ARTICLE

JOURNAL OF UNIVERSITY OF BABYLON
For Pure and Applied Sciences (JUBPAS)

Vol.30; No.3.| 2022

ISSN: 2312-8135 | Print ISSN: 1992-0652

info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية

Biometric Privacy Protection based on Combination of Hiding and Chaotic Encryption

Elaf Ali Abbood [1*], Suhad A. Ali[2], and Sheimaa A. Hadi[3]
1* Computer Department, Science College for Women, University of Babylon
wsci.elaf.ali@uobabylon.edu.iq, Hilla, Iraq
2 Computer Department, Science College for Women, University of Babylon
suhad_ali2003@yahoo.com, Hilla, Iraq
3 Computer Department, Science College for Women, University of Babylon
wsci.sheimaa.hadi@uobabylon.edu.iq, Hilla, Iraq

*Corresponding author email: wsci.elaf.ali@uobabylon.edu.iq; mobile: 07725963555

حماية الخصوصية البيومترية على أساس مزيج من الإخفاء والتشفير الفوضوي

ايلاف علي عبود[1*]، سهاد احمد علي [2] ،شيماء عبد الكاظم[3]
1* كلية العلوم للبنات، جامعة بابل،wsci.elaf.ali@uobabylon.edu.iq ، الحلة، العراق
2 كلية العلوم للبنات، جامعة بابل، suhad_ali2003@yahoo.com، الحلة، العراق
3 كلية العلوم للبنات، جامعة بابل، wsci.sheimaa.hadi@uobabylon.edu.iq، الحلة، العراق

Received:	29/ 6 /2022	Accepted:	27 /8 /2022	Published:	30 /9 /2022

ABSTRACT

With the expanded use of biometric systems, the safety of the biometric feature has become increasingly important. When biometric images are transferred through unsafe channels or stored as raw data, they become at risk of theft, forgery and attack. Data hiding is one of the main techniques of Privacy Protection. The goal of biometric data hiding is for adequate personal data is to be included in the cover of Biometrics and to maintain recognition performance. The paper idea introduces two levels of security based on hiding and encryption. The eye image is segmented into two regions Region of Interest (ROI) and Non-Region of Interest (NROI), The iris segmentation method depends on the Circular Hough Transform (CHT). The privacy data is embedded with NROI and then reassemble the image with ROI (iris) to get the embedding image. Then chaotic encryption is applied on the embedded image to get a high level of security. The experimental results are tested using the CASIA1 data set. The tests of hiding level are done using measurements such as PSNR and NC. The results show that the suggested method gives a higher value of PSNR which means not destroy the cover image and the value of NC is (1) which means a perfect reconstruction of secret data. The tests on encryption levels show good results using measurements such as histogram, correlation, and entropy.

Key words:
Biometric, Chaotic Encryption, ROI, NROI, IWT

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

الخلاصة

نتيجة لاستخدام أنظمة القياسات الحيوية بكثرة، أصبحت سلامة ميزة القياسات الحيوية ذات أهمية كبيرة. عندما يتم نقل الصور البيومترية عبر قنوات غير آمنة أو تخزينها كبيانات أولية ، فإنها تصبح عرضة لخطر السرقة والتزوير والهجوم. يعد إخفاء البيانات أحد الأساليب الرئيسية لحماية الخصوصية. الهدف من إخفاء البيانات البيومترية هو تضمين البيانات الشخصية ززفي غلاف القياسات الحيوية والحفاظ على أداء التعرف .تقدم الفكرة الورقية مستويين من الأمان يعتمدان على الإخفاء والتشفير. يتم تجزأت صورة العين إلى جزئيين او منطقتين هما (NROI) (ROI) وبقصد بهما منطقة مهمة ومنطقة غير مهمة .يتم تضمين بيانات الخصوصية مع NROI ثم إعادة تجميع الصورة باستخدام ROI للقزحية للحصول على صورة مدمجة. ثم يتم تطبيق التشفير العشوائي على الصورة المضمنة للحصول على مستوى عالٍ من الأمان. تم اختبار النتائج التجريبية باستخدام مجموعة بيانات.CASIA1 تم استخدام مقياسيين هما PSNRو .NC أظهرت نتائج الاختبار قيمة عالية لل PSNR مما يعني احتفاظ صورة الغلاف بجودتها وقيمة NC هي (1) مما يعني استرجاع مثالي للبيانات السرية. كما وتم اختبار طريقة التشفير باستخدام قياسات مثل الرسم البياني والارتباط والنتروبيا وجميع النتائج كانت جيدة.

