Periodica Polytechnica Electrical Engineering and Computer Science, 63(4), pp. 263–273, 2019

Multi-Biometric Watermarking Scheme Based on Interactive Segmentation Process

Rasha Thabit[1*]

[1] Computer Techniques Engineering Department, Al-Rasheed University College, P. O. B. 6068, Al Jamaa, 10001 Baghdad, Iraq
[*] Corresponding author, e-mail: rashathabit@yahoo.com

Received: 17 April 2019, Accepted: 28 June 2019, Published online: 23 September 2019

Abstract

Iris-based security systems are highly recommended because of their security and ease of use. Different watermarking techniques have been presented to provide security while exchanging or storing iris images. The previous iris image watermarking techniques have successfully reached their aims, however, they suffer from some limitations such as the distortions that are presented in the iris region because of the watermark embedding process, the limited embedding capacity, and the lack of robustness against unintentional attacks. On the other hand, nowadays, the biometric-based security systems have directed their interest towards multi-biometric techniques in order to improve the performance of the individual's recognition process. This paper presents a new multi-biometric watermarking (MBW) scheme in which the features of the fingerprint image and some personal information are embedded in the iris image. To avoid the abovementioned limitations, the proposed scheme presents an interactive segmentation algorithm (ISA) and a Slantlet transform based watermark embedding method. The proposed ISA prevents any distortion in the iris region which is a beneficial feature for the iris image recognition process. The experimental results proved the efficiency of the proposed ISA in comparison with the Hough transform based methods in terms of accuracy, embedding capacity, and execution time. The proposed MBW scheme performs better in comparison with the state-of-the-art methods in terms of the intactness of the iris region, the robustness against unintentional attacks, and the watermark embedding capacity.

Keywords

digital information security, iris image watermarking, data hiding

1 Introduction

The security systems are required in many places such as companies, institutions, residential areas and others. Some security systems depend on passwords and user ID to control the access to these systems, however, these systems are susceptible to the risks of hacking, forgetting, and stealing [1]. Over the years, the technology of security systems has been directed towards the use of biometric-based identification methods because of their benefits in comparison with the previous methods. The use of biometric data is more convenient to the user because these data will always be carried by the user and therefore there is no fear of losing or forgetting them. The identification and authentication processes in biometric-based security systems rely on capturing and extracting the features of the personal traits such as the face, fingerprint, iris image, voice and others [2].

The biometric data are authentic but not secure because these data can be collected without user's knowledge, therefore, the biometric based security systems should guarantee that these biometrics are generated from a reliable source. A possible method for certifying the biometric equipment is to associate some additional information to the biometric data that are generated by it such as adding digital signature or logo [3]. This additional information should be invisible and joined to the biometric data and this can be accomplished by using watermarking techniques. The recent years witnessed an increased interest in the research of biometric watermarking techniques.

Iris-based biometric systems are highly recommended because of their security and ease of use [4], therefore, a number of watermarking schemes have been presented to protect iris images either by extracting the template of the iris image and embedding it in a cover image [5-7] or by embedding a watermark and secret data in the iris image [3, 8, 9]. In [10], a study has been conducted to

Cite this article as: Thabit, R. "Multi-Biometric Watermarking Scheme Based on Interactive Segmentation Process", Periodica Polytechnica Electrical Engineering and Computer Science, 63(4), pp. 263–273, 2019. https://doi.org/10.3311/PPee.14219

investigate the effect of the two scenarios that are mentioned above and it proved that, the second scenario in which the watermark is embedded in the iris image obtained better results in recognition performance, therefore, the research in this paper will focus on the second scenario.

In [3], an iris image watermarking algorithm has been presented based on embedding one bit of the watermark in a block of 8 × 8 discrete cosine transform (DCT) coefficients of the iris image. The scheme has robustness against different attacks. In [8], seven different watermarking algorithms [11-17] have been applied to iris images to study the effect of fragile watermarking on the iris image recognition process. The study proved that the watermarking process reduces the images' recognition performance significantly when the payload is high. In [9], another approach has been presented which depends on applying a fragile watermarking to embed a secret signature in the DCT coefficients of the iris image. Any change in the iris image will destroy the signature and thus the alteration can be easily detected. At the receiver side, the altered image is considered not authentic for the recognition process.

The above mentioned iris image watermarking techniques have reached their aims, however, they suffer from some limitations. The robust watermarking technique in [3] suffers from the limited capacity as well as the distortions that are presented in the iris region because of the watermarking process. In the fragile watermarking techniques [9, 11-17], the watermark does not have robustness against attacks and thus only standardized transmission channels and storage protocols can be used. In addition, the process of embedding the watermarks in an iris image will cause distortions in the iris region. Causing distortions in the iris region can affect the features of this region and consequently the iris image recognition performance will be affected.

On another side, recently, the interest has been directed towards multi-biometric systems [18] where multiple biometric traits are used to increase the efficiency of the individuals' recognition process. For instance, in [19] a face image has been used as a host image and some biometric features have been embedded in the image using fragile watermarking. In [20], another multimodal biometric system has been presented in which the individual's voice coefficients are embedded in the face image to increase the security and improve the accuracy of the recognition process.

From the above mentioned introduction one can conclude that, there is a need for an iris image watermarking technique that has robustness against unintentional attacks and simultaneously has no effect on the iris image recognition performance. In addition, presenting a multi-biometric watermarking system will be more efficient in practical applications. To meet these requirements, this paper presents a new multi-biometric watermarking scheme in which the iris image is used as the host image and the features of the fingerprint image and some additional personal information are used as the watermark. In the proposed scheme, an interactive segmentation process is suggested to ensure the intactness of the iris region and a robust watermarking method is applied to embed the watermark in the iris region. The following sections present: the details of the proposed multi-biometric watermarking (MBW) scheme in Section 2, the experimental results and their discussion in Section 3, and the conclusions of this paper in Section 4.

