An Enhanced IRIS Output Technique (EIOT) for Biometric Security

G. Elavarasi, M. Vanitha

Abstract: ***Human biometric features form the base for many security applications which identify humans uniquely. Human eyes and specifically the Iris based identifications are regarded as highly reliable systems. Iris based systems when combined with cryptography have been able to present higher biometric based security systems. This paper presents an Iris based human identification system called EIOT which can enhance biometric security. It is a set of unique sequential steps followed in Iris recognition and can be implemented in human authentications and identifications.***

Keywords**:** ***Biometric Security, Image processing, IRIS recognition, Sobel Filter, Human Authentication.***

I. INTRODUCTION

Biometric is a reliable and secure authentication tool and is automated approach which measures Physiological or behavioral human traits [1]. Physiological traits refers to DNA, hand and palm geometry, iris, face while behavioral human traits refer to gait, voice.etc., gait, and typing rhythm. Biometric have been applied in real world applications like border security, crime tracking, fraud prevention, access controls and generic identification of individuals [2] [3]. Biometrics are used in recognition as biometric properties cannot be easily duplicated or stolen, disclosed or misused unlike traditional authentications like passwords. Iris, a circular thin structure in the human eyes is a protected internal organ and does not get easily affected by environmental changes [4]. Iris based security solutions are one of the most promising due to its unique characteristics and reliability in a solution's lifetime when implemented. Even Twins who look alike on birth have different Iris combinations making this biometric dependable [5]. Recently, Iris recognition system (IRS) have been successfully applied to internet based authentications and countering global terrorism. Figure 1 depicts an Iris in the Human Eye.

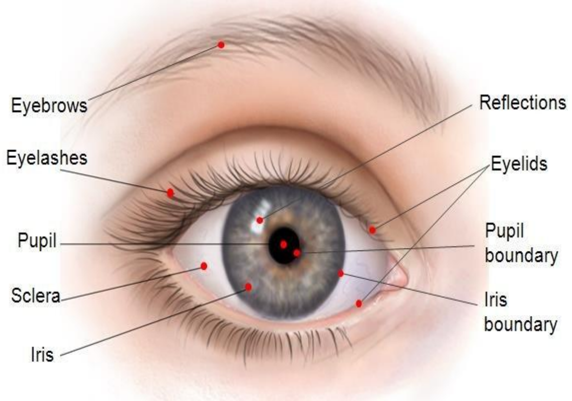

Fig. 1 – Human IRIS and Eye

An IRS acquires the image of a human eye, extracts Iris regions from the image and determines unique features that are stored and used for an individual's identification. The generic steps followed in IRS systems are depicted in Figure 2.

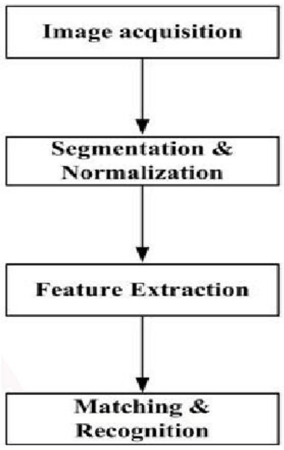

Fig. 2 – IRS Processing Steps

Several studies have reported the use of IRIS is biometric systems. The study in [6] implemented two dimensional Gabor wavelet filter for localizing the iris. Gaussian transforms were used for feature extraction and an iris code of 256 bits was used in computations. The study in [7] used an image acquisition interfaced to a Sun SPARC. An IRIS image was applied with Laplacian pyramid. Pattern matching was done using a hierarchical gradient-based registration algorithm. A novel fake iris detection method based on wavelet packet transform was proposed in [8]. Wavelet packet decomposition extracted attribute values for providing unique information. Accuracy of fake iris was detected using Support vector machine (SVM) which characterized the distribution boundary based on the extracted wavelet packet features. The study in [9] focused on segmentation and feature extraction in IRS.

Revised Manuscript Received on December 30, 2019.
***** Correspondence Author

Elavarasi. G*, Ph.D Research Scholar, Department of Computer Applications, Alagappa University, Karaikudi, India.