الكلمات المفتاحية:

القياسات الحيوية, التشفير الفوضوي، ROI، NROI،IWT

INTRODUCTION

Traditional authentication methods are mainly based on tokens e.g. ID cards, knowledge, and passwords [1]. The former is easy to lose and copied, and the latter is at risk of being forgotten or stolen. Because of this, biometric authentication technology has been widely developed recently [2]. According to the origin, characteristics can be divided into physiological bio-characteristics, e.g. finger prints, irises, faces, DNA, etc. and behavior al bio-characteristics, e.g. signatures, voice prints, gait, etc. These biometric characteristics are generally unique, life immutable, and hard to be forgotten or stolen during identity authentication.

Among the various biometric authentication systems, iris authentication [3] has attracted great attention due to its stable recognition performance and high recognition rate. In the existing iris authentication systems, personal iris images are collected as biometric templates by an authorizing institution and stored in different types of sub-data bases with the corresponding personal privacy data, e.g. name, phone number, address, bank account, etc.

One of the most important ways to protect privacy is to hide data. In authentication systems, biometrics like the iris, face, and fingerprint are frequently utilized [4, 5]. Biometrics are typically required to be kept in a database for further authentication. However, there is a chance that database-stored templates will be altered or stolen. Once the templates are stolen, it is difficult to be replaced passwords. Meanwhile, the user's private information (e.g., name, bank account, address, number, etc.) associated with the theft template would also be leaked. Thus, it is of paramount importance to protect the privacy of biometrics data. It is necessary to provide a technique to overcome the challenges outlined above. The need to protect data is not only intended to protect privacy but also to detect the manipulation that occurs by unauthorized persons during the process of transferring this information from one place to another [6]. The purpose of biometric data hiding is to keep recognition performance intact

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

while encoding enough personal data into cover biometric templates,so paper's goal is to aid in patient privacy protection.

2. RELATED WORKS

Many methods introduced concerted authentication of image techniques the authors have listed a detailed literature review method for image authentication. These techniques are recorded as follows:

In 2018, Eyad Ben Tarif [7] proposed safe biometric data transmission for multimodal biometric authentication and identification systems, a highly secure encryption/hiding strategy. Utilizing an accelerated iterative hard thresholding technique, the secret fingerprint and iris vectors are generated approximations that are then inserted in the face image's host Slantlet-SVD domain.

In 2019 Sheng Li. [8] suggested a data-hiding technique for iris images is proposed. With the help of the proposed distortion function and STC framework, the embedding adjustments are limited into the regions lacking significant iris features to minimize the impact on iris identification. The privacy of users is maintained when personal privacy information is included into iris images.

In 2020 , Nur Khaleeeda Mansor [9] produced a method for iris biometric protection that high-quality images by differencing two pixel pairs and utilizing a steganography approach to shift the bits. By integrating PVD approaches. In this work, both PSNR and MSE scales were used as metrics to measure image quality.

2. The Suggested System

The overall diagram of the suggested system consists of two stages: the embedding and extracting procedures as shown in figure (1).