2 The proposed multi-biometric watermarking scheme

The quality of the iris region is very important for the process of features extraction as well the iris image recognition process [4], therefore, any iris image watermarking technique must guarantee that the distortion that is generated by the watermarking process has no effect on the features of the iris region. The proposed scheme in this paper suggests separating the iris region from the image and excluding it from the watermarking process in order to avoid any distortion in the iris region and thus there will be no effect on the features extraction and image recognition processes. An interactive segmentation process has been applied to separate the iris region from the image. The remaining part of the image will be used to carry the watermark. The proposed segmentation algorithm is explained in the following subsection. Then, the processes of embedding and extracting watermark bits are illustrated. Thereafter, the complete algorithms of the proposed multi-biometric watermarking scheme are elucidated.

2.1 The proposed interactive segmentation algorithm

The segmentation process of the iris region is an essential step in iris image recognition techniques, therefore, several researches have been presented to achieve an effective segmentation process [21-26]. One can think about adopting a previous segmentation process to select and separate the iris region in the proposed scheme, however, there are some limitations in the previous segmentation techniques which make them not convenient for the proposed watermarking scheme. In [21-24], the process of iris region segmentation is based on calculating the binary edge map of the iris image followed by the application of Hough transform to detect the circles in the image. These techniques work effectively for ideal iris images which have a circular or near circular iris boundaries. The advantage of these techniques is the low complexity which leads to fast execution of the algorithm. However, in case of non-ideal iris images, the assumption of circular boundaries can cause inaccurate segmentation and in some cases the algorithm may fail in localizing and segmenting the iris region [21].

For an effective iris image recognition process, several details (i.e., exact iris boundaries, the occluding eyelids, the reflections, and others) have to be taken into consideration to segment the iris region accurately. In [25], a smart predication model has been used to obtain the threshold value for eyelash and eyelid detection. Then, the area which contains the iris region is divided into four quarters and assumptions are applied to extract the details of the iris region. In [26], an effective iris image segmentation technique has been presented which is based on end to end deep neural network. The target of this technique is to segment the iris region from the low-quality image that is captured using smart phone. The techniques in [25-26] can work effectively for different iris images but they are at the cost of increasing the time complexity because of extracting several details from the iris region which are required for the iris image recognition process.

To implement a watermarking scheme that is suitable for the practical applications, we need a fast and efficient segmentation process. Adopting the Hough transform techniques [21-24] is at the cost of reducing the accuracy in selecting the iris region while adopting the techniques from [25-26] is at the cost of increasing the execution time. In the proposed watermarking scheme, there is no need to extract the details of the iris region because the segmentation process is required to select the outer boundary of the iris region and separate the selected region from the remaining part of the image. Therefore, this paper presents a new method to select and separate the iris region which is named as interactive segmentation algorithm (ISA).

The block diagram of the proposed ISA and the steps of the algorithm are shown in Fig. 1 and Table 1, respectively. The resultant images after executing the algorithm are shown Fig. 2.

In Section 3.3, the performance of the proposed ISA is compared with the Hough transform based segmentation in terms of iris region segmentation accuracy, embedding capacity, and execution time to prove the efficiency of the proposed algorithm.

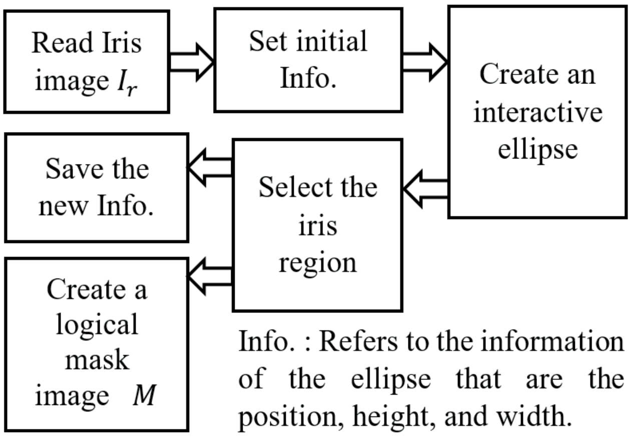

Read Iris image I_r
Set initial Info.
Create an interactive ellipse
Select the iris region
Save the new Info.
Create a logical mask image M
Info. : Refers to the information of the ellipse that are the position, height, and width.

Fig. 1 Block diagram for the proposed ISA

Table 1 The proposed interactive segmentation algorithm (ISA)

Input:	Iris image I_r .
Output:	Selected iris region and Mask image M .
Step 1:	Read and display the iris image I_r .
Step 2:	Set the initial position, height, and width for an ellipse.
Step 3:	Create an interactive ellipse using the initial information from step 2.
Step 4:	Drag the ellipse and adjust the size to select the iris region. Save the new position, height, and width in a vector V_e .
Step 5:	Read the size of the iris image and create a logical mask image M with the same size. The image M can be defined as follows: $M = \begin{cases} 1 & \text{for the corresponding pixels to the selected iris region} \\ 0 & \text{elsewhere} \end{cases}$

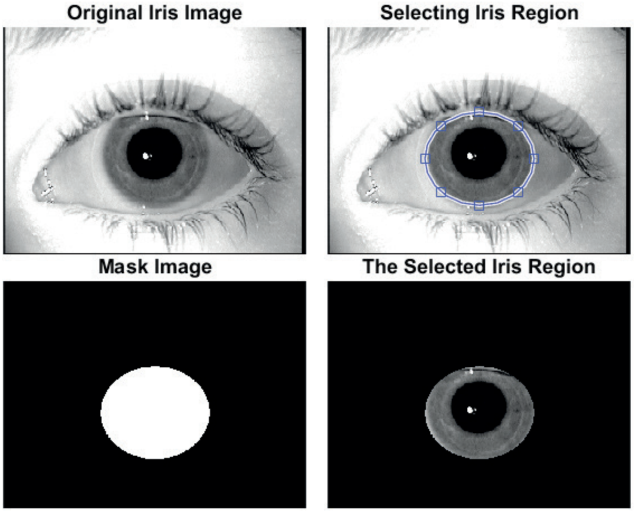


Fig. 2 The resultant images after executing ISA

2.2 The proposed watermark embedding and extraction process

The iris image watermarking scheme should have robustness against attacks especially the unintentional attacks such as channel noise and image compression which are unavoidable attacks in practical applications. On the other hand, the proposed scheme in this paper aims to hide the features of the fingerprint image in addition to some personal information, therefore, high embedding capacity is also required.

