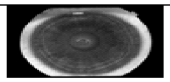
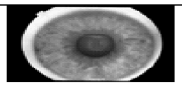
Table II
Real Iris Images

Sl No.	Iris Images	Distance from iris scanner	Threshold valuc	Flash Dctcction	Natural Movcmcnt of Iris	Result
1		10.5 cm	5.2	Yes	Yes	Real Human Iris
2		10.5 cm	5.2	Yes	Yes	Real Human Iris
3		10.5 cm	5.2	Yes	Yes	Real Human Iris

III. EXPERIMENT AND RESULT

The above algorithm is tested and analyzed on various iris templates. Fake scanned Iris detection accuracy. We use Flash and motion detection of natural eye. We successfully attained 99.98% accuracy at 5.2% threshold value at 10.5 cm distance from the Iris scanner.

Table II
Fake Scanned Iris Images

Sl No.	Fake Iris Images	Distance from iris scanner	Threshold value	Flash Detection	Natural Movement of Iris	Result
1		10.5 cm	5.2	No	No	Fake Human Iris
2		10.5 cm	5.2	No	No	Fake Human Iris
3		10.5 cm	5.2	No	No	Fake Human Iris

From the above both tables of Real and Fake scanned Iris Images we can conclude that the security algorithm introduced for Flash detection and natural movement detection are robust enough to detect and protect the system from scammers of fake users.

3.1. Comparison with Existing Method

Here, we will present a comparison between the current method and Daugman method and Xiaofu method Described for the purpose of comparison. We implement his method according

Table IV
Comparison of proposed system with Xiaofu method

Comparison of proposed system with Xiaofu method

	Xiaofu Method	*Proposed Flash Detection System*
Fake Detection Accuracy With Printed Clear Iris	98.57%	99.98
Fake Detection Accuracy With Printed Non-Clear Iris	98.18	99.24

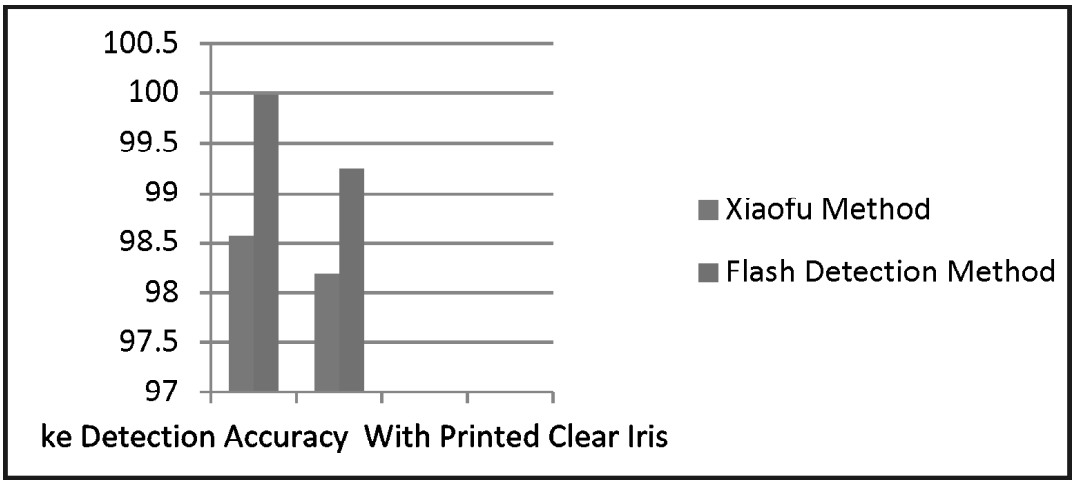


Figure 4: Comparison of proposed system with Xiaofu method

IV. CONCLUSIONS & FUTURE SCOPE

We successfully enhanced the detection of fake iris images and add the provision of detection of false of scanned iris images as fake templates. This enhanced significantly the performance of the system in terms of security and reliability. We use Flash and motion detection of natural eye. We successfully attained 99.98% accuracy at 5.2% threshold value at 10.5 cm distance from the Iris scanner. This research can be further expanded for the more accuracy level i.e. more than 99.98%. The distance can be enhanced which could be able to detect the fake iris for more than 10.5 cm distances. Further the threshold value can be reduced for higher degree of accuracy. This research can be expanded for working in low visibility conditions. This can also be expanded for the situations where person not stationary and moving with normal speed.

