ENCRYPTED FUSION OF FACE AND IRIS BIOMETRICS

Sivasankari Narasimhan
Assistant Professor, Electronics and Communication Engineering,
Mepco Schlenk Engineering College, Virudhunagar Dt, (India).
E-mail: sivani.sivasankari@gmail.com
ORCID: https://orcid.org/0000-0002-3162-4751

Muthukumar Arunachalam
Associate Professor, Electronics and Communication Engineering,
Kalasalingam University, Virudhunagar Dt, (India).
E-mail: Muthuece.eng@gmail.com
ORCID: https://orcid.org/0000-0001-8070-3475

Recepción: 28/11/2019 **Aceptación:** 17/03/2021 **Publicación:** 30/11/2021

Citación sugerida:
Narasimhan, S., y Arunachalam, M. (2021). Encrypted fusion of face and iris biometrics. *3C Tecnología. Glosas de innovación aplicadas a la pyme, Edición Especial,* (noviembre, 2021), 513-535. https://doi.org/10.17993/3ctecno.2021.specialissue8.513-535

ABSTRACT

Security is the main concern in storing databases. Any methods can be used to secure the data. In addition to that identification also done to provide the correct service to the person. In our model we propose the methodology to include biometric fusion and encryption to store and secure user's information. Image fusion is done from the information from different face and iris images. The method of considering only high intensity pixel based image fusion generate new images that hold the attractive information and characteristics of each input image. The fused resulting image is given to the encryption module and encrypted information in stored in database which is further used for identification and authentication. Fusion techniques and lightweight encryption algorithm has been implemented and simulated in MATLAB. The parameters correlation, computation time, Unified averaged changed intensity(UACI), Number of changing pixel rate(NCPR)and Entropy are calculated and the results show the effectiveness of encrypted fusion based on DWT. Entropy has been increased by 67%. NCPR of 99.6239 and UACI of 3.3004.

KEYWORDS

Fusion, Face biometric, Iris biometric, DWT, Encryption.

https://doi.org/10.17993/3ctecno.2021.specialissue8.513-535

1. INTRODUCTION

Image fusion is an essential step in multimodal biometrics. Image fusion is a process by which two images are fused together to obtain a single image. Images with different focused regions, images from different modalities or images taken in different times have been fused together to give enhanced results. With change in time, the face images produced by persons may differ due to aging. These images cannot give a clear picture needed for clear identification. Thus, for efficient diagnosis, one needs different multimodal image information in a single image. The features that are not changes more with age is iris. To this point, in research, many fusion techniques based on Iris and face images, were proposed by the researchers. The transform based fusion methods include decomposition of image by Stationary Wavelet Transform (SWT), Discrete Wavelet Transform (DWT), Lifting Wavelet Transform (LWT), Redundancy Discrete Wavelet Transform (RDWT), Dual-Tree Complex Wavelet Transform (DTDWT). These methods have unique drawbacks but all of them share some common drawbacks such as introduced additive noise in fused image.

A multimodal biometric system is developed using fingerprint and iris biometric in Rajbhoj and Mane (2015). The system combines fingerprint and iris at feature level. Single feature vector is obtained by fusing fingerprint and iris image and unique textural pattern from fused image is obtained by efficient wavelet transform. Matching is carried using Hamming distance. Here independent databases are used for face and iris images and each fingerprint is assigned a corresponding iris image.

The multimodal biometric system in ElAlami, Amin, and El-Alfi (2012) combines face and fingerprint biometrics in matching score level. They used the gray-level co-occurrence matrix (GLCM) as an effective method for extracting the texture features in the face recognition and crossing number method is used for fingerprint feature extraction. For matching process they used correlation coefficient as the similarity measure. A multimodal biometric system is developed by combining face and fingerprint biometric by score level fusion. According to \cite{19} face recognition is done using PCA and fingerprint recognition is done using minutiae matching and Gabor filtering.

A multimodal biometric system in Krishneswari and Arumugam (2012) combines palm print and fingerprint in feature level. Palm print and finger print images were fused using

https://doi.org/10.17993/3ctecno.2021.specialissue8.513-535

wavelet based image fusion techniques with min-min approximation. Features were extracted using Discrete Cosine Transform (DCT) and feature reduction is done. In their work also independent databases are used for palm print and fingerprint and they are combined by assigning a fingerprint image to each palm print image. Their shows that multi modal biometrics are more efficient than conventional palm print based methods.

Usman et al. (2017) explains about, light weight encryption algorithm which will fit for IoT. The single input image is authenticated using encryption algorithm.

In the proposed method, source images are decomposed into low-level sub band, high-level sub bands using DWT. Next, low-level sub-images are again decomposed into low and high level images. In two level decomposition, iris image is fused.

Our project gives the following significant works

1. Dual modal biometric as face and iris recognition fusion have been taken.
2. Encryption to safeguard the fused database.
3. Analysis of security concerns in both fusion and encryption.

The remaining sections are organized as follows: section 2 provides the proposed methods and section 3 gives the implementation results followed by conclusion in section 4.

2. PROPOSED METHODOLOGY

The proposed DWT consists of four steps: Enhancement, decomposition, fusion and encryption. The block diagram of the proposed DWT-based face iris fusion is shown in Figure 1. Now let us see the process involved and used components in the process one by one.

https://doi.org/10.17993/3ctecno.2021.specialissue8.513-535

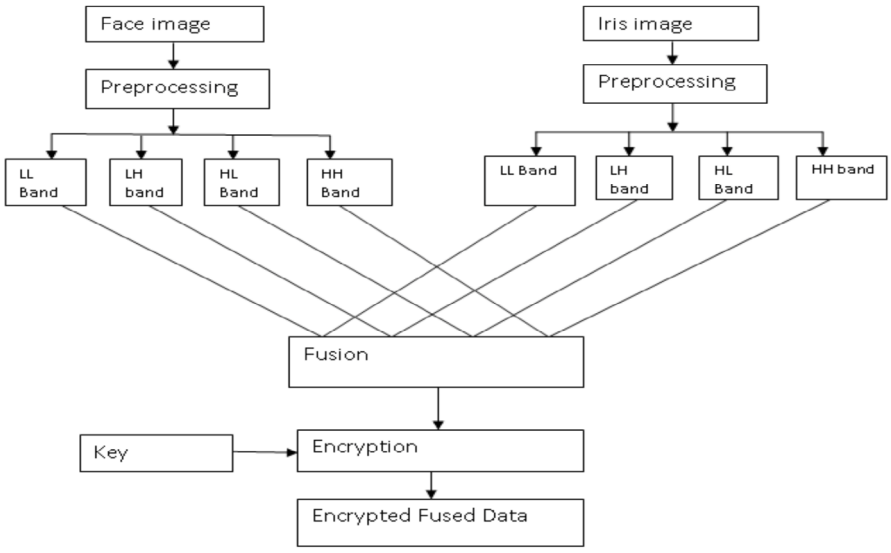


Figure 1. Overall block diagram.
Source: own elaboration.

Step1: Face image and iris images are preprocessed. Color images are converted into gray scale images. They have been resized into 256x256

Step 2: As per Discrete Wavelet Transform (DWT), approximation, horizontal, vertical and diagonal details have been found out for two levels for both images. The individual sub images are compared and the highest intensity value image is taken for fused image.