In recent years, different Slantlet transform (SLT) based watermarking schemes have been presented which proved their efficiency in terms of high embedding capacity, robustness against attacks, and high visual quality [27-28], therefore, a SLT-based watermarking algorithm is applied in the proposed MBW scheme. The procedures of the watermark embedding and extraction in an image block are explained in the following subsections.

2.2.1 Watermark embedding algorithm in an image block:

Input: Iris image block B_i of size $L \times L$, and sequence of bits S.

Output: The watermarked image block WB_i.

1. Apply SLT to transform input iris image block B_i using: $TB_i = SLT_L \quad B_i \quad SLT_L^T$ [27].
   Where B_i and TB_i are the original image block and the transformed block, respectively. SLT_L is the SLT matrix of size $L \times L$.
2. Select the horizontal (H) and vertical (V) subbands from the resultant SLT coefficients in TB_i as follows:
$$H = TB_i \left(\begin{matrix} x = 1, 2, \ldots, \left(\dfrac{L}{2} \right) \\ y = \left(\dfrac{L}{2} \right) + 1, \ldots, (L) \end{matrix} \right),$$
$$V = TB_i \left(\begin{matrix} x = \left(\dfrac{L}{2} \right) + 1, \ldots, (L) \\ y = 1, 2, \ldots, \left(\dfrac{L}{2} \right) \end{matrix} \right).$$
   Where x and y are the coordinates of the coefficients in TB_i. L is the side length of TB_i.
3. Initialize a counter $(C = 1)$ for the input sequence of bits S; set a threshold value (Thr) which is used to control the robustness and invisibility of the watermark.
4. Repeat
   - Take a bit from S and embed it by modifying the difference between one coefficient from H and one coefficient from V at the same coordinates. The modification rules are explained in details in [28].
   - Increase the counter $(C = C + 1)$
5. Until $C = \frac{L}{2} \times \frac{L}{2}$
6. Replace the original H and V subbands with the modified subbands then apply the inverse SLT using: $WB_i = SLT_L^T \quad TB_i \quad SLT_L$.
   Where WB_i is the watermarked image block.

2.2.2 Watermark extraction algorithm from an image block:

Input: The watermarked image block WB_i of size $L \times L$.

Output: The extracted sequence of bits ES.

1. Apply SLT to transform WB_i using: $TWB_i = SLT_L \quad WB_i \quad SLT_L^T$ [27].
   Where WB_i and TWB_i are the watermarked block and the transformed block, respectively.
2. Select the horizontal (H) and vertical (V) subbands from the resultant SLT coefficients in TWB_i as explained in the embedding algorithm (Section 2.2.1).
3. Initialize a counter $(C = 1)$ for the extracted sequence of bits ES and use the same Thr value that has been used at the embedding side.
4. Repeat
   - Set the extracted bit of ES to (1) when the coefficient in H is more than or equal to the coefficient in V at the same coordinates, otherwise the extracted bit is considered (0).
   - Increase the counter $(C = C + 1)$
5. Until $C = \frac{L}{2} \times \frac{L}{2}$

2.3 The procedures of the proposed multi-biometric watermarking scheme

The proposed watermarking scheme used two types of biometric data that are the iris image and the fingerprint image in order to provide security while storing or exchanging these biometric data. The complete algorithms for the watermark embedding and extraction procedures in the proposed MBW scheme are explained in the following subsections:

2.3.1 MBW embedding procedures:

1. Read the original iris image I_r and the fingerprint image F.
2. Apply the proposed ISA to select the iris region and create the mask image M. The vector V_e should accompany the watermarked image at the extraction side.
3. Divide the mask image into non-overlapping blocks of size (16×16) pixels as shown in Fig. 3 (a) then calculate the mean value of each block μB_i.
4. Classify the blocks into two groups according to the calculated mean values as follows:

$$\begin{array}{ll} \text{if } \mu B_i \neq 0 & \text{Then the block } B_i \in \text{iris region} \\ \text{if } \mu B_i = 0 & \text{Then the block } B_i \notin \text{iris region} \end{array}.$$

5. Divide the original iris image I_r into non-overlapping blocks of size (16×16) pixels and select the blocks that are not belong to the iris region as shown in Fig. 3 (b). The selected blocks are saved in a matrix called EB which is required for carrying the watermark bits. The total number of the selected blocks is calculated and saved as N_{EB}.
6. Read and prepare the watermark which consists of two parts. The first part of the watermark is the fingerprint features (i.e., ridges and bifurcation) that are generated using the software from [29] and the second part of the watermark is some personal information (such as the name, age, address, affiliation, …). The two parts of the watermark are saved and combined in one text file which is converted to a binary sequence called $BSeq$.
7. Calculate the total capacity TC of the selected blocks in EB as follows:

$$TC(bits) = N_{EB} * 64.$$

Where each block in EB of size (16 × 16) can carry 64 bits.

Then compare TC with the total number of bits in $BSeq$ as follows:

$$\begin{array}{l} \text{if } TC \geq \text{length}(BSeq) \\ \quad \text{Then continue to the next steps} \\ \text{if } TC < \text{length}(BSeq) \\ \quad \text{Then stop the execution of the algorithm.} \end{array}$$

If the total capacity is not enough for embedding the watermark, a message is sent to the user notifying him/her on the limitation in the embedding capacity.

8. Apply pixel adjustment process for the blocks in EB when necessary to avoid overflow/underflow as follows:

$$MEB_i(x,y) = \begin{cases} 3, & \text{if } EB_i(x,y) \leq 2 \\ 252, & \text{if } EB_i(x,y) \geq 253 \end{cases}.$$

Where EB_i and MEB_i are the embedding block and the modified embedding block, respectively. The (x,y) are the coordinates of the pixel in the processed block.