ACKNOWLEDGEMENTS

We thank the I.K.G. Punjab Technical University for the opportunity given us for the research in this critical area of Iris security which is the real demand of time. We also thank the Chandigarh Engineering College which motivate and facilitates us for this research in the field of Iris recognition system.

REFERENCES

[1] *Doggart, J.H., Ocular Signs in Slit-Lamp Microscopy*, Kimpton (1949), page 27.

[2] *Adler, F.H., Physiology of the Eye* (Chapter VI, page 143), Mosby (1953).

[3] *Leonard Flom, Aran Safir*: Iris recognition system. 28 August 1986; also: US 4641349 issued 2/3/1987.

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

[5] *Adam Czajka*, "Pupil dynamics for Iris Liveness detection ", IEEE, Vol 10,No. 4 April 2015.

[6] *Xiaofu He, Yue Lu and Pengfei Shi*, "A New Fake Iris Detection Method", Springer,pp. 1132-1139, ICB 2009.

[7] *Eui Chul Lee, Kang Ryoung Park*, "Fake Iris detection Based on iris Pattern ", Wiley Periodicals Inc, 2010.

[8] *Sung Joo Lee, Kang Ryoung Park, Youn Joo Lee, Kwanghyuk bae, Jaihie Kim* "Multifeature-based fake iris detection method", SPIE, Vol 46, No. 12, 2007.

[9] *Eui Chul Lee, Kang Ryoung Park, Jaihie Kim* "Fake Iris Detection by Using Purkinje Image ", Springer, Advances in Biometrics, Vol 3832,pp 397-403, 2006.

[10] *Xiaofu He* "A fake Iris detection Method Based on FFT and Quality assessment", IEEE, CCPR 2008.

[11] *B. Sabarigiri and D. Suganyadevi*, "Counter measures against Iris Direct Attacks using Fake images and Liveness detection Based on Electroencephalogram", World Applied Sciences Journal, Vol. 29., pp 93-98, 2014.

[12] *Chun-Wei Tan, Ajay Kumar*,"Integrating Ocular and Iris Descriptors for fake Iris Image Detection", IEEE, 978-1-4799-4370-8/14, 2014.

[13] *Xiaofu He, Pengfei Shi*, " Extraction of Complex Wavelet Features for Iris Recognition " IEEE, 978-1-4244-2175, 2008

[14] *Daksha Yadav, james S. Doyle, Richa singh*, Kevin W. Bowyer "Unraveling the effect of Textured contact lences on iris Recognition", IEEE, October 2013.

[15] *James S. Doyle,and Kevin W. Bowyer* "Robust detection of textured contact lences in iris recognition using BSIF ", IEEE, Vol 3, Oct 2015.

[16] Vijay Kumar Sinha, Dr. Ravinder Khanna and Dr. Manish Pandey, " ENHANCING SECURITY AND INTELLIGENCE OF IRIS RECOGNITION SYSTEM" IJSTM, Vol.-4, Issue -2, Sep. 2013.

[17] *Vijay Kumar Sinha, Dr. Ravinder Khanna and Dr. Manish Pandey*, "DETECTION AND FILTERATION OF FAKE IRIS IMAGES BY ANALYSING ITS DYNAMIC AND NATURAL MOVEMENT FEATURES", IJSTM, Vol. 3 Issue 3, July 2013.

[18] *Vijay Kumar Sinha, Dr. Anuj Gupta*, "Enhancing Iris Security by Detection of Fake Iris", National Conference Gyan Jyoti –National Conference MITE 2016.