Step 3: The image is encrypted using secure light weight encryption algorithm.

2.1. DWT ALGORITHM

The Haar wavelet illustrates the desirable properties of wavelets in general. It can generally use for image denoising. It uses the orthonormal basis vector in the rows of $\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & -1 \end{bmatrix}$. DWT demonstrates the localization: the first row (1,1,1,1) term gives the average signal value; Second row (1,1,-1,-1) places the signal in the left side of the domain; and (1,-1,0,0) places it at the left of the left side. The explanation of DWT is

https://doi.org/10.17993/3ctecno.2021.specialissue8.513-535

available in "Discrete wavelet transform" (2008). First, the samples are passed through a low pass filter with impulse response g (n), Hence the convolution operation between input image function and impulse function has been taken place.

$$y(n) = \sum_{k=0}^{n-1} x(k).g(n-k) \tag{1}$$

The signal is decomposed simultaneously using high pass filter (h). So, the two filters are related to each other and they are known as a quadrature mirror filter.

$$y_{low}(n) = \sum_{k=-\infty}^{\infty} x(k)g(2n-k) \tag{2}$$

$$y_{high}(n) = \sum_{k=-\infty}^{\infty} x(k)h(2n-k) \tag{3}$$

With the sub sampling factor 2, the process is continued and all the levels are cascaded. For the representation of images in multi resolution wavelets can be used. If it has to be converted into other domain, the properties in one domain are easily separable and scalable. There is a unique set of expansion coefficients in every representable function of Fourier kernals.

2.2. FUSION

The performance of biometric system is improved by choosing correct fusion. In our approach feature level fusion is used. The feature vectors at second level of DWT are combined to produce the fused image. For verification of individual persons biometric, different images of any biometric can be fused. But authentication purpose, two different biometrics have been connected.

2.3. ENCRYPTION

Various encryption algorithms are being developed still now. For message encryption Symmetric encryption algorithm is used. In our algorithm, due to space complexities, light weight encryption algorithm is used. Usually, encryption operation is performed with specified number of bits known as key. With a 64 bit initial key further rounds of keys are generated. Key expansion is done as per the logic provided by Usman et al. (2017). The initial key is set as "AAAAAAAAAAAA" for this algorithm. It can be expanded for next

https://doi.org/10.17993/3ctecno.2021.specialissue8.513-535

rounds. The key expansion diagram is shown in Figure 2. The confusion and diffusion are introduced by 'F' function in it.

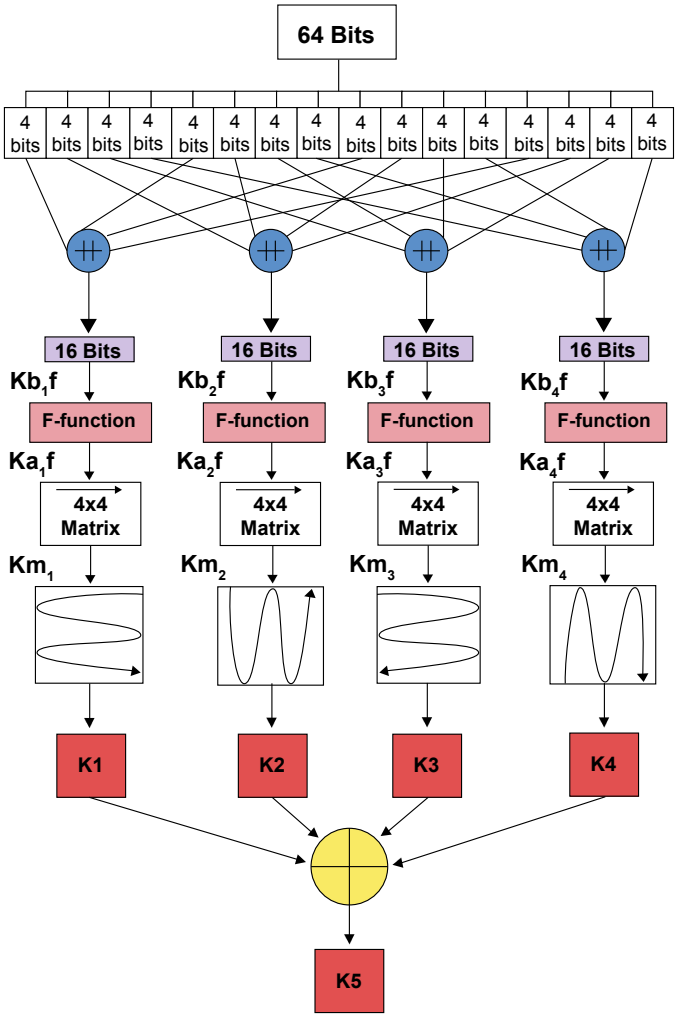


Figure 2. Key expansion.
Source: (Usman *et al.*, (2017).

As per the figure, from the initial key K5 is derived as XOR function of K_1, K_2, K_3, K_4. The function 'F' has done some permutations which gets 16 bits input and 16 bit output. Then encryption process is done as per equation 6. The intermediate ciphertext is given as:

$$IC_{i,j} = \begin{cases} Px_{i,j} \Theta K_i \\ Px_{i,j+1 \oplus Ef} \\ Pxi, j-1 \oplus Ef \end{cases} ; \quad (4)$$

https://doi.org/10.17993/3ctecno.2021.specialissue8.513-535

$IC_{i,j}$ is the intermediate result. $Px_{i,j}$ is the plaintext. If j=1 or 4 first equation is performed. If j=2 second operation is performed. If j=3 third operation is done. The final encryption operation is performed as the concatenation result of fifth round.

$$C=IC51 \,||\, IC52 \,||IC53 \,||IC54 \quad (5)$$

The encrypted information is stored in database, further it is used for identification.

4. IMPLEMENTATION RESULTS

Yale database is taken for face image in our experiment, which contains 15 subjects each of which have 15 images under different postures. The size of the image is 320 x 243. CASIA database is taken for iris images which contains 36 iris subjects and 7 for each. For our experiments, first 7 images of face are merged with first 15 images of IRIS database.

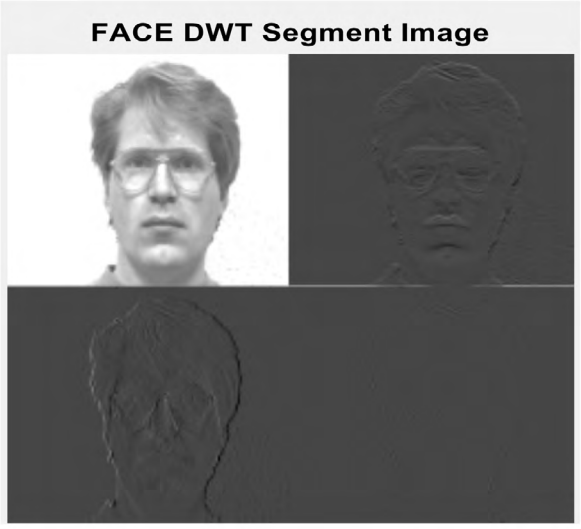


Figure 3. FACE DWT segment image.
Source: own elaboration.