9. Divide $BSeq$ into non-overlapping consecutive subsets of 64 bits and apply watermark embedding process as follows:
   - Take one block MEB_i where $i = 1$ to N_{EB} and one subset from the binary sequence.
   - Apply the watermark embedding algorithm from (Section 2.2.1) to embed the subset in MEB_i.
   - Continue embedding subsets until the end of $BSeq$.

Save the watermarked blocks in WEB.

10. Replace the original blocks of the iris image (EB) by the watermarked blocks (WEB) to obtain the watermarked iris image.

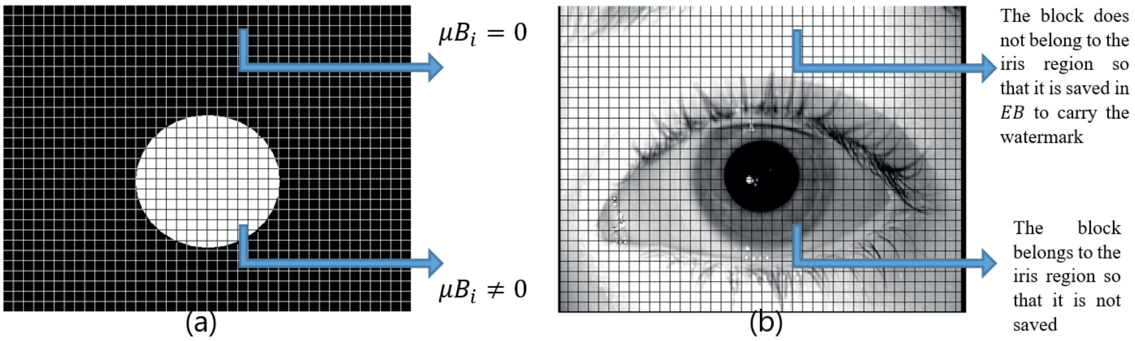

$\mu B_i = 0$
$\mu B_i \neq 0$
(a)
(b)
The block does not belong to the iris region so that it is saved in EB to carry the watermark
The block belongs to the iris region so that it is not saved

Fig. 3 (a) Dividing the mask image, and (b) Selecting the blocks of the iris image that are not belong to the iris region.

2.3.2 MBW extraction procedures:

1. Read the watermarked iris image and the vector V_e; then, display the image and draw an ellipse to select the iris region according to the information in V_e as shown in Fig. 4.
2. Create a logical mask image M as shown in Fig. 4 using the rules that have been explained in Table 1 (step 5).
3. Divide the mask image M into non-overlapping blocks of size (16×16) pixels and calculate the mean value of each block μB_i in order to classify the blocks as explained in (Section 2.3.1).
4. Divide the watermarked iris image into non-overlapping blocks of size (16×16) pixels. Then select the blocks that are not belong to the iris region and save them in a matrix called WEB.
5. Apply the watermark extraction algorithm to extract the embedded data from WEB as explained in (Section 2.2.2).
6. Rearrange the extracted binary bits to obtain the binary sequence $BSeq$. Then convert $BSeq$ to a text file to recover the original fingerprint features and the personal information.

3 Experimental results and discussion

This section explains the experiments and their results for different iris images that have been collected from [30] and [31] in order to evaluate the performance of the proposed MBW scheme. The following subsections elucidate the experiments that have been conducted to test the visual quality and capacity. The final subsection presents a general comparison between the proposed MBW and the state-of-the-art iris image watermarking methods. The SLT-based watermarking methods proved their efficiency in terms of robustness as explained in [27-28], therefore, the robustness test is not repeated in this research paper.

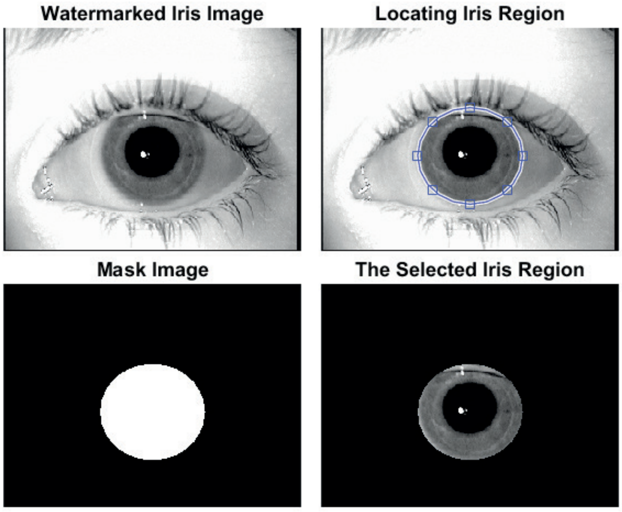
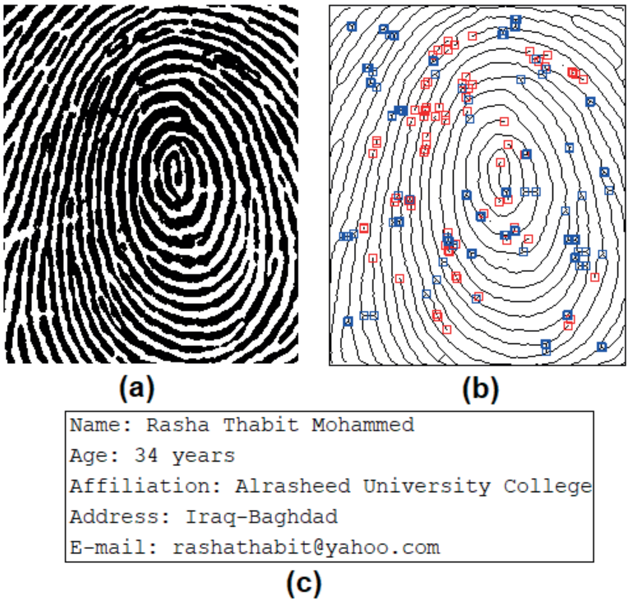


Fig. 4 Locating the iris region in the watermarked image and creating the mask image.

