Journal of Theoretical and Applied Information Technology
30th April 2018. Vol.96. No 8

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

COMBINATION MATHEMATICAL DISTANCE MEASURE APPROACH FOR SOME IMAGE PROCESSING APPLICATIONS

[1] SHAHAD ADIL TAHER, [2] HIND RUSTUM MOHAMMED

[1] University Of Kufa Asst. lecturer of Computer Science And Mathematics, Department of Computer Science, Iraq

[2] University Of Kufa, prof. of Computer Science And Mathematics, Department of Computer Science, Iraq,

E-mail: [1] shahada.alkhafaji @uokufa.edu.iq, [2] hindrustum.shaaban@uokufa.edu.iq

ABSTRACT

In this paper the researcher presents a Combination mathematical Distance Measure approach for Image Encryption; it had been applied on different images . The aim of this method to protect the images by encryption them. The proposed method is depending on find a new distance between image pixels by using interpolation. The study data base consists of (40 images) of different types (color images and gray images) with different formats(. jpg, .bmp, .tif , .gif, . png). The Proposed method gave more accurate results, stronger encoding of images and high encryption efficiency via using the performance evaluation factors to evaluate labor standards and proved the successfulness of this high encryption ratios method of. MATLAB® 2010 software had been highly relied in this study.

Keywords: *Image processing, Image encryption, Distance Measure, Performance analyses image*

1. INTRODUCTION

Image processing field concerned with the development and use of methods and algorithms for images processing digital. In this research we focused on image processing applications. Digital image encryption occupied a great deal of importance in the security and military fields. Encryption is one of the branches of mathematics that converts the messages information into unreadable form, no one can read it except the intended recipient who must has the decode to decipherer or decrypt the encrypted data. Encryption requires operations that are easy to perform one way called encoding yet nearly impossible to perform the other way called decoding without key. [1].

Image Cryptosystem can be classified into two main sections first for encryption and second for decryption. The block cipher and stream cipher are two types of cryptosystem, so private key and public key are two strategies to be used in an encryption[2] .

The paper is organized as following: section 2 discussion of the definitions, section 3 the researchers presented the Common distance measures for encryption, the proposed image encryption method is described in section 4, while in section 5 the results of the experiment are discussed and evaluated. Performance analyses Measures in section 6,Finally, the conclusions are expressed in Section 7.

2. DEFINITIONS

2.1 Correlation Of Raw Scores And Means[3]

The mathematical formula for this important measure which is invariant to linear transformations of either variable, it is developed first by Pearson in 1895:

$$r = \frac{\sum(t_i - \bar{t})(s_i - \bar{s})}{\left[\sum(t_i - \bar{t})^2 \sum(s_i - \bar{s})^2\right]^{\frac{1}{2}}} \qquad (1)$$

where $\bar{t}, \bar{s}$ are mean value of t_i, s_i respectively.

If r = 1, then the Correlation coefficient is very strong in positive .

If r = 0, then the Correlation coefficient is very week . (i.e. good encryption).

If r = -1 then the Correlation coefficient is very strong in negative

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

2.2 Peak signal-to-noise ratio (PSNR) [4], [11].

Given original image O and t a test image, both of size M×N, the PSNR between o and t is defined by:

$$\mathrm{PSNR}\ (o,t) = 10\log_{10}\frac{255^2}{\mathrm{MSE}\ (o,t)} \qquad (2)$$

-for Maximum intensity of 256*256 images is 255(0 to 255)

Where (MSE) is Mean square error and given by :

$$\mathrm{MSE} = \frac{1}{MN}\sum_i^M\sum_j^N\left(o_{ij} - t_{ij}\right)^2 \qquad (3)$$

2.3 Histogram: [5]

Let $w = \{w\ (i,j)\}$ is an image that is composed of S discrete gray levels denoted by $\{w_0, w_1, \dots, w_{S-1}\}$. Here, $w(i,j)$ represents the intensity of the image at spatial location (i,j) with the condition that $w\,(i,j)\ \epsilon\ \{w_0, w_1, \dots, w_{S-1}\}$. The histogram (h) is defined as:

$$\mathrm{h}(\mathbf{w}_c) = n_c \qquad c = 0,1,2 \dots\dots L-1 \qquad (4)$$

Where

w_c: the c-th gray level.

n_c : the number of times that the gray level w_c.

2.4 Histogram Equalization:[6]

The Mathematical formula of the discrete form of the transformation function for histogram equalization is given by:

$$Y_C = G(r_C) = \sum_{j=0}^{C}\frac{m_j}{M} = \sum_{j=0}^{C}R_r(r_j)\,,$$

$$0 \le r_C \le 1\,, C = 0,1,2, \dots\dots\dots, l-1 \qquad (5)$$

Where

m_j: the number of times the j^th gray level.

l : the gray levels number.

$R_r(r_j)$: the probability of the j th gray level .

M: the total number of pixels .

