

Iris Image Authentication based on Adaptive Watermarking System

Dr. Methaq Talib Gaata^{#1}, Refah Aamer Jaafar^{*2}

Computer Science Department, University of Mustansiriyah
Baghdad, Iraq

Abstract— In recent years, biometric data play a key role in the identification and verification systems. With this significant progress in the use of biometric data many of the attacks that threaten the security and authenticity and integrity of biometric data itself emerged. For that, biometric data protection has become an urgent need for the purpose of protecting against fraud and alteration. This paper introduces an authentication approach to establish the authenticity of iris images based on adaptive watermarking system. The key idea is based on extract features from the iris image early and then uses these features as a watermark in order to insert into the same iris image. The fuzzy edge detector has been used to determining appropriate embedding locations and to avoid the region used during the iris recognition system. After avoid the region of interest (ROI) which used for iris recognition the Genetic Algorithm (GA) is used to find the optimal locations for watermark embedding in intelligently manner. The GA is applied in embedding and extracting the watermark. Also, original iris image does not require in watermark extraction process. Experimental results show the performance of proposed system is good enough to achieve the iris image authentication with very high quality and the embedding of watermark is not affected on the ROI which used in iris recognition.

Keywords — Adaptive Watermarking, Biometric, Iris, GA, Fuzzy.

I. INTRODUCTION

The identification systems aim to distinguish between an authorized person and else one who gets illegally the access right of an authorized person. Most identification systems used two main types of data in order to achieve its target include traditional token-based or biometric data. In current time, biometric data becoming progressively more accepted when compare with traditional data. Many reasons for popularity of biometric data are: impossible to stolen, replacing, falsify or borrowing. With a variety of commercially existing biometric applications such as fingerprint, facial information, iris, speech, ... etc. On other hand, the authentication and integrity of the biometric data represent big challenge to validation of biometric data and established new research issues [1].

Cryptograph and watermarking techniques can consider possible solution to guarantee the authentication and integrity of the biometric data. Cryptograph techniques provide high security level but require high time complexity and do not present any security level when the biometric data is decrypted. On the contrary that, watermarking techniques involves inserting watermarking data into the biometric data itself without degeneration to their information that are utilized during the identification process for authorized person. Therefore, it can provide authentication and integrity of the biometric data in addition to privacy and security level after decryption process. Consequently typically watermarking technique should be imperceptible, robust to unauthorized persons, able to detect of attempt to tamper with it and introduces authentication [2,3].

Digital watermarking can be consider one of the well-known approaches used to authentication and copyright protection for digital media such as documents, still images, speech, video, 3D objects, ... etc [4]. In literature, there are several kinds of watermarking techniques can be used to inserting watermark information securely into digital image. These techniques can divided into two main kinds are spatial domain and frequency domain. During spatial domain, the watermark information is inserted with trivial effect into the Least Significant Bits (LSB) of selected pixel in the host image. While in frequency domain, the host image should be transformed to frequency domain through one of available transformation such as the Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT) or any other transformation. Then, watermark information is inserted by changing the selected coefficients [5].

In recent years, some of research works appeared which are interested to protecting the authenticity of biometric data based on the digital watermark. Poonam et al [6] presented robust watermarking scheme for multimodal biometric images using intelligent approach which is Particle Swarm Optimization (PSO). The facial information of individual considered a watermark inserted into fingerprint image. Jinyu Lu et al [7] proposed novel watermarking scheme for iris biometric image in order to increasing the security of the iris biometric image. The host iris image is separated into four parts with same size. The watermark bits are inserted

within the singular values of each part coefficients after applied DCT.

This paper is arranged as the following manner: The proposed system is presented in Section II. Experiments and results are displayed in Section III. Section IV presented conclusions this paper.

II. PROPOSED SYSTEM

This system is designed to embed iris texture as watermark in iris image after avoid the regions that used for iris recognition based on fuzzy edge detector. In order to avoid the distortion that produced through inserting the watermark information into iris image that may be affected on the features regions which used in identification system. Therefore, the embedding locations should be selected adaptively based on features analysis. The block diagram of the proposed system is shown in Figure 1.