3.1 Visual quality test

To test the visual quality of the watermarked iris images, a sample fingerprint image and some personal information have been used which are shown in Fig. 5. In practical application, the iris image, fingerprint image, and the personal information should be collected from the same individual. The features of the sample fingerprint image and the personal information have been combined in one text file and converted to binary sequence ($BSeq$) as explained in (Section 2.3.1). The number of bits in $BSeq$ for the chosen samples is (13424 bits).

The proposed scheme does not cause any distortion in the iris region because this region has been excluded from the embedding process by applying the proposed ISA, however, the overall visual quality of the watermarked iris images is still important to prevent arousing suspicion about the contents of the image. Several experiments have been conducted to test the visual quality of the watermarked iris images and samples of the obtained results at threshold value (Thr = 3 as an example) are illustrated in Fig. 6. The Peak Signal-to-Noise Ratio (PSNR) between the original iris images and the watermarked images has been calculated and shown beneath each watermarked



Name: Rasha Thabit Mohammed
Age: 34 years
Affiliation: Alrasheed University College
Address: Iraq-Baghdad
E-mail: rashathabit@yahoo.com

Fig. 5 (a) sample fingerprint image, (b) the features of the fingerprint image, and (c) sample text file contains personal information.

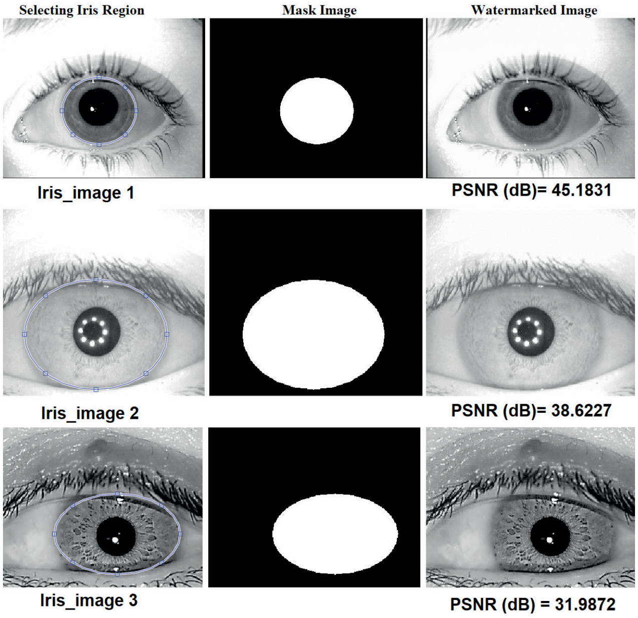


Fig. 6 Samples of the watermarked iris images after embedding *BSeq* of length (13424 bits).

image. Table 2 contains the PSNR (dB) values for the test images shown in Fig. 6 at different *Thr* values. The results proved that the higher the *Thr* value the lower the visual quality of the watermarked iris images.

3.2 Embedding capacity test

The capacity of the proposed multi-biometric watermarking scheme is affected by two main factors that are the size of the iris image and the size of the selected iris region. The capacity has been tested for iris images that have the same size but different iris regions as shown in Fig. 7. The results proved that (at the same image size) the larger the selected iris region the lower the capacity. Fig. 8 shows the results of testing capacity for different iris images at different sizes. The results proved that the larger the size of the iris image the higher the capacity.

Table 2 Visual quality results at different threshold values (*Thr*) and *BSeq* (13424 bits)

(*Thr*)	Iris_image 1 (480 × 640) pixels	Iris_image 2 (280 × 320) pixels	Iris_image 3 (240 × 320) pixels
2	45.5258	38.9794	32.2690
3	45.1831	38.6227	31.9872
4	44.8009	38.2512	31.8897
5	44.3831	37.8606	31.6975
6	43.9545	37.4626	31.4998

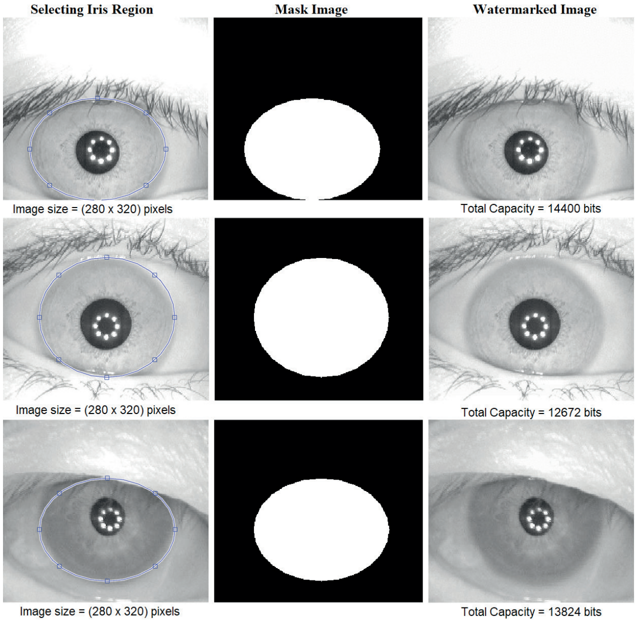

Selecting Iris Region
Mask Image
Watermarked Image
Image size = (280 x 320) pixels
Total Capacity = 14400 bits
Image size = (280 x 320) pixels
Total Capacity = 12672 bits
Image size = (280 x 320) pixels
Total Capacity = 13824 bits

Fig. 7 Capacity test for iris images that have the same size and different iris regions.