Dr.Vanitha. M, Assistant Professor, Department of Computer Applications, Alagappa University, Karaikudi, India.

Canny Edge Detector, a commonly used image processing tool was used for detecting edges robustly. This paper proposes a sequence of steps that can be followed in IRS systems for enhanced security and is called Enhanced IRIS Output Technique (EIOT). The Study in [10] proposed the visual cryptographic approach in High Definition and Very High Definition images without damaging its pixels. The encrypted data are only hidden in the least significant bits. Through this approach the sender can prevent the data access from unauthorized person and the receiver can safely access the sender's message.

II. ENHANCED IRIS OUTPUT TECHNIQUE (EIOT)

Biometric recognition systems automatically recognize individuals based on attributes extracted from eye/IRIS features. Any such system should provide a reliable recognition schema for identifying individuals. EIOT uses a sequence of steps that cab stored in a Database and retrieved while matching IRIS patters based on feature vectors. EIOT architecture is illustrated in Figure 3.

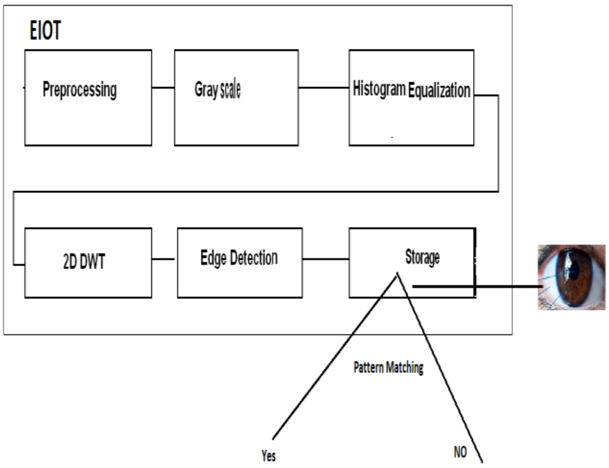

Fig. 3 – EIOT Architecture

The first step in EIOT is Image acquisition and Preprocessing. The image of the eyes is truncated and resized from the original image for lower dimensions. This image is then converted to gray scale. Since there may be impurities in the acquired image after gray scale conversion, Histogram Equalization is applied on the image for redistributing the image pixels and enhancing the overall quality of the image. Most significant features from the image are identified by using a two dimensional DWT. EIOT follows this step to minimize the processing time on images while obtaining a minimum reduction size of the acquired image. Since the IRIS is circular in nature, the edges have to be identified accurately. EIOT uses the Sobel method for its edge detection. On identifying the edges of the IRIS, the generated features are arranged into a feature vector before being sent to storage. Any IRS implementing EIOT and generating feature vectors can easily identify the person based on IRIS textures. One additional advantage of the EIOT is in encrypting the feature vector storage for disallowing unauthorized access while retrieving it from storage.

III. EIOT RESULTS

EIOT was tested on different IRIS images in an IRS. The visualized results of EIOT are presented for each step.

Step 1, 2 - Resizing and Gray Scale: Preprocessing is the first step in EIOT where the image is acquired and filtered to specify the boundaries of the iris image. This step minimizes noise in the image by resizing the original image and converted to gray scale and is depicted in Figure 4.

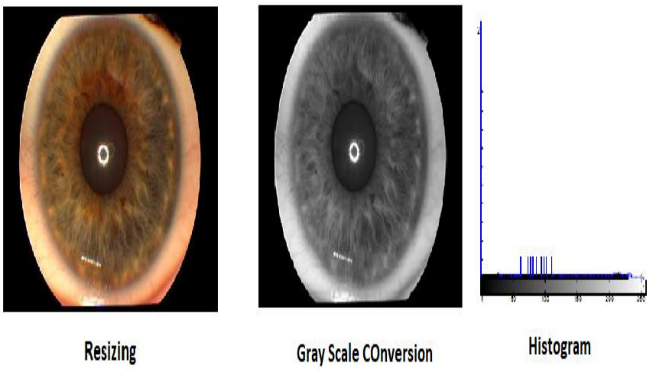

Fig. 4 – EIOT Preprocessing

Step 3 - Image Enhancement: EIOT follows image enhancement by using Histogram equalization for normalizing the image and then applying an adaptive Histogram to improve its equalization, depicted in Figure 5.