First both face and iris images are undergone for DWT segmentation. The segmented image is shown in Figures 3 and 4.

https://doi.org/10.17993/3ctecno.2021.specialissue8.513-535

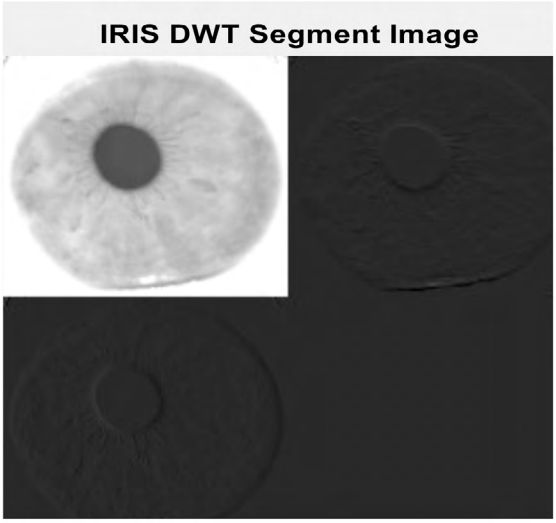


Figure 4. IRIS DWT segment image.
Source: own elaboration.

The images are getting fused by highest intensity feature level fusion logic. The fused image is shown in Figure 5.

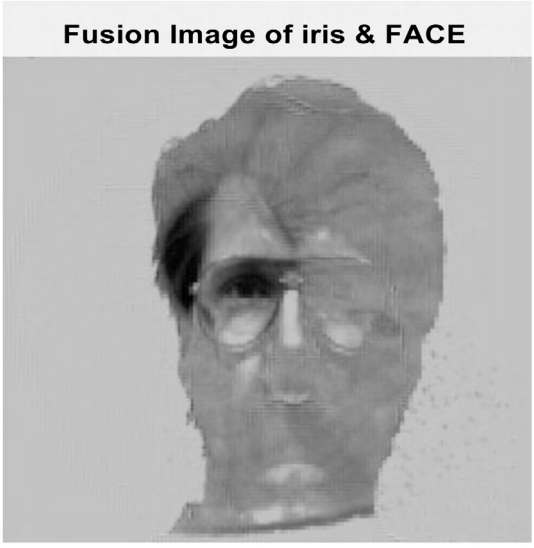


Figure 5. Fused image.
Source: own elaboration.

But fused image is intermediate stage. It is not visible by anybody. This image is going for encryption. In our algorithm, we are using light weight encryption algorithm. Hence it

https://doi.org/10.17993/3ctecno.2021.specialissue8.513-535

can be used for chip implementation. The fused image is resized to 256x256 image. After encryption we got the image as given in Figure 6.

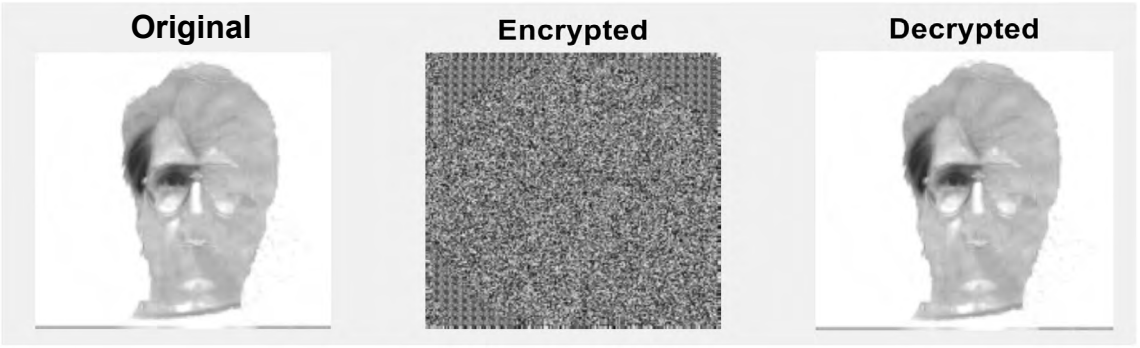


Figure 6. Encryption and Decryption by correct key.
Source: own elaboration.

When the same user is used for authentication the correlation score should be high. The encrypted image and original image are shown with their histograms in Figure 7.

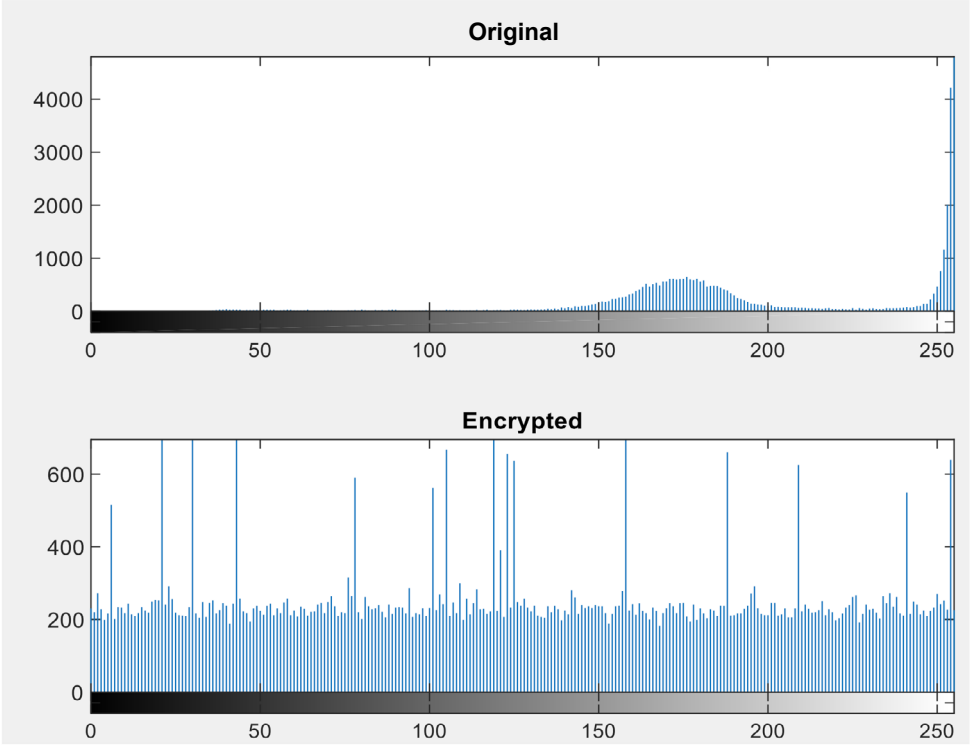


Figure 7. Correlation of original and encrypted image.
Source: own elaboration.

https://doi.org/10.17993/3ctecno.2021.specialissue8.513-535

Now, the image correlation and entropies have been calculated. The scatter plot of image is given in Figure 8.