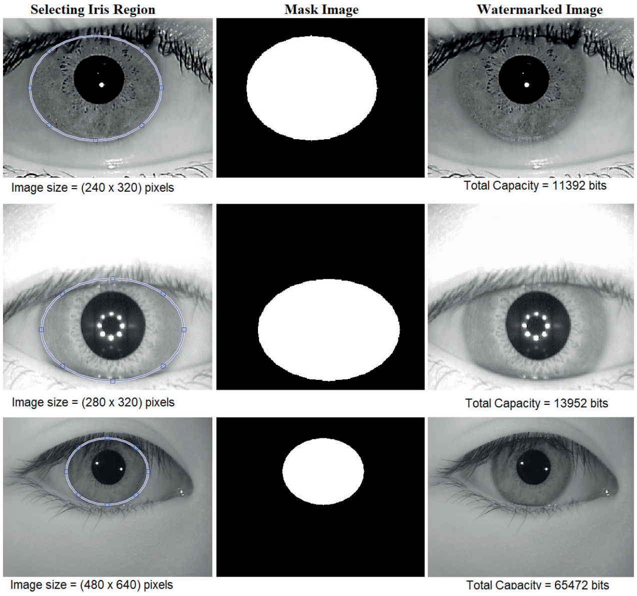

Selecting Iris Region
Mask Image
Watermarked Image
Image size = (240 x 320) pixels
Total Capacity = 11392 bits
Image size = (280 x 320) pixels
Total Capacity = 13952 bits
Image size = (480 x 640) pixels
Total Capacity = 65472 bits

Fig. 8 Capacity test for different iris images.

3.3 Comparison with the state-of-the-art methods

This section presents the comparisons of the proposed MBW scheme with the state-of-the-art methods. The first subsection illustrates the experiments that have been conducted to evaluate the performance of the proposed segmentation algorithm (ISA) in comparison with the Hough transform based segmentation [21-24]. The second subsection presents a general comparison between the proposed MBW scheme and the schemes in [3, 9, 11-17].

3.3.1 Performance evaluation of ISA

The proposed algorithm has been implemented in MATLAB (R2017a) and the computer properties are 1.80 GHz Intel® core TM i7 CPU and 16 GB memory. To compare the performance of ISA with Hough transform based segmentation [21-24], the algorithms have been applied for ideal and non-ideal iris images from CASIA iris image database [30]. Samples of the experimental results are shown in Fig. 9 which proved that the proposed ISA is more accurate in segmenting the iris region than the Hough transform based segmentation. The embedding capacity for the test images from Fig. 9 (a)-(c) has been calculated and is shown in Table 3. The results proved that the proposed ISA obtained higher embedding capacity in comparison with the Hough transform segmentation method.

As shown in the results, there are two cases of inaccurate segmentation as follows:

1. Case 1: part of the iris region is left outside the segmented region; in this case, distortions are generated in the iris region because of the watermark embedding process.
2. Case 2: the segmented iris region is larger than its actual size; in this case, the embedding capacity is reduced.

The execution time has been calculated for the test images from Fig. 9 (a)-(c) using tic toc commands in MATLAB and the comparison results are shown in Table 4. The results proved that, the proposed ISA performs better than the Hough transform based segmentation in terms of execution time.

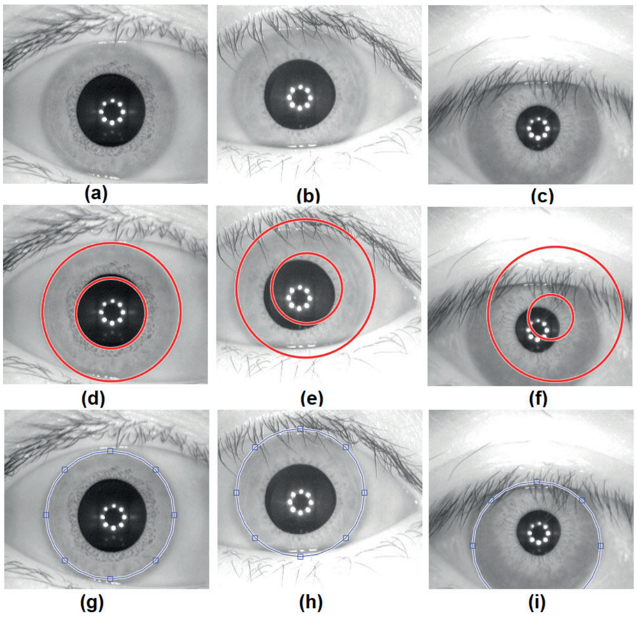


Fig. 9 Segmentation comparison for ideal and non-ideal iris images, (a)-(c) are the original iris images, (d)-(f) segmentation results using Hough transform, (g)-(i) segmentation results using ISA

Table 3 Comparison of embedding capacity using ISA and Hough transform segmentation

Iris image	Image size in pixels	Capacity (bits) using Hough transform	Capacity (bits) using ISA
Fig. 9 (a)	280 × 320	10880	12608
Fig. 9 (b)	280 × 320	11008	12544
Fig. 9 (c)	280 × 320	11776	14144

3.3.2 Performance evaluation of MBW

The characteristics of MBW scheme can be summarized as follows:

1. The scheme used multiple biometric traits (i.e., iris image and fingerprint image) thus the efficiency of the individuals' recognition process can be improved.
2. The scheme ensures the attachment of the personal information with their related traits by hiding the personal information and the features of the fingerprint image in the iris image for the same individual.
3. The scheme ensures the intactness of the iris region by excluding it from the watermark embedding process using the proposed ISA.
4. The scheme used an efficient interactive segmentation algorithm to select and separate the iris region.
5. The scheme has robustness against attacks, which makes it more efficient in practical applications.

Table 5 shows a general comparison between the proposed MBW scheme and the schemes in [3, 9, 11-17]; where the schemes [11-17] have been applied to iris images in the study that have been presented in [8], therefore, the comparison here depends on the performance of these schemes in [8].