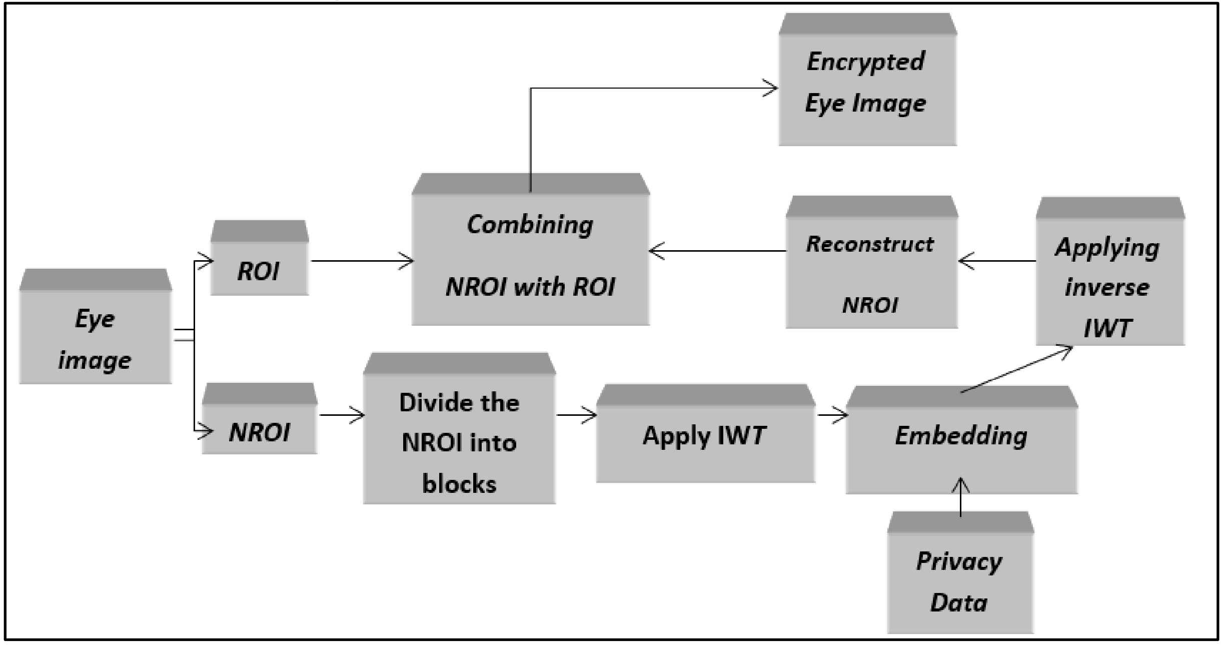


Figure (1): Proposed Privacy protection in biometric image system

مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

2.1 Embedding Procedure

The embedding process is done in on the sender side. It includes several steps which depict as follow:

2.1.1 Iris Image Segmentation

In the suggested system, block-based embedding in the lifting Integer Wavelet Transform (IWT) domain is applied, lifting wavelet transform (LWT) is a method for breaking down wavelet transforms into a number of stages. Compared to the conventional wavelet techniques, the lifting scheme algorithms reduce computing time and memory requirements. To achieve this purpose, the eye image is divided into two regions (ROI and NROI), The crucial data needed for diagnosis is contained in the ROI. The ROI region is always determined by the specialist user interactively and is in an irregular form. The ROI represents the iris region which is important later in the recognition system, while the NROI represents the pixels of the background which can be used for embedding process in order not recognition accuracy. Figure (2) shows the iris segmentation method.