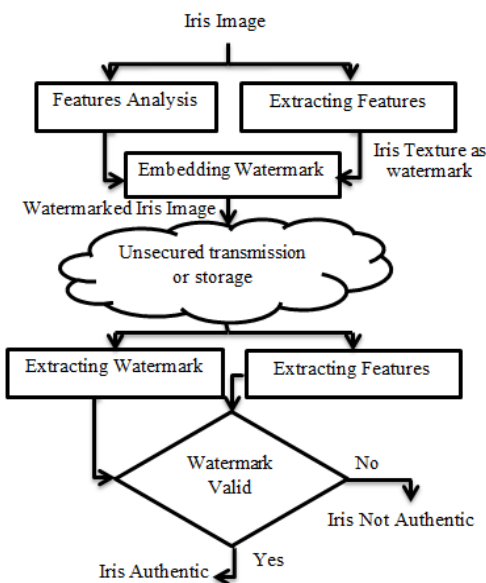


Fig. 1 The Block Diagram of the Proposed System

A. Features Analysis by Using Fuzzy edge detector

The fuzzy edge detection approach has been used to detect the edges area in iris image. The reason to use fuzzy approach is to solve the frequent trouble in traditional edge detectors is that sometimes the edges are not clear and opaque in nature.

Steps of edge detector by using fuzzy template as follows:

1. Choice a group of 16 fuzzy templates, each one of size 3 ×3, representing the probable directions of the edges of iris image.

$t1 = [a \ a \ a; \ 0 \ 0 \ 0; \ b \ b \ b];$ etc., (different templates).

where a, b, and 0 indicate the elements of the edge templates. The values of a and b are equal to 0.3 and 0.8 respectively. It has been selected trials to detect a good edge of iris image.

2. Initially the original iris image is normalized. All values will be in the interval of [0 1] this process achieved by the following equation:

$$A = (\text{element of the iris image}/\text{maximum pixel value}) \dots (1)$$

where A indicates the normalized iris image.

3. Apply the fuzzy edge templates over the output image from the previous step by putting the centre of each template over each pixel (i, j) of the normalized iris image.
4. The value of fuzzy divergence has been computed for both pixels in window and edge template of image (the size of window and template is equal) and then the min value selected.

$$\text{Div}(a_{ij}, b_{ij}) = [2 - (1 - u_A(a_{ij}) + u_B(b_{ij})) \cdot e^{u_A(a_{ij}) - u_B(b_{ij})} - (1 - u_B(b_{ij}) + u_A(a_{ij})) \cdot e^{u_B(b_{ij}) - u_A(a_{ij})}] \dots (2)$$

where A indicates the chosen window of the normalized iris image which is the similar size as the edge template, and B indicates the edge template. The $\mu_A(a_{ij})$ indicates the values of the image A and the $\mu_B(b_{ij})$ indicates the values of the template B.

5. Do again step 4 for each one of sixteen fuzzy templates.
6. Decide the max value from the minimum values of sixteen fuzzy divergence values.

$$\text{Div_measure}(i,j) = \max[\min(\text{Div}(A,B))] \dots (3)$$

7. Set the max value over element when the template is centered on the image.
8. Reapplied from step 4 to step 7 for all the image pixel coordinates.
9. Apply the threshold value of the divergence matrix at 0.17 to obtain an edge-detected iris image.

B. Extracting Features

In this section the iris texture is extracted to use as watermark information which will be unique for any individual instead of the traditional digital watermarking schemes which use a digital samples such as arbitrary numbers, logo, and symbols as the watermark.

Steps of extracting iris texture as a watermark as follows:

1. Reading the pixels of the Iris image from Iris database.
2. Convert the iris image to edge image by apply canny edge detector.
3. Using Circular Hough Transform (CHT) [8] to find the iris boundary and pupil boundary. In each edge point of edge image draws a set of circles of different radius in the accumulator space. These circles are defined by range of possible values of the radius and they are centred on the coordinates of the edge point. After assembly evidence of all the edge points, the maximum in the accumulator space

corresponds to the radius and centre of the iris and pupil circles.

4. Transform the iris region that lies between iris circle and pupil circle to rectangular block depends on Daugman's rubber sheet model. The Daugman's model is used to transform each Cartesian coordinates (x, y) of the iris ring to a polar coordinates (r, θ) , where $r \in [0, 1]$ and $\theta \in [0, 2\pi]$. To transform the iris ring (I) from Cartesian coordinates to the polar coordinates as follows:

$$I(x(r, \theta), y(r, \theta)) \rightarrow I(r, \theta) \quad \dots (4)$$

with

$$x(r, \theta) = (1 - r) \times x_p(\theta) + r \times x_i(\theta) \quad \dots (5)$$

and

$$y(r, \theta) = (1 - r) \times y_p(\theta) + r \times y_i(\theta) \quad \dots (6)$$

where x_p, y_p and x_i, y_i are the coordinates of each of the pupil and iris circles respectively.