2.5 Structural similarity index (SSIM) [7].

Structural similarity index contain three comparison functions known for: luminance comparison, contrast comparison, and structure comparison between two signals a and b :

$$k(a,b) = \frac{2\mu_a\mu_b + c_1}{\mu_a{}^2 + \mu_b{}^2 + c_1}, c(a,b) = \frac{(2\sigma_a\sigma_b + c_2)}{\sigma_a{}^2 + \sigma_b{}^2 + c_2},$$

$$s(a,b) = \frac{(\sigma_{ab} + c_3)}{\sigma_a\sigma_b + c_3} \qquad (6)$$

which the relative importance of the three components define as :

$$SSIM(x,y) = \frac{(2\mu_a\mu_b + c_1)(2\sigma_{ab} + c_2))}{(\mu_a{}^2 + \mu_b{}^2 + c_1)(\sigma_a{}^2 + \sigma_b{}^2 + c_2)} \qquad (7)$$

Where μ_a , μ_b are the means of a and b, and σ_a , σ_b are the standard deviations of a and b, respectively, and $\sigma_{ab}$is the correlation coefficient between a and b. The constants c_1 , c_2 , and c_3 are used to stabilize the algorithm when the denominators approach to zero ,s.t:

$$\mu_a = \frac{1}{S}\sum_{i=1}^{S}a_i,\ \ \mu_b = \frac{1}{S}\sum_{i=1}^{S}b_i\,, \sigma_a = \left[\frac{1}{S-1}\sum_{i=1}^{S}(a_i - \mu_a)^2\right]^{\frac{1}{2}},$$

$$\sigma_b = \left[\frac{1}{S-1}\sum_{i=1}^{S}(b_i - \mu_b)^2\right]^{\frac{1}{2}}$$

(8)

3. TYPES OF DISTANCE MEASURES FOR ENCRYPTION

Distance in matric space :

Let Z be a set a function C : Z × Z → R is called a distance (or dissimilarity) on Z if, for all s, z ∈ Z, there holds:

. C(s, z) ≥ 0 (non-negativity), C(s, z) = C(z, s) (symmetry), C(s, s)=0 (reflexivity) **[8]** .

A common distance measures:

3.1 Euclidean distance [9]:

is defined by Euclidean as

$$D_{\mathrm{Euclidean}}(x_i, x_j) = \sqrt{\sum_{k=1}^{d}(x_{ik} - x_{jk})^2} \qquad (9)$$

3.2 Manhattan (or City-Block) Distance, L1 distance [9].

proposed by Minkowsky is defined by:

$$D_{\mathrm{Manhattan}}(x_i, x_j) = \sum_{k=1}^{d}\left|x_{ik} - x_{jk}\right| \qquad (10)$$

3.3 Mahalanobis Distance

this distance between two vectors x_i, x_j is given by

$$D_{\mathrm{Mahalanobis}}(x_i, x_j) = \sqrt{(x_i - x_j)^T\ \Sigma^{-1}(x_i - x_j)} = \sqrt{\sum_{k=1}^{d} x_{ik}\sum_{i=1}^{-1} x_{ji}}$$

(11)

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

3.4 Chebychev Distance (or chessboard Distance)

is defined by :

$$D_{\text{Chebychev}} = max_k |x_{ik} - x_{jk}| \qquad (12)$$

3.5 Minkowski Distance

The distance is given by :

$$D_{\text{Minkowski}}(x_i, x_j) = \sqrt[p]{\sum_{k=1}^{d} |x_{ik} - x_{jk}|^p} \qquad (13)$$

when p = 1 ,2, ∞ this yields the Manhattan, Euclidean and Chebychev distances respectively **[10].**

4. PROPOSED METHOD

The two points **W** and **M** in two dimensional Euclidean spaces and **W** with the coordinates (**w_1, w_2), M** with the coordinates (**m_1, m_2**). The line segment with the endpoints of **W** and **M** will form the hypotenuse of a right angled triangle. The distance is defined by :

$$\mathbf{D(W, M)} = \left|\mathbf{1 - \tan\sqrt{(m_1 - w_1)^2 + (m_2 - w_2)^2}}\right| \qquad (14)$$

The proposed method will be called " **Shahad .A .H**"

5. E XPERIMENTS AND RESULTS

In this section we will analyze the effect of some prescriptions on image components as follows:
1- The effect of all distance, on the original image.
2 - Histogram . 3 - Histogram equalization.

Figure 1 showed direct effect of all distances on the pixels of plain image in Combination mathematical Distance Measurement approach.

Figure 2 showed the effect of distances on the plain image , showed that in terms of image shape the proposed distance of the aggregate method is best in hiding all the main image features with the image internal parts.

While figure number 3 showed the effect of histogram criterion on the plain image and encrypted images. The figure shows that Chebychev distance (or chessboard distance) containing histogram parameters followed by Manhattan (or City-Block), Euclidean distance and **Shahad. A.H** distance. The histogram in **Shahad. A.H** distance hides all internal components and surrounding areas then the image appeared as an encrypted image.