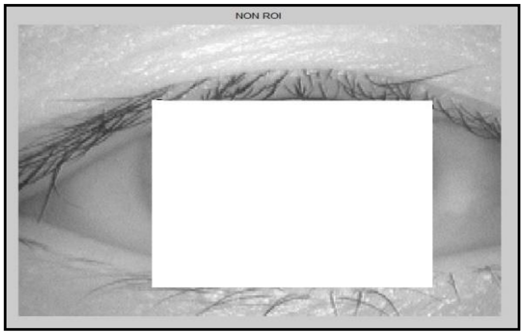


Figure (2): The iris segmentation method

2.1.2 Embedding process

The process of embedding patient information (secrete data) in RONI begins after the privacy data have been converted into binary form. These privacy data are stored in the form of a single matrix. Firstly, the NROI is partitioned into 4×4 blocks. In the second step, the IWT is applied on each block on NROI. Each block is transformed into the frequency domain which divided (decomposed) the mapping block into four sub bands (ss, sd, ds, and dd). Three bits of data are embedded in the middle bit plane (mid=2(second-bit plane)) of each sub-band (sd, ds, and dd) of each block of NROI. Repeat these steps until all bits of the data are embedded. Applying inverse IWT on each block. After the completion of embedding processes, the ROI is combined with NROI to configure eye images.

2.1.3 Encryption Process

To provide a second level of security, chaotic encryption algorithm is applied to embedding images. Firstly, a chaotic sequence is generated using the equation of quadratic map (1).

$$Seq(n+1) = -(r*(Seq(n).{}^{\wedge}2)) \quad \ldots (1)$$

After generating random sequence, Convert it from the range (-0.5 — 0.5) to the (-1 — 1) range,according to the following equation (2)

$$New\_Seq = (((Seq - OldMin) * NewRange) / OldRange) + NewMin \quad \ldots (2)$$

OldRange represents the chaotic sequence that was formed from (-0.5 to 0.5).

The new chaotic sequence from NewRange is (-1 to 1)
OldMin is the lowest number in the resulting chaotic sequence (-0.5).
NewMin stands for the lowest value in a new chaotic sequence (-1)

The generated chaotic sequence is used to encrypt the image through two steps that are combined simultaneously: shifting the positions and changing the values of bits of the input image. Firstly, scrambling bits of the image is applied to change bit locations by sorting the generated. New_Seq in ascending (or descending) order then change bit location according to corresponding indices (loc) of New_Seq.

[Sorted_Seq,loc]=sort(New_Seq) … (3)
Scrambled_Template (i)= Template(loc(i)) …(4)
Where i=1…length(Template)

Then the secret image encryption (Coding) depends on the following equations:

$$Bipolar\_image(i) = \begin{cases} New\_Seq(i) & if\ (Template(i) = 1) \\ New\_Seq(i) * -1 & if\ (Template(i) = 0) \end{cases} \ldots(5)$$

for i= 1 to length (Template)

finally, Converted the Generated Bipolar_ image to binary Encrypted_image by adding value (lies between -10.5):

Encrypted_ image =Round(Bipolar_ image + es) …(6)

2.1.4 Decryption Process

The decryption process is performed to generate the random sequence using New_Seq using equation (1) with the same initial parameters used in the encryption process. Then Shifting Encrypted_image by 0.5 and round the result according to the following :

S_ Encrypted_image =round (Encrypted_image -0.5)…(7)

Multiply *S_ Encrypted_image* by generated sequence as follows:

*bipolar_imag= New_Seq * S_ Encrypted_image*…(8)

Get the decrypted bits of *Encrypted_image* by thresholding the *bipolar_image* :

$$Decrypted\_image(i) = \begin{cases} 1 & if\ (bipolar\_image(i) > 0) \\ 0 & otherwise \end{cases} \ldots(9)$$

for *i*= 1 to length(*bipolar_image*)

Finally, re- shuffle the locations of *Decrypted_ image* bits by sorting the generated *New_Seq* in ascending (or descending) order then change bit location according to corresponding indices (*loc*) of *New_Seq*

[Sorted_Seq,loc]=sort(New_Seq) … (10)
Decrypted_ image(loc(i))= Decrypted_ image(i)…(11)
Where i=1…length(*Decrypted_ image*)

2.2 Extraction Procedure

On the receiver side, the extraction process is done in reverse order. At first, the process of decryption is applied on the received image then the decrypted eye image is segmented into ROI and NROI. Secondly, the embedding privacy information is extracted from RONI and the decompression is applied to get the original data as . On the receiver side, the extraction process

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

is done in reverse order. At first, the process of decryption is applied to the received image then the decrypted eye image is segmented into ROI and NROI. Secondly, the embedding privacy information is extracted from RONI . Extracting process is done by dividing the NROI into blocks (BL), each of size 4×4, and applying integer wavelet transform (IWT) on each mapping block.Then extract two data bits in each sub-bands (sd, ds, and dd) of each block.