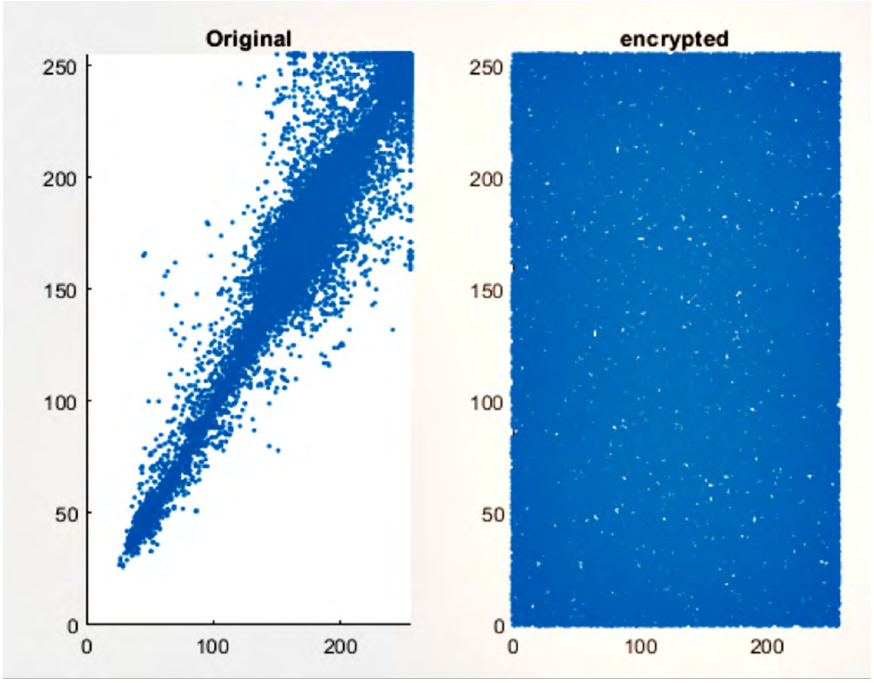


Figure 8. Scatter plot of encrypted image.
Source: own elaboration.

4.1. EVALUATION PARAMETERS

Image Entropy: the encryption algorithm adds extra information to the data so as to make it difficult for the intruder to differentiate between the original information and the encrypted information. Entropy is defined as:

$$H(I) = \sum_{i=1}^{2^8} P(I_i) \log_b P(I_i) \quad (6)$$

How much entropy is higher, more in formations are present, and hackers cannot find it easily. The results for the 35 image fusion are given in Table 1. Average of 7.7512 for the encrypted image is obtained. Almost 69% of entropy is increased, compared with original fused image.

https://doi.org/10.17993/3ctecno.2021.specialissue8.513-535

Correlation: dependency of statistical relationship between two images is said to be correlation. A well-designed cipher should not possess any relationship with original message.

In our experiment the correlation coefficient is calculated for original fused message and encrypted images. The correlation coefficient is defined as:

$$\gamma_{x,y} = \frac{\mathrm{cov}(x,y)}{\sqrt{D(x),D(y)}} \tag{7}$$

where cov(x, y), D(x) and D(y) are covariance and variances of variable x and y directions respectively. For ideal cipher case γ should be equal to 0 and for the worst case γ will be equal to 1.

In our experiment the original fused image has correlation coefficient of 0.98157, whereas the encrypted images have -0.109 correlation coefficient. (They are negatively correlated).

Number of changing pixel rate (NCPR): this is the parameter for testing the encryption against differential attacks. As per Wu, Noonan and Agaian (2011) the range of percentage is [0-100]. When it is zero it remains that all the pixels are having the same value. Clearly NCPR concentrates on absolute number of pixels which changes values in differential attacks.

$$NPCR : N(C^1, C^2) = \sum_{i,j} \frac{D(i,j)}{T} x100\% \tag{8}$$

Where C^1, C^2 are the before and after one pixel image in cipher.

$$D(i,j) = \begin{Bmatrix} 0, if \;\; C^1(i,j) = C^2(i,j) \\ 1, if C^1(i,j) \neq C^2(i,j) \end{Bmatrix} \tag{9}$$

T denotes the total number of pixels in ciphertext. The average value we obtain for NCPR is 99.6239.

Unified averaged changed intensity (UACI):

UACI concentrates on the averaged difference between two paired ciphertext images.

$$UACI : U(C^1, C^2) = \sum_{i,j} \frac{abs(C^1(i,j) - C^2(i,j))}{F.T} x100\% \tag{10}$$

https://doi.org/10.17993/3ctecno.2021.specialissue8.513-535

Where F is the maximum supported pixel value compatible with the cipher text. In our experiment F is taken as 255. The average value we obtained from this as 3.3004

Table 1. Analysis of parameters with key 'AAAAAAAAAAAAAAAA'.

Image 1	Image 2	Correlation		Total Encryption time (ms)	NCPR (%)	UACI (%)	Entropy	
		Original Image	Encrypted Image				Original image	Encrypted image
Subject 1. glasses	Iris 1	0.9782	-0.0206	9.172	99.661	3.082	4.124	7.9318
	Iris 1b	0.9751	-0.0246	8.113	99.653	2.2138	4.2116	7.9311
	Iris 1c	0.9848	-0.0048	8.096	99.597	3.8024	4.2159	7.9152
	Iris 1d	0.9689	-0.0138	8.165	99.676	1.6850	4.2351	7.9251
	Iris 1e	0.9831	-0.0138	8.093	99.679	3.4871	4.2117	7.9319
	Iris 1f	0.9800	-0.0168	8.453	99.557	2.4720	4.3174	7.9716
Subject 2. glasses	Iris 2	0.9831	-0.0058	8.003	99.565	3.8076	4.2263	7.2146
	Iris 2b	0.9817	-0.0014	8.158	99.623	3.7036	4.2247	7.2308
	Iris 2c	0.9737	-0.0096	8.034	99.586	1.8903	4.2126	7.2310
	Iris 2d	0.9737	-0.0096	9.002	99.586	1.8903	4.2329	7.5151
	Iris 2e	0.9845	-0.0077	8.197	99.627	4.0569	4.2352	7.4151
	Iris 2f	0.9795	-0.0021	8.232	99.632	2.6016	4.1247	7.5309
Subject 3. glasses	Iris 3	0.9821	-0.0139	8.358	99.632	2.6081	4.2147	7.9308
	Iris 3b	0.9856	-0.0071	8.264	99.577	3.1991	4.2146	7.9310
	Iris 3c	0.9854	-0.0142	8.875	99.636	3.1645	4.2359	7.9151
	Iris 3d	0.9854	-0.0142	8.270	99.636	3.1645	4.2359	7.9151
	Iris 3e	0.9798	-0.0100	8.522	99.630	2.4692	4.2147	7.9309
	Iris 3f	0.9889	-0.0115	8.415	99.638	4.5532	4.3374	7.9726
	Iris 3g	0.9880	-.0169	8.679	99.676	3.9941	4.2663	7.9146
Subject4. glasses	Iris 4	0.9804	-0.0124	8.508	99.600	3.3139	5.1418	7.9561
	Iris 4b	0.9804	-.0167	8.426	99.638	3.1778	5.0205	7.9314
	Iris 4c	0.9804	-.0167	8.426	99.638	3.1778	5.0205	7.9314
	Iris 4d	0.9804	-0.0167	8.8108	99.638	3.1778	5.0205	7.9314
	Iris 4e	0.9795	-0.0102	8.8440	99.658	3.8139	5.2303	7.9743
	Iris 4f	0.9808	-0.0152	9.0458	99.627	4.0870	5.2835	7.9536
	Iris 4g	0.9801	-0.0167	9.1555	99.615	4.1067	5.2935	7.9506
Subject05. glasses	Iris 5	0.9822	-0.0037	9.0337	99.624	3.5343	5.0542	5.0542
	Iris 5b	0.9848	-0.0039	9.0955	99.551	4.0488	5.0956	7.9943
	Iris 5c	0.9833	-0.0091	9.1250	99.644	3.4544	4.8371	7.9641
	Iris 5d	0.9833	-0.0091	9.0839	99.644	3.4544	4.8371	7.9641
	Iris 5e	0.9837	-0.0050	8.8077	99.679	3.4289	4.7934	7.9699
	Iris 5f	0.9855	-0.0030	9.1667	99.575	4.1457	5.1360	7.9884
	Iris 5g	0.9855	-0.0030	8.8251	99.575	4.1457	5.1360	7.9884