Figure 4 exhibits the original image and the encrypted images, shows the difference between the images that had been encrypted by the previously mentioned methods and the image that is encrypted by **Shahad. A.H** whatever the type of image, colored or gray, or indexed or bilateral, with the different extension of image, where, in previously mentioned methods the effect of Histogram equalization was almost noted, while in **Shahad. A.H**. it was so clear.

Figure 5 showed one case(cameraman image) of intersection points of the original and encrypted images sequentially began with the Shahad .A.H method followed by Chess board, the City block and finally Euclidean methods.

Figure 6 reviews a collection of (Portrait photography with very high resolution and clarity indicating the significant difference between the effect of distances relative to the proposed method.

6. PERFORMANCE ANALYSES MEASURES

In order to calculate the performance of Shahad. A.H method and use the new distance to encrypt the image, the researchers use the mean square error(MSE) , Peak Signal to Noise Ratio (PSNR) ,Correlation Coefficient and Structural Similarity Index(SSIM). Table 1 showed the performance results which demonstrated the efficiency of Shahad. A.H method of coding with mean square error(MSE) , Peak Signal to Noise Ratio (PSNR), while table 2 showed the performance results which demonstrated the efficiency of (Shahad. A. H)method of coding with Correlation Coefficient and Structural Similarity Index(SSIM),
We also demonstrated the similarity between the original image (Portrait photography)of high-resolution images and the encoded image in a certain way, where it proved that the least similarity is between the (Shahad. A. H) method and the original image as shown in table 3.
Note: Figures 1,2,3,4,5 and 6 with Table 1,2 ,3in the end of paper .

7. CONCLUSION.

This paper proposed a Combination mathematical Distance Measure approach to Image Encryption; it is named (Shahad. A.H), found very efficient and active in encrypting any type of image and any size by applying equation No. 14.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

For Image Quality evaluation the researcher used Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR), Correlation Coefficient and Structural Similarity Index(SSIM) .

The results of the first criterion(Mean Square Error (MSE)) Shahad. A. H method gives very high difference for all other cases in table(1): 5338.63733683551,623.36145441012,113.1185420 69761. Then City block method gives high difference Followed by Euclidean method. Chessboard gives the less (MSE), where the error was zero.

For a good encrypted image the value of (MSE) must be high, and the (PSNR) must be low that is to say an inverse relation between them. Note Eq. (2).

Shahad. A. H method gives lowest (PSNR) for all cases in table(1): 10.856499414074, 20.1834041672006, 27.5954656179078, followed by city block method and Euclidean method. Chessboard gives the highest (PSNR) where equal infinity.

The results of the third criterion(Correlation Coefficient)is :By the def.(3) ,If r = 0, that means the encrypted image is completely different from the original (i.e. good encryption) , Shahad. A. H method gives low (Correlation Coefficient) near to zero for all cases in table(2): 0.0194845942730301, 0.0506777176381649 , 0.0321563703417517, followed by city block method , Euclidean method. Chessboard gives the highest (Correlation Coefficient) where it is equal 1and that means the original image and the encoded one are identical.

The results of the fourth criterion(Structural Similarity Index(SSIM))is: in table 2 Shahad. A. H method gives the lowest value of (SSIM): 0.178959110580514, 0.36029683383587, 0.241952832794539, respectively and that means the similarity between the two images (the original and the encrypted one) in Shahad. A. H method is very weak, for more accuracy and to support the method provided, we took the Portrait photography is one of the most common forms of photography, in which the beauty of a person (whether a child, a young man or a girl) is highlighted, and the focus of their gaze or way of standing or any particular style they prefer to take pictures as in table **3**

the amount of similarity between the encryption images and the original image by applying the definition (**2.5**) of SSIM.

We found that the most similar method is Chessboard was equal **1,1,1** in all cases

And then the Euclidean method was equal **0.9227, 0.9208, 0.9262**

The least of them is the city block method were equal **0.2852, 0.1316, 0.2807**

The proposed method(Shahad. A. H) has shown the weakest similarity of all the above was equal **0.0211, 0.0790, 0.0237**. this gives support to our method as It does not match the original image, hence we achieved our aim of the method which is to hide all the original features of the image so as to be unreadable.

REFRENCES

[1] J. c. Stillwell, “Mathematics and Its History”, Third Edition, Springer-Verlag New York, 2010 .

[2] W. Y. Noonan J, and Agaian S., “NPCR and UACI randomness tests for image encryption”, of Selected Areas in Telecommunications (JSAT), pp. 31–38,2011

[3] J. L. Rodgers, W.A. Nicewander, “Thirteen Ways to Look at the Correlation Coefficient”, The American Statistician, Vol. 42, No. 1, pp.59-66, February 1988 .