3. EXPERIMENTAL RESULTS

3.1 Data set

The performance of a proposed biometric system is tested on the CASIAV1.0 iris image database. This database is publicly available via the internet. The CASIA-1 iris image database includes 756 iris images from 108 eyes collected over two sessions for of two months.

3.2 Testing the Imperceptibility Fidelity Performance

This section illustrates after applying the embedding procedure with the proposed system. At first, the cover (eye) image is segmented manually into two regions these are a region of interest (ROI) and a non-region of interest (NROI). The ROI represents the important region of the eye image which is the iris. This region is important in the recognition system therefore we must keep it unchanged. The embedding process is done in the second region (NROI) which contains not important information.

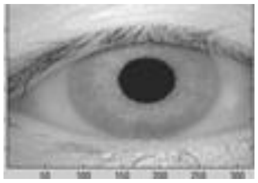
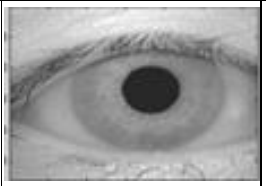
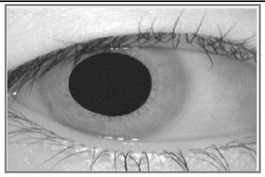
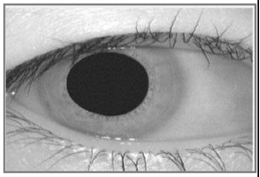
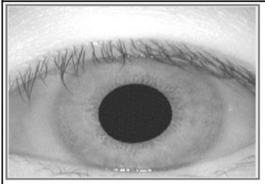
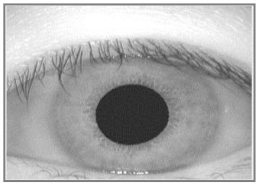
Table (1) illustrates the eye images before and after implementing the embedding the procedure with the proposed system. The testing includes imperceptibility and fidelity. Related to imperceptibly, visually, there is no difference between the original and embedding eye image. Related to fidelity, table (1) shows the value of PSNR is of high value which means that there is a little distortion in the image after embedding procedure.

مجلة جامعة بابل للعلوم الصرفة والتطبيقية

ISSN: 2312-8135 | Print ISSN: 1992-0652

info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

Table (1): Original eye image, embedding eye image, no. of blocks needed for embedding, maximum blocks available, and values of PSNR

Original eye image	Embedding eye image	No. of blocks needed for embedding	Maximum blocks available	MSE	PSNR
		50	3665	0.103	52.21
		50	3401	0.2694	53.8609
		50	3675	0.1482	56.4559

3.3 Experimental Results Related to the Encryption Process

The embedding images will be sent through a channel from sender to receiver therefore it is necessary to protect the embedding images. The second level of security is applied using the stream cipher method on embedding images. Figure (3) shows an example of embedding, encryption and decryption processes