5. This transformation will make each iris ring have the same fixed dimensions. The output of this transformation is the rectangular shape (iris texture) that represents the watermark information.

C. Embedding Watermark

Edges resulted from fuzzy edge detector are exclude during watermark embedding to avoid the region used for iris recognition, therefore the proposed system inserts watermark information (i.e. iris texture) into locations which not use in feature extraction operation (i.e. non-edges). After determining appropriate locations for watermark embedding, the GA is used in intelligently manner to find the optimized locations for embedding the watermark with least influence on the visual quality of the iris image.

The steps for applying GA into iris watermarking as follow:

1. The Non edges of iris image are divided into m of blocks; size of each block is equal to size of the watermark information. Each block represents a solution for embedding the watermark in iris image.
2. Execute the embedding procedure with all blocks one by one. Inserting the watermark information in the pixels of each block is done by changing the specific bit of pixels. This means that m of watermarked iris images will be produced.
3. Compute the PSNR value for all watermarked iris images.
4. Select the two blocks that achieve the best PSNR value.
5. End the training process if all blocks achieve the same PSNR value.
6. Apply crossover on the selected blocks and replace with two blocks have worst PSNR value.

7. Repeat from Step 2 to Step 7 until the condition is achieved.

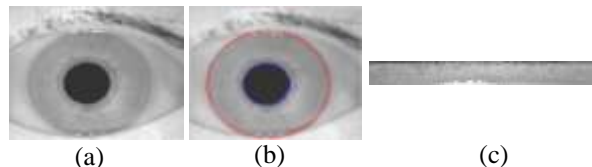
After termination of GA training, the optimized block is produced and used as embedding locations and these locations used as a secret locations in embedding and extraction processes. The size of watermark (iris texture) is 10×140 , each value in iris texture convert into 8-bit to generate bits stream as a watermark (i.e. 11200 bits) will be embedded in the optimized block. The watermark information embedded in optimized block by changing the specific bit of the pixels of optimized block. The output of embedding process is watermarked iris image.

D. Extracting Watermark

The steps of the extracting watermark are the same steps of the embedding watermark. The extracting watermark steps are implemented as follows: First, detect the edges area in watermarked iris image by using fuzzy edge detector. Second, using non-edges to extract the watermark information from the embedding locations depending on the secret locations that generated by using the GA as in the embedding watermark.

III. EXPERIMENTS AND RESULTS

In this section evaluation of the results which obtained during implementation of the proposed system. We are use gray "iris" image of size 280×320 as an original biometric image from the CASIA IrisV1 Database [9]. The watermark information is generated by using the proposed approach in this paper. The Figure 2 shows the



results of extract the iris texture as a watermark.

Fig. 2 Extract iris texture as a watermark

As shown in Figure 2, (a) present the iris image, (b) present determined iris and pupil circles in iris image and the (c) present the rectangular image of the iris ring image that used as a watermark.

The watermark information embedded in determined locations of non-edges of iris image. The edge-detected iris image is built by using fuzzy edge detector. The Figure 3 shows the original iris images with the corresponding edge images and watermarked iris image for each one.

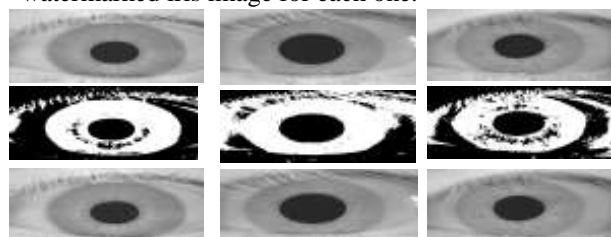


Fig. 3 Results of edge images and watermarked iris images

As seen in Figure 3, original iris images are presented in first row, the edge images are presented in second row and the watermarked iris images are presented in third row. The proposed system is providing high degree of transparency between original iris image and its watermarked iris image, because the embedding locations are selected by using GA with least influence on the visual quality of the iris image.

To determine the amount of distortion on the host iris image due to the proposed watermarking system, the Peak-Signal-to-Noise-Ratio (PSNR) [10, 11] of watermarked iris images is calculated. The results of PSNR are shown in Table 1.

Table 1
PSNR values of watermarked iris images

Watermarked Iris Images	PSNR Values
Sample 1	60.3768
Sample 2	60.2471
Sample 3	60.2243

As noted from results of PSNR values in Table 1, the proposed system has the good watermarked iris images quality although the capacity of watermark information is high. The reasons for that, the proposed system embedded the watermark information in locations which are achieving least influence on the visual quality of the iris image by using the GA.