[4] A. Horé and D. Ziou, “Image quality metrics: PSNR vs. SSIM', IEEE Computer Society , ISBN 978-0-7695-4109-9,2010.

[5] M. L. Najman, J. Facon, and A. de A. Ara´ujo, “Multi-histogram equalization methods for contrast enhancement and brightness preserving,” Consumer Electronics, IEEE Transactions on, vol. 53, no. 3, pp. 1186–1194, 2007.

[6] A. A. Rani1 ; G. Rajagopal2 ; A. Jagadeeswaran3 , “Bi-Histogram Equalization with Brightness Preservation Using Contras Enhancement”, International Journal of Basic and Applied Science, Vol. 02, No. 03, ,pp.21-30 Jan 2014.

[7] Z. Wang, A.C. Bovik , H.R.Sheikh, and E.P.Simoncelli, “Image quality assessment: From error measurement to structural similarity”, IEEE Transaction on Image Processing, 13 (4), 600-612,2004.

[8] M. M. Deza ,E. Deza , “Encyclopedia of Distances”, Springer-Verlag Berlin Heidelberg 2009.

[9] R. Zhang, Z. Zhang, K. Liu , J. Zhang , “Proceedings of 3rd International Conference on Logistics”, Informatics and Service Science, Liss2003.

[10] T. Hertz, “Learning Distance Functions: Algorithms and Applications”, Thesis for the degree of Doctor of PHILOSOPHY, Submitted

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

to The Senate of The Hebrew University Of Jerusalem December 2006.

[11] R.Srivastava1, O. P. Singh2, “Performance Analysis of Image Encryption Using Block Based Technique”, IJAREEIE,Vol. 4, Issue 5, May 2015.

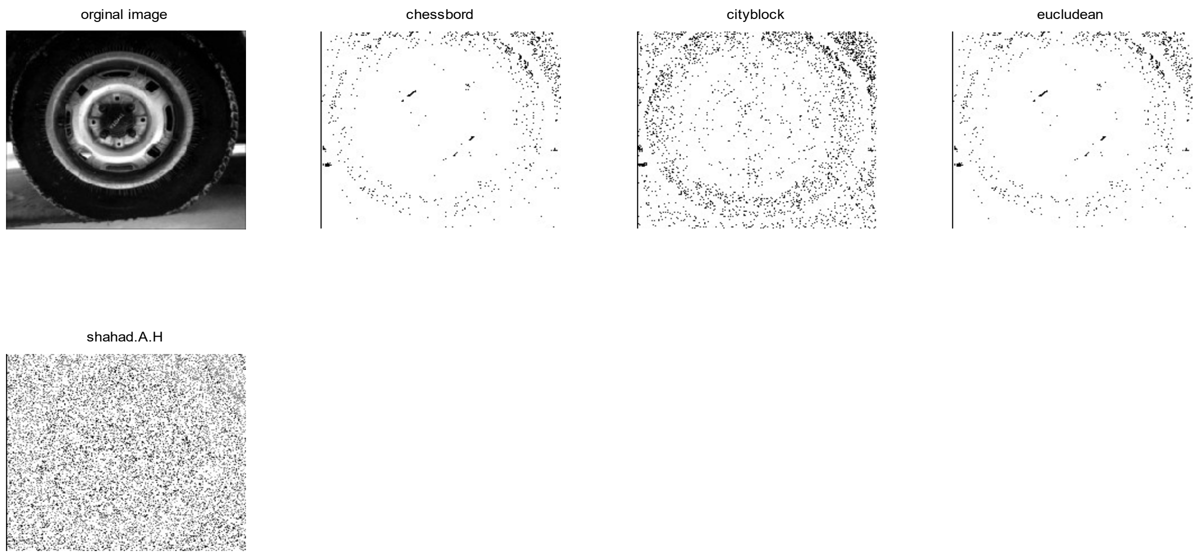


Figure 1: Direct effect of all distances on the pixels of plain image .