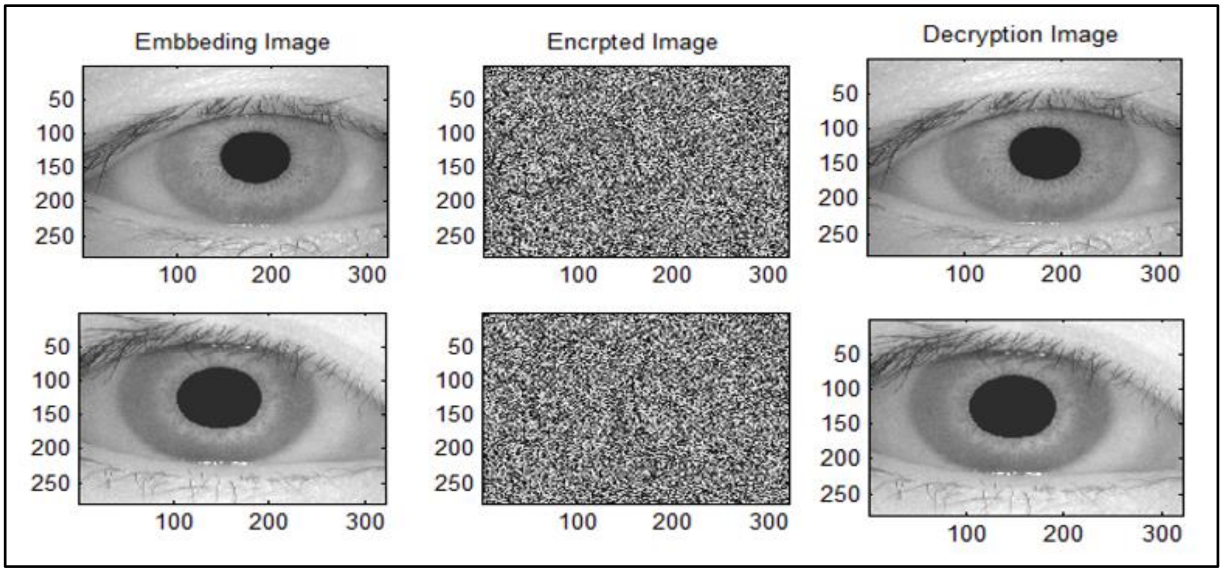


Figure (3): Encryption and Decryption Process

1. Histogram Analysis

Any image's histogram is a graph that displays the distribution of pixel intensity values. For instance, there are 256 different potential intensities in an 8-bit grayscale image. As a result, 256 digits representing the histogram's distribution of pixels among those intensities values will be displayed. However, for all simple photos, the histogram of a suitable encryption image must have a somewhat regular shape. Figure (4b) displays the histograms of the two original photos, each of which has quite distinct content, as well as the histograms of the encrypted versions of those images (4d).

2. Entropy

The input image's texture can be described using entropy, a statistical measure of randomness. It used in information theory; it mean number of bits need to code an image. For example, in 256 gray scale images, the perfect value of entropy is(8), which indicates to a truly random source. The calculated results in figure (4e) indicate that all the entropies values of the encrypted images are very close to the value of 8.

3. Correlation

The statistical dependents between two observed quantities are represented by the correlation coefficient,As noted in Figure (4f) that the correlation coefficients are very small (C≈0), which points that the encrypted image and original images are entirely uncorrelated with each other.

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية
ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