Table 4 Comparison of execution time (ET) using ISA and Hough transform segmentation

Iris image	Image size in pixels	ET (sec) using Hough transform	ET (sec) using ISA
Fig. 9 (a)	280 × 320	4.0979	3.2681
Fig. 9 (b)	280 × 320	3.9028	2.1606
Fig. 9 (c)	280 × 320	5.0480	4.6234

Table 5 Comparison between the proposed MBW scheme and the state-of-the-art methods

Scheme	Embedding Domain	Embedding Technique	Intactness of iris region	Robustness	Multi-biometric
Tian, 2003 [12]	Spatial	Difference expansion (DE)	Distortions in iris region	Fragile	×
Yang et al., 2004 [16]	Transform	DCT bits shifting	Distortions in iris region	Fragile	×
Celik et al., 2005 [11]	Spatial	Least Significant Bit (LSB)	Distortions in iris region	Fragile	×
Lee et al., 2007 [17]	Transform	Integer discrete wavelet transform (IDWT)	Distortions in iris region	Fragile	×
Weng et al., 2008 [14]	Spatial	Modified difference expansion	Distortions in iris region	Fragile	×
Sachnev et al., 2009 [13]	Spatial	Expanding prediction-error differences	Distortions in iris region	Fragile	×
Li et al., 2010 [15]	Spatial	Shifting histogram of adjacent pixel differences	Distortions in iris region	Fragile	×
Abdullah et al., 2015 [3]	Transform	DCT interchanging coefficients	Distortions in iris region	Robust	×
Czajka et al., 2016 [9]	Transform	DCT and LSB	Distortions in iris region	Fragile	×
Proposed MBW scheme	Transform	Slantlet transform (SLT)	No distortions in iris region	Robust	✓

As shown in Table 5, the proposed scheme performs better than all the compared schemes in [3, 9, 11-17] in terms of intactness of the iris region which is an essential property to avoid affecting the features of the iris region and consequently there will be no effect on the recognition performance. In terms of robustness, the proposed scheme performs better than the schemes in [9, 11-17]. In comparison with the robust scheme in [3], the proposed scheme performs much better in terms of capacity because each block from the iris image of size (16 × 16) pixels can carry 4 bits using the scheme in [3] while the block of the same size can carry 64 bits using the proposed scheme.

4 Conclusion

This paper presents a new multi-biometric watermarking scheme in which the features of the fingerprint image and some personal information are embedded in the iris image. The intactness of the iris region has been ensured by applying interactive segmentation algorithm (ISA) which selects and separates the iris region to exclude it from the watermark embedding process. The performance evaluation of ISA proved its efficiency in comparison with the Hough transform segmentation method. The experimental results that have been conducted to evaluate the proposed MBW scheme illustrate that the visual quality of the watermarked images depends on the threshold value which is a factor used in the embedding process to control the robustness and invisibility of the watermark. The watermarked images obtained good visual quality at different threshold values. The embedding capacity of the proposed scheme depends on two factors that are the size of the iris image and the size of the selected iris region. As illustrated in the results, the larger the iris image the higher the embedding capacity, while for the images with the same size, the larger the selected iris region the lower the embedding capacity. The comparisons of the proposed scheme with the state-of-the-art methods proved its efficiency in terms of the intactness of the iris region, robustness against attacks, and the watermark embedding capacity. The main contribution of this work can be summarized as follows:

1. The use of multiple biometric data (i.e., iris image and fingerprint image) will be more beneficial in practical applications that are related to the individuals' recognition process.
2. The use of the proposed ISA contributes in ensuring the intactness of the iris region by effectively segmenting this region.
3. The use of the proposed SLT based watermarking algorithm contributes in improving the performance of the scheme in terms of robustness and embedding capacity.

The future work can proceed to present the hardware implementation for the proposed MBW scheme.

References

[1] Bowyer, K. W., Hollingsworth, K., Flynn, P. J. "Image understanding for iris biometrics: A survey", Computer Vision and Image Understanding, 110(2), pp. 281–307, 2008.
https://doi.org/10.1016/j.cviu.2007.08.005

[2] Jain, A. K., Bolle, R. M., Pankanti, S. "Biometrics: Personal Identification in Networked Society", Springer US, New York, USA, 2006.
https://doi.org/10.1007/978-0-387-32659-7

[3] Abdullah, M. A. M., Dlay, S. S., Woo, W. L. "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), Vol. 3, Berlin, Germany, 2015, pp. 108–114. https://doi.org/10.5220/0005305701080114

[4] Bowyer, K. W., Hollingsworth, K. P., Flynn, P. J. "A Survey of Iris Biometrics Research: 2008–2010", In: Burge, M., Bowyer, K. (eds.) Handbook of Iris Recognition, Advances in Computer Vision and Pattern Recognition book series, Springer-Verlag, London, UK, 2013, pp. 15–54. https://doi.org/10.1007/978-1-4471-4402-1_2

[5] Mostafa, E., Mansour, M., Saad, H. "Parallel-Bit Stream for Securing Iris Recognition", International Journal of Computer Science Issues, 9(3), pp. 347–351, 2012. [online] Available at: http://www.ijcsi.org/articles/Parallelbit-stream-for-securing-iris-recognition.php [Accessed: 01 April 2019]

[6] Lu, J., Qu, T., Karimi, H. R. "Novel Iris Biometric Watermarking Based on Singular Value Decomposition and Discrete Cosine Transform", Mathematical Problems in Engineering, 2014, article ID: 926170, 2014. https://doi.org/10.1155/2014/926170

[7] Hima bindu, B. A., Saraswati, V. "Watermarking of digital images with iris based biometric data using wavelet and SVD", International Journal of Engineering Development and Research (IJEDR), 4(1), pp. 726–731, 2016. [online] Available at: https://pdfs.semanticscholar.org/fb3c/f6150da8feb7626b0e79862333e-baeb36d25.pdf [Accessed: 01 April 2019]

[8] Lock, A., Allen, A. "Effects of Reversible Watermarking on Iris Recognition Performance", International Journal of Mechanical and Mechatronics Engineering, 8(4), pp. 606–611, 2014. [online] Available at: https://waset.org/publications/9998046/effects-of-reversible-watermarking-on-iris-recognition-performance [Accessed: 01 April 2019]

[9] Czajka, A., Kasprzak, W., Wilkowski, A. "Verification of iris image authenticity using fragile watermarking", Bulletin of the Polish Academy of Technical, 64(4), pp. 807–819, 2016. https://doi.org/10.1515/bpasts-2016-0090