Source: own elaboration.

https://doi.org/10.17993/3ctecno.2021.specialissue8.513-535

This work has been accomplished with first image of yale database and CASIA database of second image. Various parameters have analyzed in this methodology and the parameters are given in Table 1.

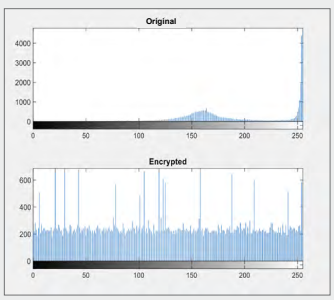
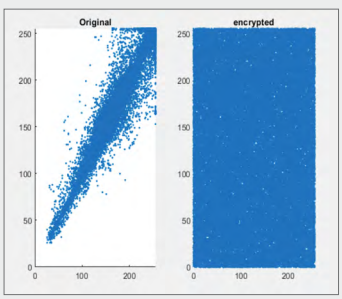
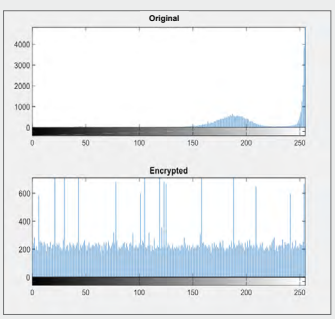
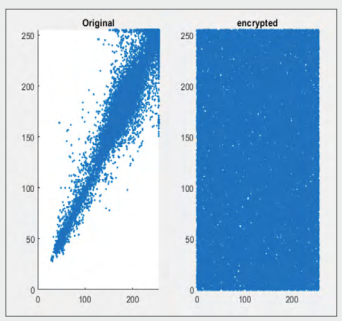
Key sensitivity: all encryption algorithms have to be designed in such a way that, if one bit is changed almost 60 % of the data should be changed in ciphertext. The changes in seed key value for the same biometric subjects are taken and the result is compared in Table 2. The distribution of histogram is given in Table 3.

Table 2. Comparison of various keys to show the key sensitivity.

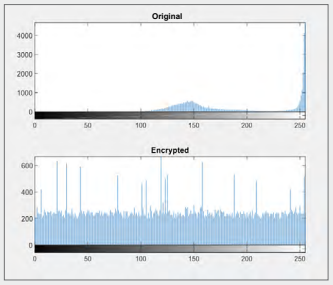
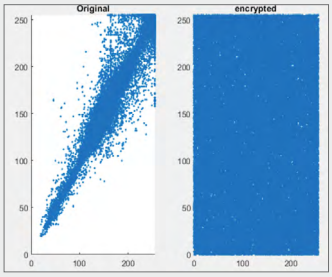
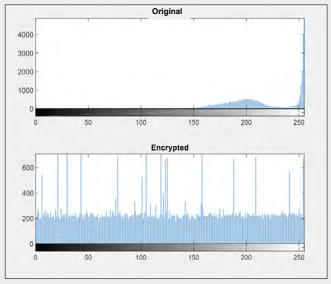
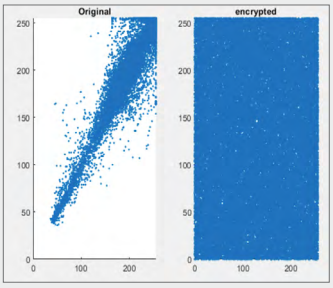
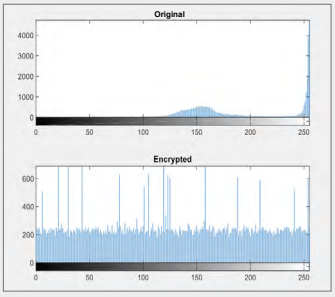
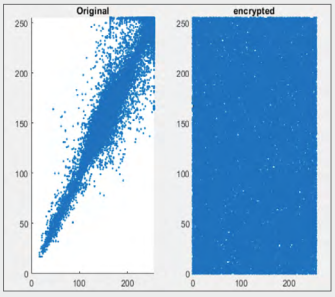
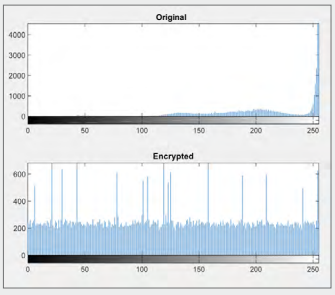
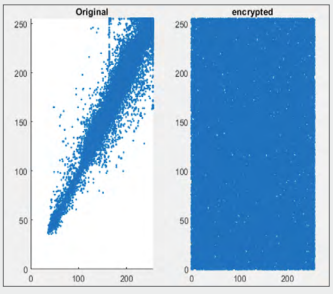
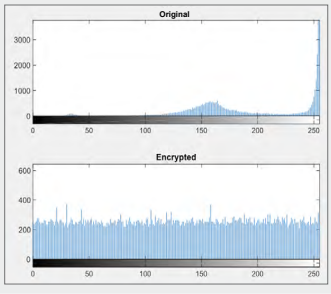
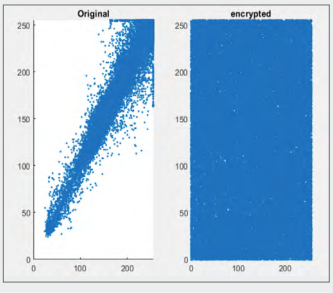
Image	Image 2	Key	Correlation of Original fused Image	Correlation of Encrypted Image	Total Encryption time (ms)	((NCPR)	(UACI)
Subject 1 glasses	Iris 1	AAAAAAAA AAAAAAAA	0.9782	-0.0206	9.172423	99.66	3.082
Subject 1 glasses	Iris 1	ABACADAE AFAA1234	0.9796	-0.0134	10.920902	99.6363	3.1735
Subject 3 glasses	Iris 3	ABACADA EAFAA1234	0.0110	0.9867	8.282109	99.6323	3.4111

Source: own elaboration.