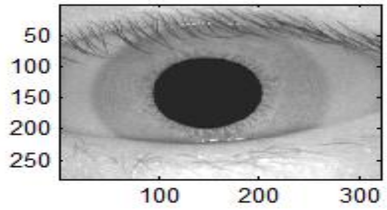
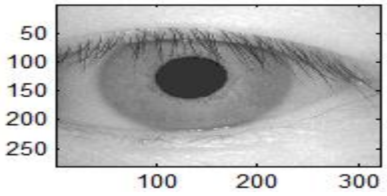
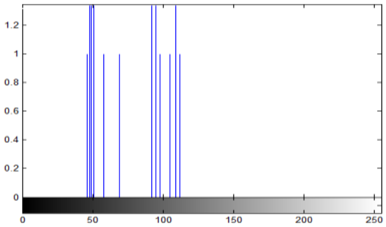
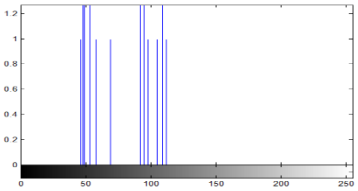
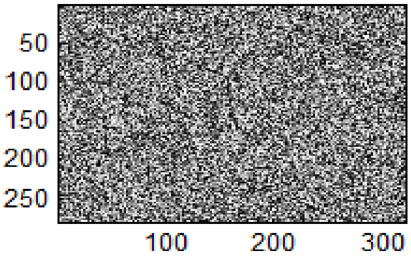
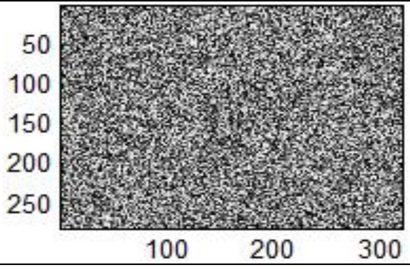
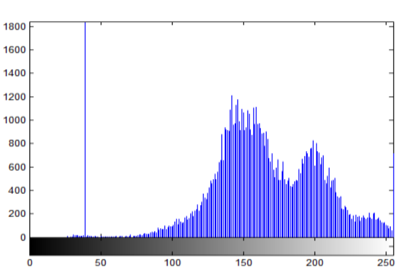
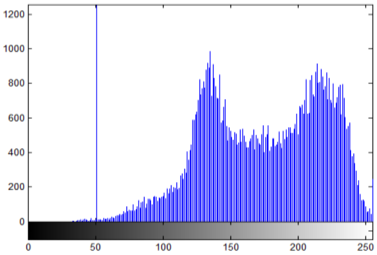
(a) Original Image		
(b)Histogram of Original Image		
(c) Encrypted Image		
(d)Histogram of Encrypted Image		
(e) Entropy	**7.911**	**7.98**
(f)Correlation	**0.00023**	**0.0025**

Figure (4): Measurements of Proposed System

4. CONCLUSIONS

This paper proposed a robust method for biometric privacy protection. Firstly, the secret data is embedded in the non-interest region of the biometric image. Secondly, to increase the security layer, the encryption operation is applied using the chaotic method. Later, the proposed method is tested using several parameters and gives good results.

Conflict of interests.

There are non-conflicts of interest.

References

1- Handbook of biometrics[M]. New York, NY: Springer Science Business Media, 2007.

2- A. K. Jain, A. Ross, and S. Prabhakar, “An introductionto biometricrecognition[J],” IEEE Transactions on Circuitsand Systems for VideoTechnology, Vol. 14, no. 1, pp. 4–20,2004.

3- L. Masek. Recognition of Human Iris Patterns for BiometricIdentification [D].TheUniversity ofWestern Australia, 2003.

4- C. Qin, C. C. Chang, and YP. Chiu ,“A novel joint datahiding and compression scheme based on SMVQ and image inpainting[J],” IEEE Transactions on Image ProcessingA Publication of the IEEE Signal Processing Society, Vol. 23, no. 3, pp. 969–978, 2014.

5- C. Qin, and X. Zhang, “Effective reversible data hiding in encrypted image with privacy protection for image content [J].” *Journal of Visual Communication & Image Representation*,",Vol. 31, pp. 154–164, 2015.

6- B. Ma, C. Li, Y. Wang, Z. Zhang, and Y. Wang. Block pyramid based adaptive quantization watermarking for multimodal biometric authentication. s.l. : *"in Proc. 20th Int. Conf. Pattern Recognition, Istanbul*", 2010.

7- Ben Tarif, Eyad, Wibowo, Santoso,and Wasimi, Saleh; Tareef," A hybrid encryption/hiding method for secure transmission of biometric data in multimodal authentication system".*CQ University. Journal contribution"*. https://hdl.handle.net/10018/1231400

8- Sheng Li, Xin Chen, Zichi Wang, Zhenxing Qian and Xinpeng Zhang, “Data Hiding in Iris Image for Privacy Protection,” *IETE Technical Review*", 2019.

9- Nur Khaleeeda Mansor, Syed Muhammad Hazry Asraf and Syed Zulkarnain Syed Idrus," Steganographic on Pixel Value Differencing in Iris Biometric","*Journal of Physics: Conference Series*",2020.

مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com