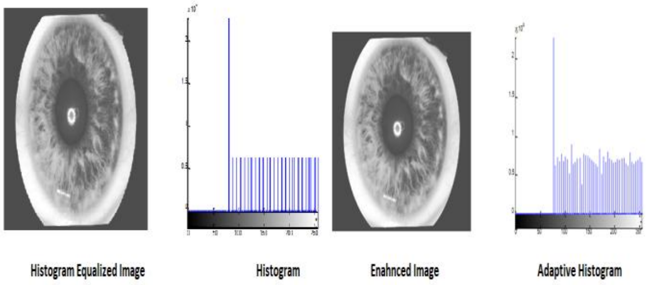

Fig. 5 – EIOT Image Enhancement

Step 4 – Feature Generation: 2D DWT is used by EIOT to generate specific features from the enhanced image of step 3. EIOT compresses the output image for generating minimum that are suitable pixels and depicted in figure 6.

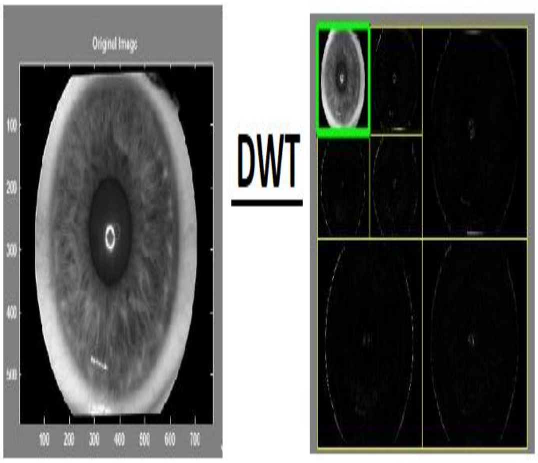

Fig. 6 – EIOT 2D DWT Output

Step 5 – Detecting Edges: EIOT uses Sobel operators for detecting IRIS edges and feature extractions. Figure 7 depicts the edge detected IRIS. Figure 8 depicts the feature vectors that are generated and stored in the database.