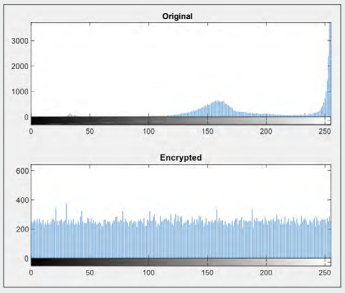
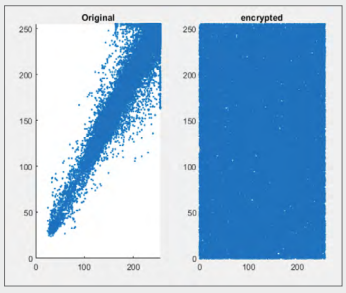
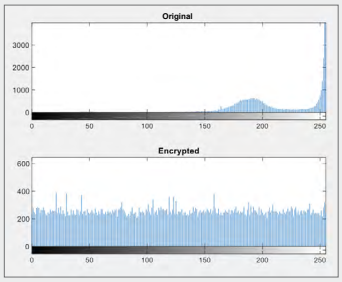
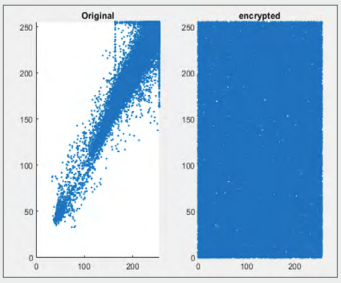
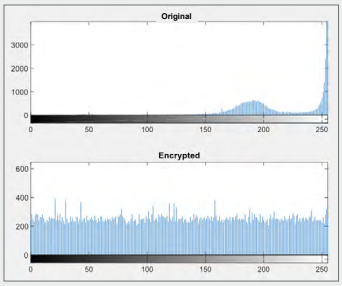
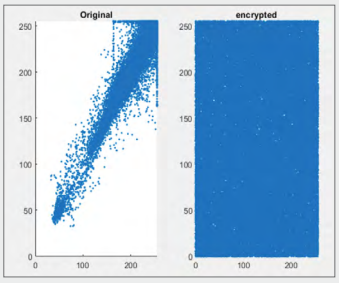
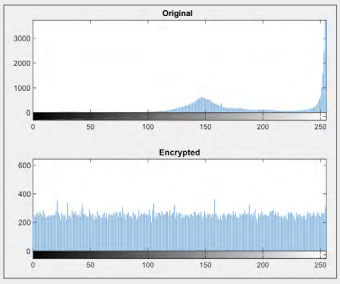
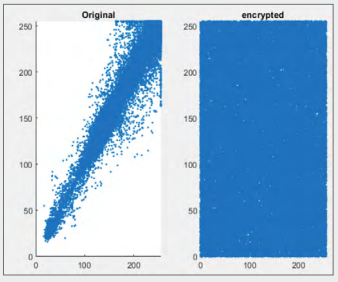
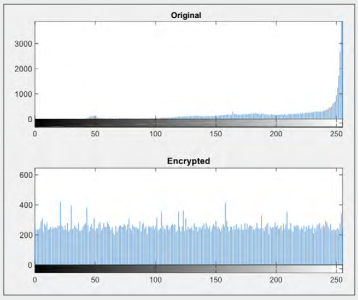
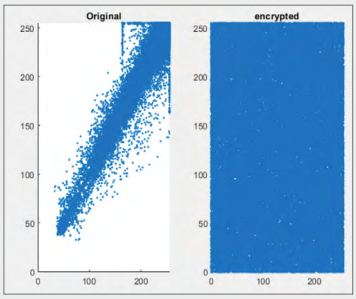
Table 3. Comparison of different correlation histograms and scatter diagrams.

Biometric-1	Biometric-2	Correlation Histogram	Scatter diagram of encryption
Yale- subject 1 with glasses	Iris 1.a		
subject 1 with glasses	Iris 1.b		

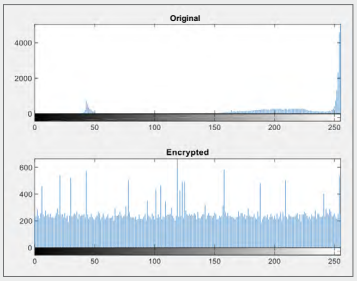
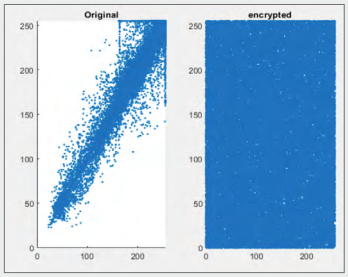
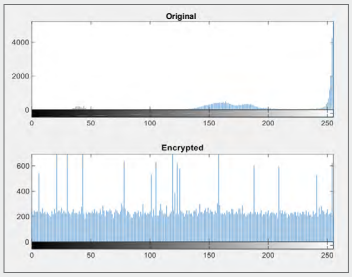
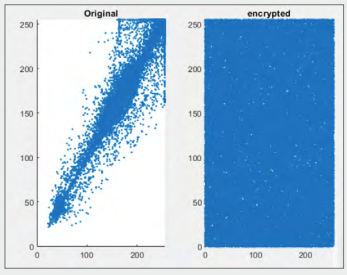
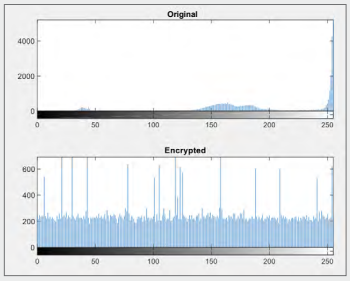
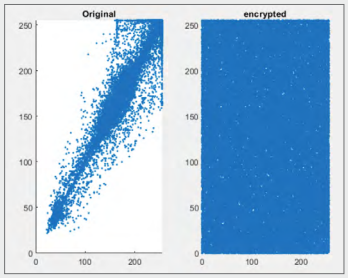
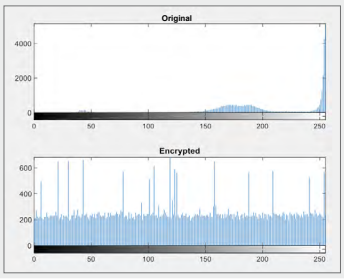
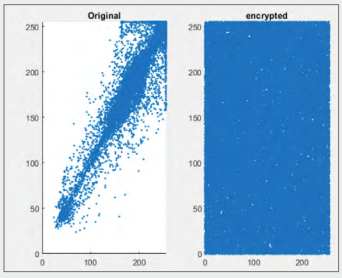
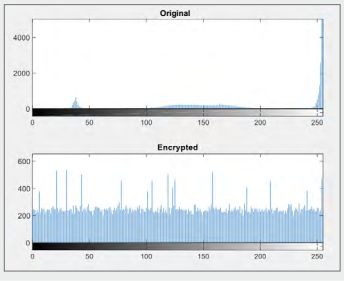
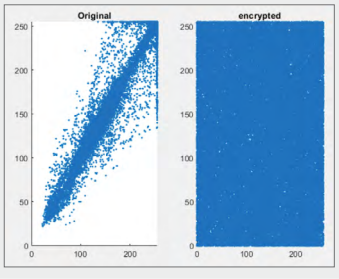
https://doi.org/10.17993/3ctecno.2021.specialissue8.513-535

subject 1 with glasses	Iris 1c		
subject 1 with glasses	Iris 1d		
subject 1 with glasses	Iris 1e		
subject 1 with glasses	Iris 1f		
Subject 2with glasses	Iris 2a		