For checking the watermarked iris image is authentic or not authentic, this is done through determining the validity of extracted watermark from watermarked iris image. The extracted watermark information from watermarked iris image compared with extracted features from watermarked iris image by computes the Tamper Assessment Function (TAF) [12], between extracted watermark information and extracted features by apply the equation as follows:

$$TAF(EW, EF) = \frac{\sum_{i=1}^{NW} (EW)_i \oplus (EF)_i}{NW} \dots (7)$$

where

TAF: The floats ratio between 0 and 1.

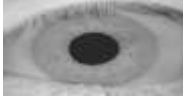

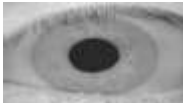

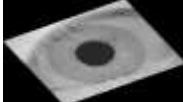





EW: Extracted Watermark.

EF: Extracted Features.

NW: Number of bits.

The TAF is floats ratio between 0 and 1, and among these values a certain threshold value can be set for discrimination between authentic or not authentic iris images. If the value of TAF is less than the threshold value (T=0.01), the iris image considered as authentic otherwise the iris image considered as not authentic. Table 2 show the TAF values of watermarked iris image without attack and with attacked.

Table 2
Values of TAF

Watermarked Iris Images	Extracted watermark	TAF	Decision
No attack 		0.003< T	Authentic
Add noise 		0.499> T	Not-Authentic
Rotation 		0.507> T	Not-Authentic
Scaling 		0.505> T	Not-Authentic
Fake Iris 		0.481> T	Not-Authentic

IV. CONCLUSIONS

In this paper, adaptive watermarking system for achieves the authentication of iris images is presented. The advantages of this system are the watermark information is embedded in such a way that the iris features that are used for iris recognition are not altered during the embedding watermark. As a consequence, the iris texture of watermarked iris images is very similar to that with original iris images. The proposed system has a good watermarked iris images quality although the quantity of watermark information is high.

REFERENCES

- [1] Abdullah MAM, Dlay SS, Woo WL. "Securing Iris Images with a Robust Watermarking Algorithm based on Discrete Cosine Transform" In: *10th International Conference on Computer Vision Theory and Applications (VISAPP 2015)*. 2015, Berlin, Germany.
- [2] S.Usha, M.Karthik, "A Robust Digital Image Watermarking for Biometric Template Protection Applications" *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering*, Vol. 4, Issue 4, April 2015.
- [3] Ajay Jangra and Shivi Goel, "Biometric based Security Solutions for MANET: A Review" *International Journal*

- Computer Network and Information Security*, Vol.10, pp. 44-50, 2013.
- [4] Rakhi C. Motwani, "A Voice-Based Biometric Watermarking Scheme For Digital Rights Management of 3D Mesh Models" Ph.D Thesis in in Computer Science and Engineering, University of Nevada, Reno, 2010.
 - [5] Methaq T. Gaata "An Efficient Image Watermarking Approach based on Fourier Transform" *International Journal of Computer Applications*, Vol. 136, No. 9, 2016.
 - [6] Punam Bedi, Roli Bansal, Priti Sehgal, "Multimodal Biometric Authentication using PSO based Watermarking" *Published by Elsevier Ltd. Procedia Technology* 4 (2012) pp. 612 – 618.
 - [7] Jinyu Lu, Tao Qu, and Hamid Reza Karimi, "Novel Iris Biometric Watermarking Based on Singular Value Decomposition and Discrete Cosine Transform" *Mathematical Problems in Engineering*, Vol. 2014.
 - [8] Marcin Smereka, Ignacy Dule, "CIRCULAR OBJECT DETECTION USING A MODIFIED HOUGH TRANSFORM" *International Journal of Appl. Math. Comput. Sci.*, Vol. 18, No. 1, pp. 85–91, 2008.
 - [9] CASIA IrisV1 Database. <http://biometrics.idealtest.org>.
 - [10] Z. Wang, A. Bovik, H. Sheikh and E.Simoncelli, "Image Quality Assessment: From Error Visibility to Structural Similarity," *IEEE Transactions on Image Processing*, vol. 13, no.4, pp. 600-612, April 2004.
 - [11] Sonam Chauhan, Sachin Chaudhary, " A Robust Invisible Digital Image Watermarking using DWT, DCT and SVD" *International Journal of Computer Trends and Technology (IJCTT) – volume 23 Number 3–May 2015*.
 - [12] Gaurav Gupta, Kanika Sharma, "A Hardware Efficient Robust Digital Image Watermarking Algorithm Using Integer DCT" *International Journal of Engineering Trends and Technology (IJETT) – Volume 25 Number 2- July 2015*.