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

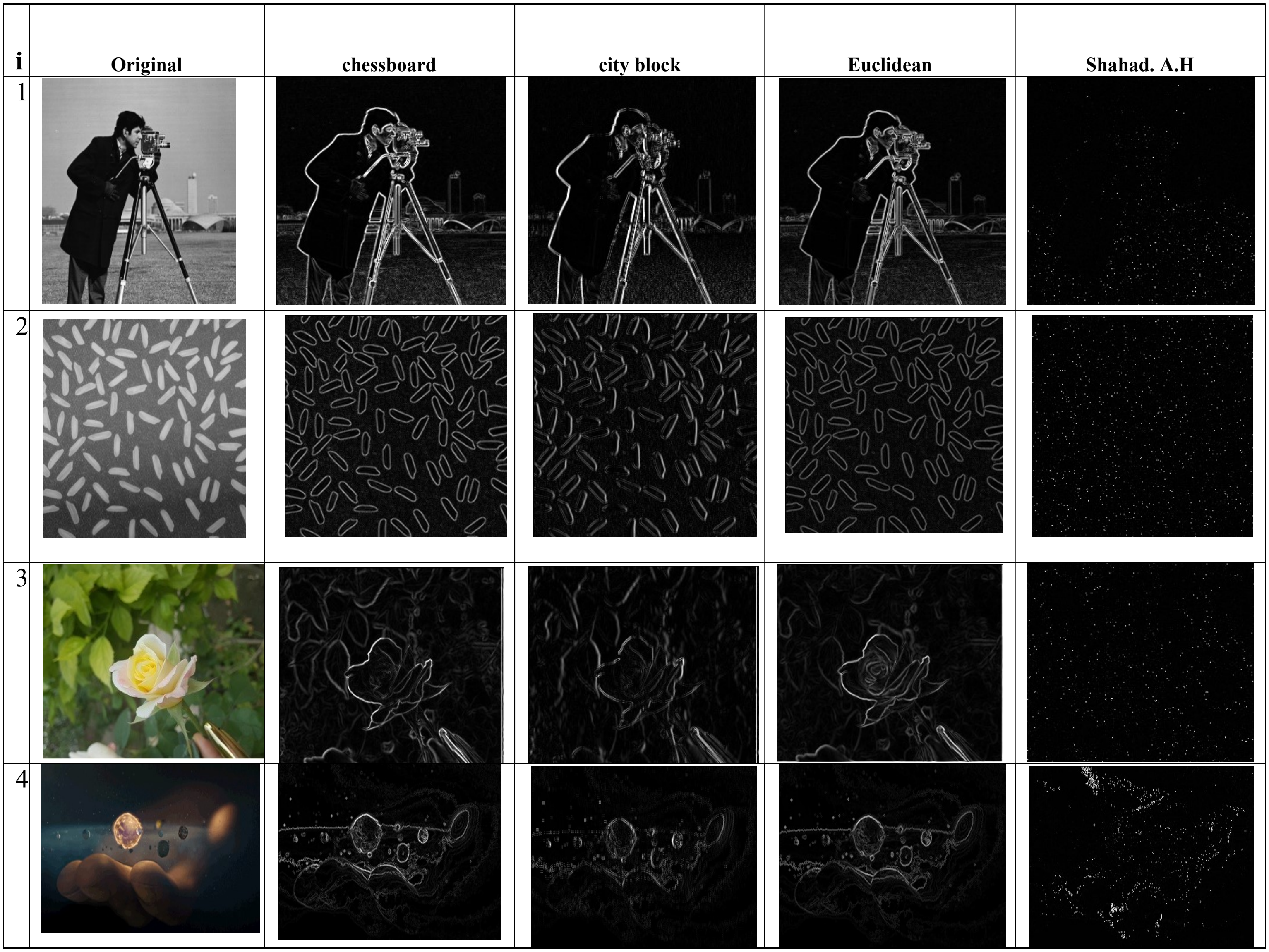


Figure 2: The effect of distances on the plain image.

Journal of Theoretical and Applied Information Technology
30th April 2018. Vol.96. No 8

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

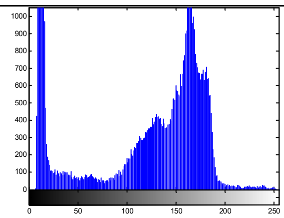
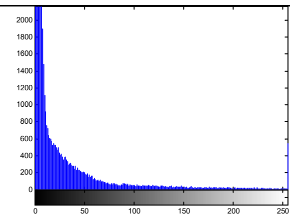
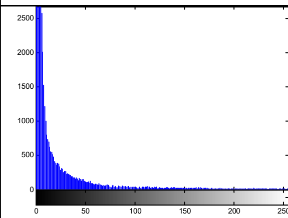
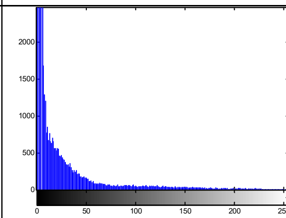
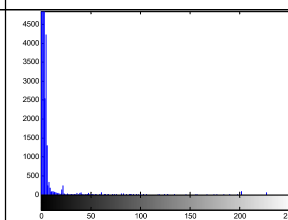
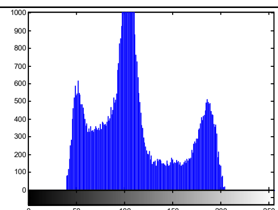
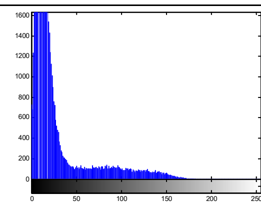
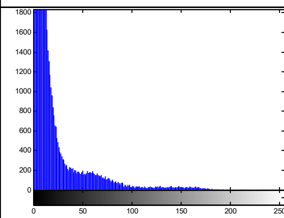
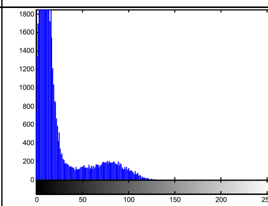
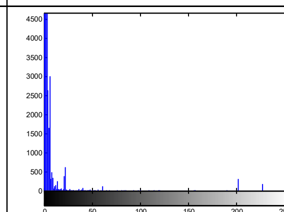
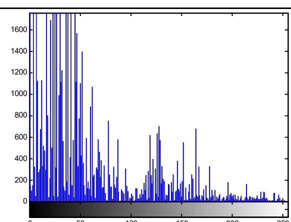
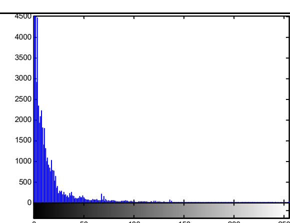
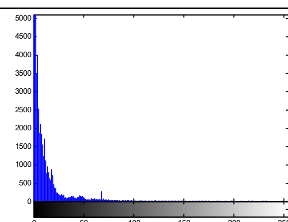
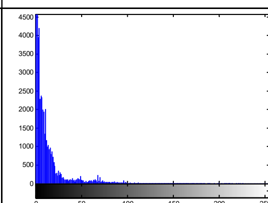
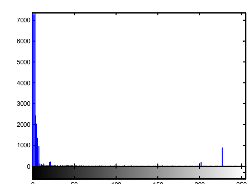
	Original	chessboard	city block	Euclidean	Shahad. A.H
1					
2					
3					