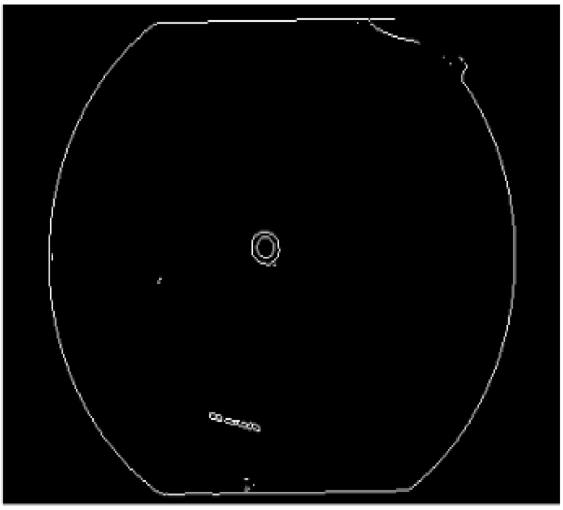

Fig. 7 – EIOT Detected IRIS Image

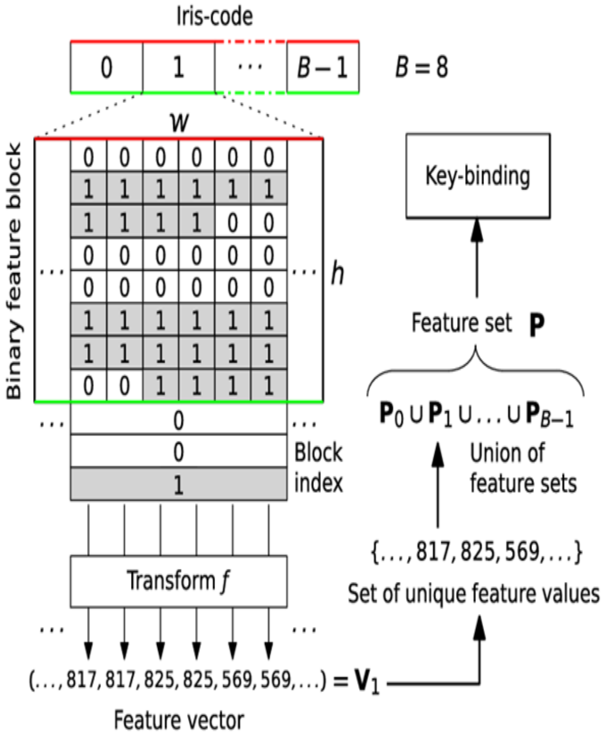

Fig. 8 – EIOT IRIS Feature Vectors

EIOT performance is better than others as shown in Table 1. Runtime of 50 iris templates in second was executed along with EIOT.

Table 1 - Comparison of classification-time EIOT with other techniques.

Methods	Time per attempt	Mean	Median
Features Extracted using PCA	5.5169 5.52865 5.5096 5.51725 5.5108 5.5233 5.52865	5.519307	5.51725
Feature Extraction Using Gabor Filter	7.67545 7.6248 7.6404 7.6454 7.62425 7.689 7.67505 7.66575	7.655013	7.655575
EIOT Feature Extraction	4.56625 4.55675 4.58025 4.61025 4.59845 4.56685 4.5991	4.582557	4.58935

It is evident from Table 1 that EIOT performs better than the compared techniques in its extraction of feature vectors and classifications based on feature extracted parameters.

IV. CONCLUSION

Iris is a physiological biometric feature that is used in biometric identification systems for high level of reliability. It can also be used in combination with cryptography. This paper has proposed and demonstrated with results a set of possible steps that can be implemented in IRS for faster and accurate identifications. It can be concluded that the proposed EIOT is implementable and reliable in IRS and moreover, its dimensionality reduction and feature vector storage helps in speedy matching of the IRIS in IRS.

V. ACKNOWLEDGMENT

This research work has been supported by RUSA PHASE 2.0, Alagappa University,Karaikudi.

REFERENCES

1. M. Pradhan, "Next Generation Secure Computing: Biometric in Secure E-transaction," International Journal of Advance Research in Computer Science and Management Studies, vol. 3, no. 4, pp.473-489, 2015.J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68-73.
2. Jin Ok Kim, Woongjae Lee, Jun Hwang, Kyong Seok Baik, Chin Hyun Chung, Lip print recognition for security systems by multi-resolution architecture, Future Gener. Comput. Syst. 20 (2) (2004) 295-301.
3. D. Maltoni, D.Maio. A.k. Jain, S. Prabhakar. Handbook of Fingerprint Recognition, Springer Verag, Berlin, Germany, 2003.

4. J. Trader, "M2SYS Blog On Biometric Technology," Delta ID, 11 June 2012.
5. J. G. Daugman, "High Confidence Visual Recognition of Persons," Ieee Transactions On Pattern Analysis And Machine Intelligence, vol. 15, 1993.
6. John G. Daugman, "High Confidence Visual Recognition of Persons by a Test of Statistical Independence", IEEE Trans. on Pattern Analysis and Machine Intelligence, 15(11), pp. 1148-1161, 1993. International Journal on Soft Computing (IJSC) Vol.2, No.4, November 2011
7. Wildes, R.P., Asmuth, J.C., et.al, "A System for Automated Iris Recognition", Proc. of the Second IEEE Workshop on Applications of Computer Vision, pp.121- 128, 1994.
8. Xiaofu He and et al," A New Fake Iris Detection Method", Department of Computer Science and Technology, East China Normal University, Shanghai 200241, China, 2009.
9. Bhawna chouhan, shailja shukla." Iris Recognition System using canny edge detection for Biometric Identification", Interrnational Journal of engineering Sciences and Technology (IJEST), ISSN: 0975-5462 Vol. 3 No. I Jan 2011.
10. Saranya P and Vanitha M (Jan 2018) “User Authorization With Encrypted Visual Cryptography Using High Definition Images”, International Journal of Pure and Applied Mathematics, Volume 118, No.8 2018,PP:429-433, ISSN:1314-3395 Impact Factor : 2.13