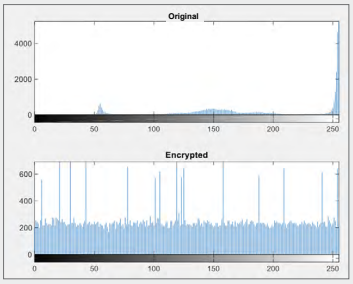
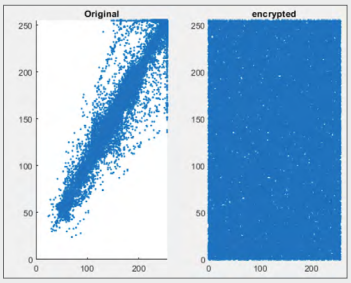
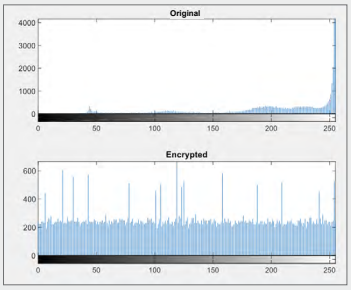
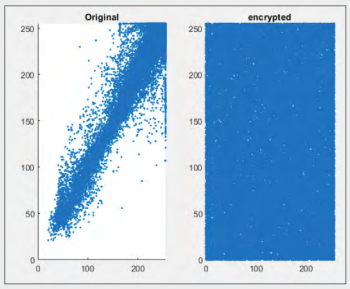
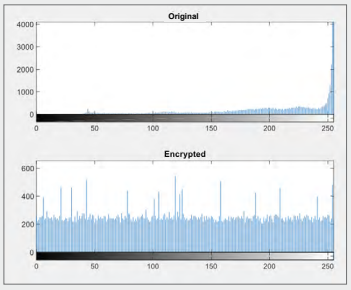
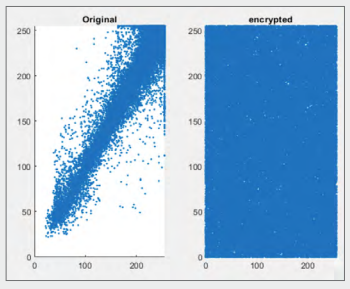
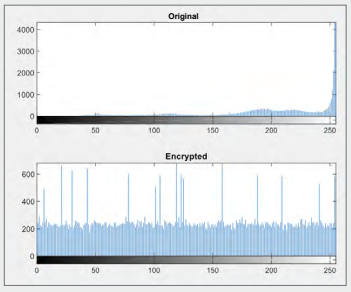
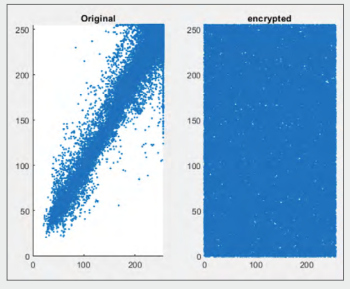
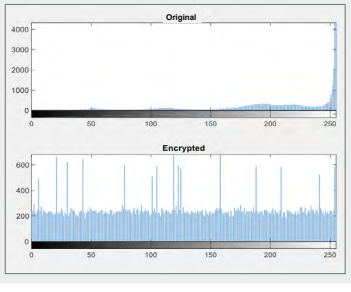
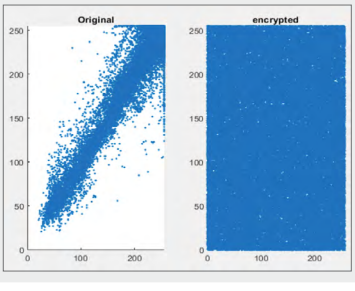
https://doi.org/10.17993/3ctecno.2021.specialissue8.513-535

subject 2 with glasses	Iris2b		
Subject 2 with glasses	Iris2c		
subject 2 with glasses	Irsi 2d		
Subject 2with glasses	Iris2e		
subject 2 with glasses	Iris 2f		

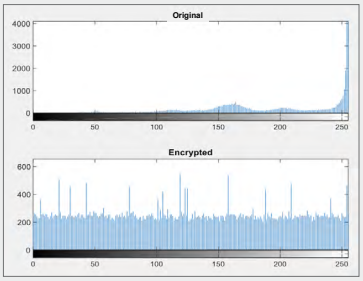
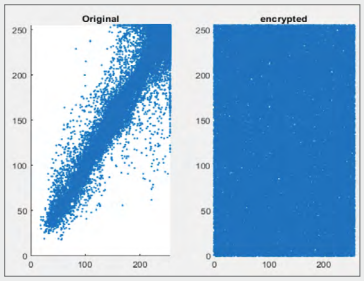
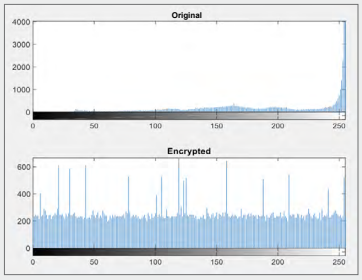
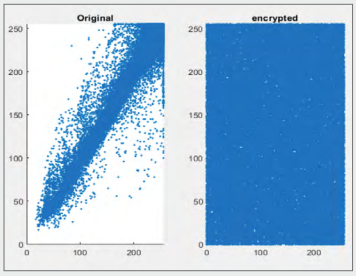
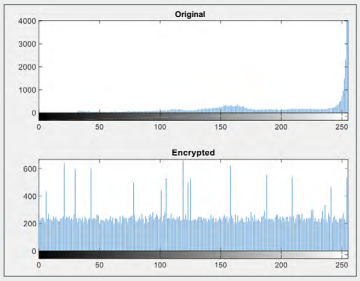
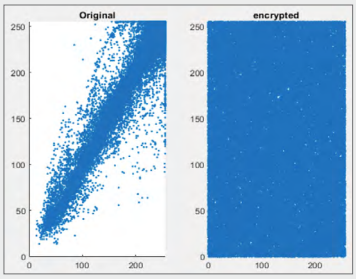
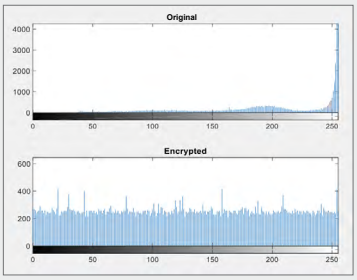
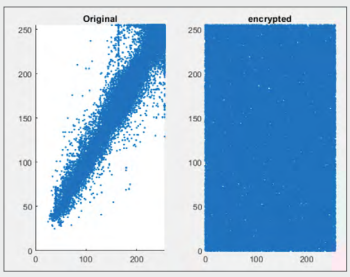
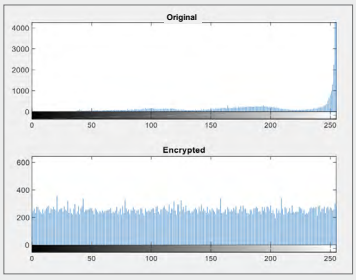
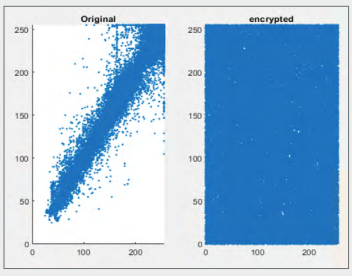
https://doi.org/10.17993/3ctecno.2021.specialissue8.513-535