Figure3: The effect of histogram criterion of the plain image and encrypted images

Journal of Theoretical and Applied Information Technology
30th April 2018. Vol.96. No 8

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

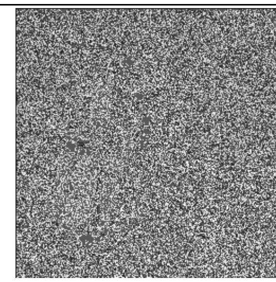
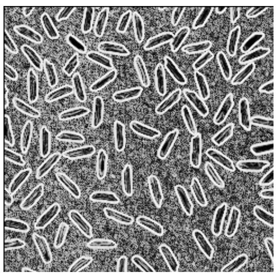
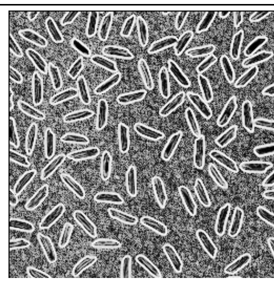
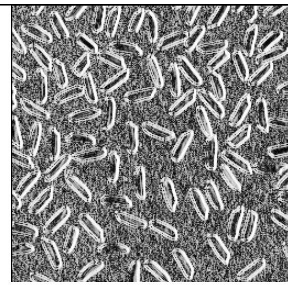
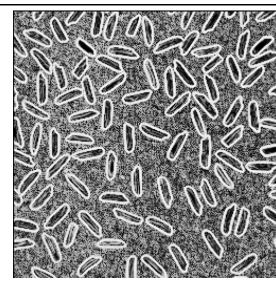
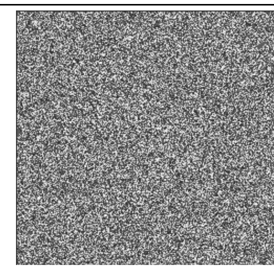
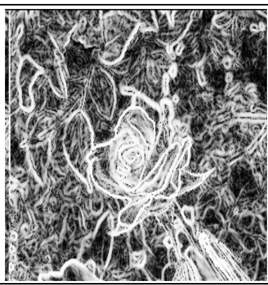
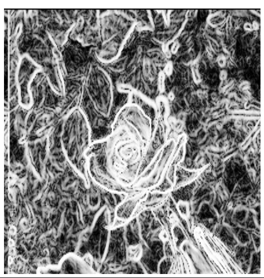
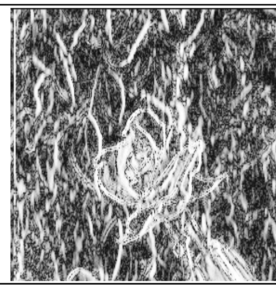
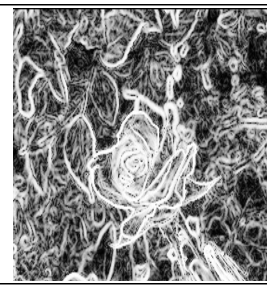
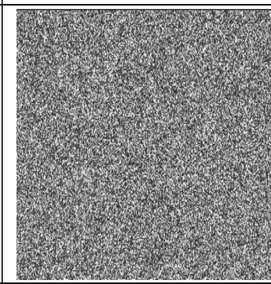
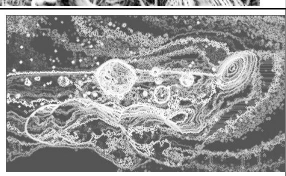
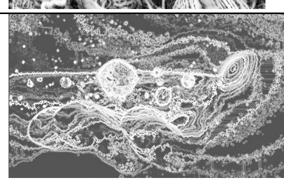
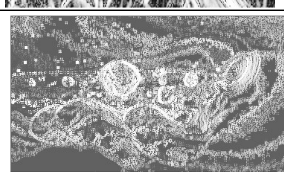
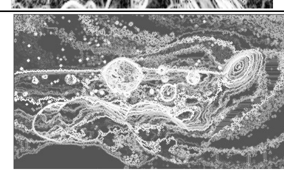
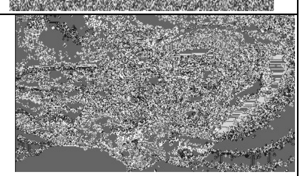
i	Original	chessboard	city block	Euclidean	Shahad. A.H
1					
2					
3					
4					