[10] Dong, J., Tan, T. "Effects of watermarking on iris recognition performance", In: 10th International Conference on Control, Automation, Robotics and Vision, Hanoi, Vietnam, 2008, pp. 1156–1161. https://doi.org/10.1109/ICARCV.2008.4795684

[11] Celik, M. U., Sharma, G., Tekalp, A. M., Saber, E. "Lossless generalized-LSB data embedding", IEEE Transactions on Image Processing, 14(2), pp. 253–266, 2005. https://doi.org/10.1109/TIP.2004.840686

[12] Tian, J. "Reversible data embedding using a difference expansion", IEEE Transactions on Circuits and Systems for Video Technology, 13(8), pp. 890–896, 2003. https://doi.org/10.1109/TCSVT.2003.815962

[13] Sachnev, V., Kim, H. J., Nam, J., Suresh, S., Shi, Y. Q. "Reversible Watermarking Algorithm Using Sorting and Prediction", IEEE Transactions on Circuits and Systems for Video Technology, 19(7), pp. 989–999, 2009. https://doi.org/10.1109/TCSVT.2009.2020257

[14] Weng, S., Zhao, Y., Pan, J.-S., Ni, R. "Reversible Watermarking Based on Invariability and Adjustment on Pixel Pairs", IEEE Signal Processing Letters, 15, pp. 721–724, 2008. https://doi.org/10.1109/LSP.2008.2001984

[15] Li, Y.-C., Yeh, C.-M., Chang, C.-C. "Data hiding based on the similarity between neighboring pixels with reversibility", Digital Signal Processing, 20(4), pp. 1116–1128, 2010. https://doi.org/10.1016/j.dsp.2009.10.025

[16] Yang, B., Schmucker, M., Funk, W., Busch, C., Sun, S. "Integer DCT-based reversible watermarking for images using companding technique", In: Electronic Imaging, San Jose, California, USA, 2004, pp. 405–415. https://doi.org/10.1117/12.527216

[17] Lee, S., Yoo, C. D., Kalker, T. "Reversible Image Watermarking Based on Integer-to-Integer Wavelet Transform", IEEE Transactions on Information Forensics and Security, 2(3), pp. 321–330, 2007. https://doi.org/10.1109/TIFS.2007.905146

[18] Subramanian, P., Krishna, K. N., Sebastian, R. M., Rahman, N. U. "Multibiometric Systems", International Journal of Chemical Sciences, 14(S3), pp. 805–808, 2016. [online] Available at: https://www.tsijournals.com/articles/multibiometric-systems.pdf [Accessed: 01 April 2019]

[19] Hoang, T., Tran, D., Sharma, D. "Remote multimodal biometric authentication using bit priority-based fragile watermarking", In: 19th International Conference Pattern Recognition, Tampa, FL, USA, 2008, pp. 1–4. https://doi.org/10.1109/ICPR.2008.4761869

[20] Vatsa, M., Singh, R., Noore, A. "Feature based RDWT watermarking for multimodal biometric system", Image and Vision Computing, 27(3), pp. 293–304, 2009. https://doi.org/10.1016/j.imavis.2007.05.003

[21] Charles, O. U. "Biometric Iris Image Segmentation and Feature Extraction for Iris Recognition", PhD Thesis, Newcastle University, Newcastle upon Tyne, UK, 2015.

[22] Walia, M., Jain, S. "Iris Recognition System Using Circular Hough Transform", International Journal of Advance Research in Computer Science and Management Studies, 3(7), pp. 13–21, 2015. [online] Available at: https://pdfs.semanticscholar.org/e808/3ec6c9b081974085709735844bb2c8500b15.pdf [Accessed: 01 April 2019]

[23] Yew, R., Ng, F., Tay, Y. H., Mok, K. M. "An effective segmentation method for iris recognition system", In: 5th International Conference on Visual Information Engineering (VIE 2008), Xian, China, 2008, pp. 548–553. [online] Available at: https://ieeexplore.ieee.org/document/4743483 [Accessed: 01 April 2019]

[24] Verma, P., Dubey, M., Basu, S., Verma, P. "Hough Transform Method for Iris Recognition-A Biometric Approach", International Journal of Engineering and Innovative Technology (IJEIT), 1(6), pp. 43–48, 2012. [online] Available at: https://pdfs.semanticscholar.org/0a9a/3f30798459cffd7bb9b327662ca931da6df1.pdf [Accessed: 01 April 2019]

[25] Thalji, Z., Alsmadi, M. "Iris Recognition Using Robust Algorithm for Eyelid, Eyelash and Shadow Avoiding", World Applied Sciences Journal, 25(6), pp. 858–865, 2013. [online] Available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.591.8868&rep=rep1&type=pdf [Accessed: 01 April 2019]

[26] Bazrafkan, S., Thavalengal, S., Corcoran, P. "An end to end Deep Neural Network for iris segmentation in unconstrained scenarios", Neural Networks, 106, pp. 79–95, 2018. https://doi.org/10.1016/j.neunet.2018.06.011

[27] Thabit, R., Khoo, B. E. "Capacity improved robust lossless image watermarking", IET Image Processing, 8(11), pp. 662–670, 2014. https://doi.org/10.1049/iet-ipr.2013.0862

[28] Mohammed, R. T., Khoo, B. E. "Image watermarking using slantlet transform", In: IEEE Symposium on Industrial Electronics and Applications (ISIEA), Bandung, Indonesia, 2012, pp. 281–286. https://doi.org/10.1109/ISIEA.2012.6496644

[29] Narayanan, A. "Program for Fingerprint Minutiae Extraction, (version 1.0.0.0)", [computer program] Available at: https://www.mathworks.com/matlabcentral/fileexchange/31926-fingerprint-minutiae-extraction [Accessed: 01 January 2019]

[30] Center for Biometrics and Security Research "CASIA iris image database", [online] Available at: http://www.cbsr.ia.ac.cn/Databases.htm [Accessed: 01 January 2019]

[31] Indian Institute of Technology Delhi "IIT Delhi Iris Database version 1.0", [online] Available at: http://web.iitd.ac.in/~biometrics/Database_Iris.htm [Accessed: 01 January 2019]