Subject3 glasses	Iris 3a		
Subject3 glasses	Iris 3c		
Subject3 glasses	Iris 3d		
Subject3 glasses	Iris 3e		
Subject3 glasses	Iris3f		

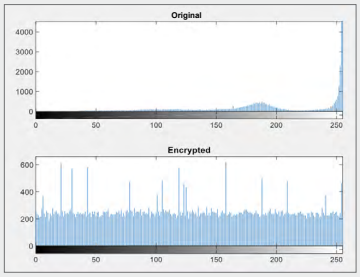
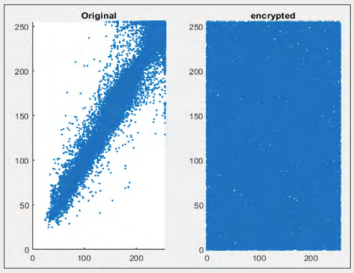
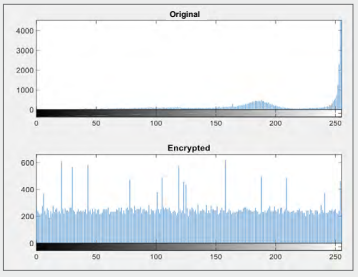
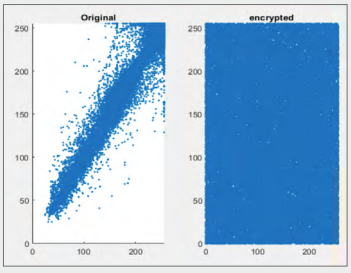
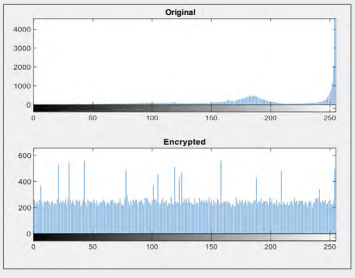
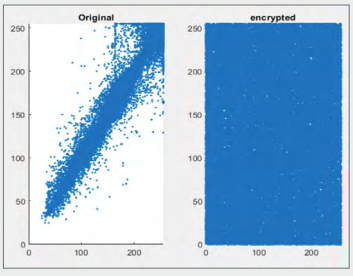
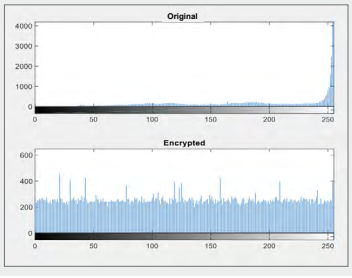
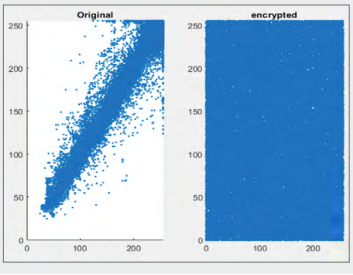
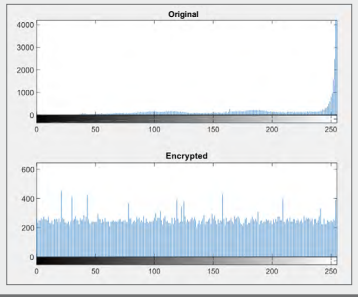
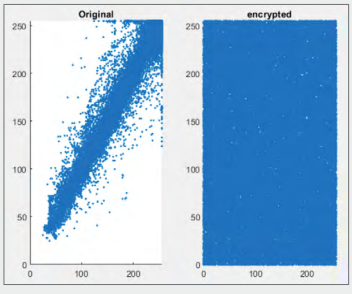
https://doi.org/10.17993/3ctecno.2021.specialissue8.513-535

Subject3 glasses	Iris 3g		
Subject4 glasses	Iris 4a		
Subject4 glasses	Iris 4b		
Subject4 glasses	Iris 4c		
Subject4 glasses	Iris 4d		

https://doi.org/10.17993/3ctecno.2021.specialissue8.513-535

Subject4 glasses	Iris 4e		
Subject4 glasses	Iris 4f		
Subject4 glasses	Iris 4g		
Subject05 glasses	Iris 5a		
Subject05 glasses	Iris 5b		

https://doi.org/10.17993/3ctecno.2021.specialissue8.513-535

Subject05 glasses	Iris 5c		
Subject05 glasses	Iris 5d		
Subject05 glasses	Iris 5e		
Subject05 glasses	Iris 5f		
Subject05 glasses	Iris 5g		

Source: own elaboration.

https://doi.org/10.17993/3ctecno.2021.specialissue8.513-535

5. CONCLUSIONS

In this algorithm, a feature level fusion method to fuse the two biometrics is introduced. Encryption algorithm to do the operations in a simple manner without the need of S-box is performed for fused image. Finally, the security parameters such as entropy, correlation, computation time, Unified averaged changed intensity, Number of changing pixel rate are calculated. As a future scope, this logic can be implemented with some public key algorithms to implement in ATM.

REFERENCES

Discrete wavelet transform. (2008). https://en.m.wikipedia.org/wiki/Discrete_wavelet_transform

ElAlami, M. E., Amin, A. E., & El-Alfi, A. E. (2012). A Personal Identification Framework based on Facial Image and Fingerprint Fusion Biometric. *International Journal of Computer Applications, 51*(7), 41-48. https://doi.org/10.5120/8058-1411

Krishneswari, K., & Arumugam, S. (2012). Multimodal Biometrics using Feature Fusion. *Journal of Computer Science, Science Publications, 8*(3), 431-435. https://doi.org/10.3844/jcssp.2012.431.435

Rajbhoj, S. M., & Mane, P. B. (2015). An Approach of Combining Iris and Fingerprint Biometric At Image Level in Multimodal Biometrics System. *International Journal of Soft Computing and Engineering, 5*(1), 102-106. https://docplayer.net/151961568-An-approach-of-combining-iris-and-fingerprint-biometric-at-image-level-in-multimodal-biometrics-system.html

Usman, M., Ahmed, I., Aslam, M. I., Khan, S., & Shah, U. A. (2017). SIT: A Lightweight Encryption Algorithm for Secure Internet of Things International *Journal of Advanced Computer Science and Applications, 8*(1), 1-10. https://doi.org/10.14569/IJACSA.2017.080151

Wu, Y., Noonan, J. P., & Agaian, S. (2011). NPCR and UACI Randomness Tests for Image Encryption. Cyber Journals: Multidisciplinary Journals in Science and Technology,

https://doi.org/10.17993/3ctecno.2021.specialissue8.513-535

Journal of Selected Areas in Telecommunications (JSAT), 31-38. https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.390.2127&rep=rep1&type=pdf

https://doi.org/10.17993/3ctecno.2021.specialissue8.513-535

https://doi.org/10.17993/3ctecno.2021.specialissue8.513-535