Figure 4: The effect of Histogram equalization of the plain image and encrypted images.

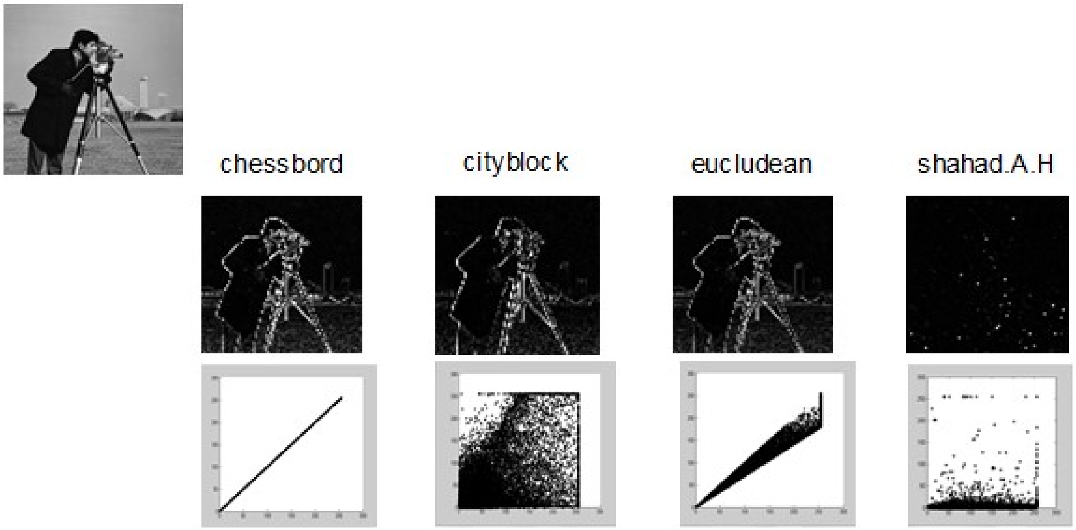


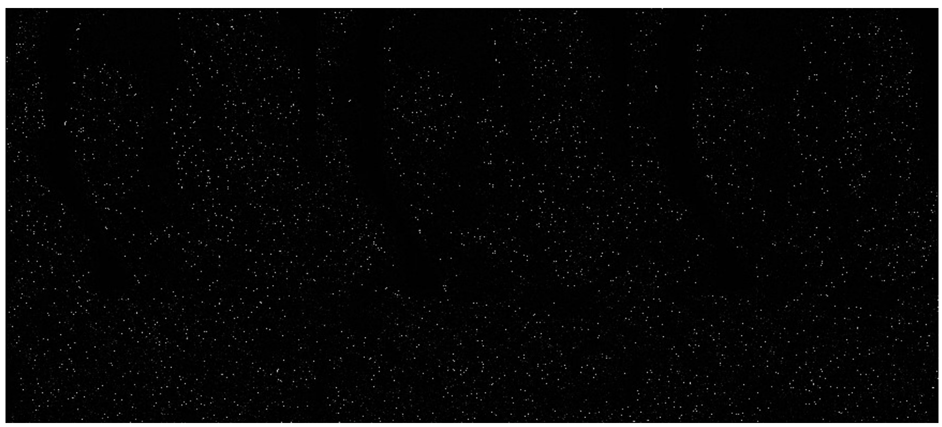
Figure 5: correlation between the original image with all methods of encryption

orginal image

Chess bord

cityblock

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

orginal image 	eucludean  shahad.A.H 

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

orginal image

chessbord

cityblock

eucludean

shahad.A.H

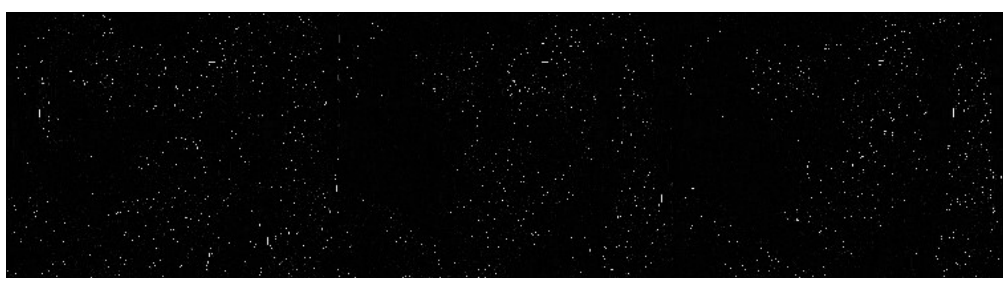


Figure 6 : demonstrates the effectiveness of the method provided in encrypting a set of Portrait photography taken with high quality and accuracy compared to other methods.

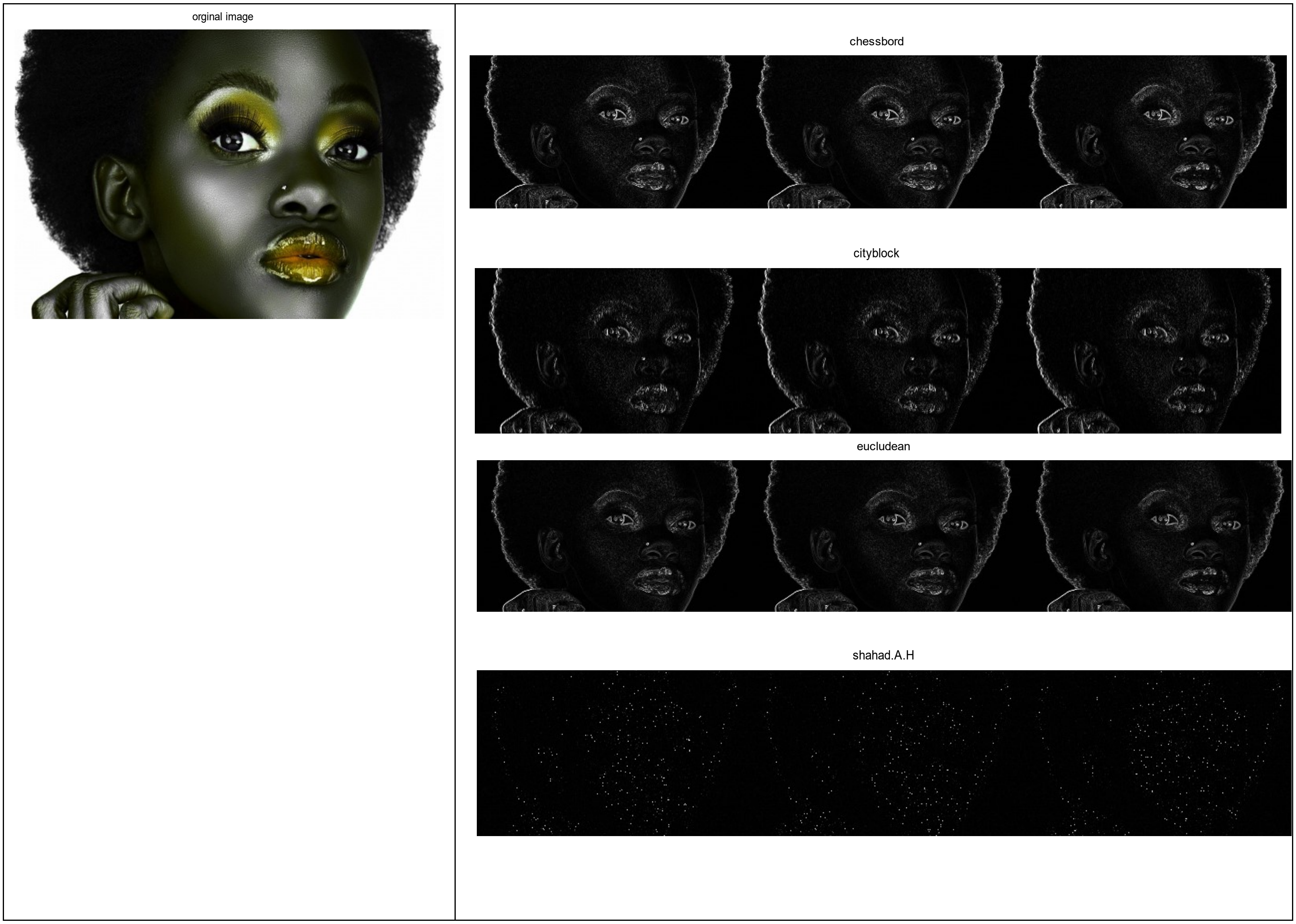


Table 1 : Efficiency of the proposed method of coding with (mean square error(MSE)) , (Peak Signal to Noise Ratio (PSNR))

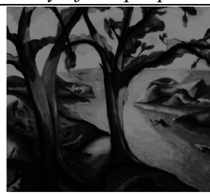
						
	MSE	**PSNR**	**MSE**	**PSNR**	**MSE**	**PSNR**
Original	0	∞	0	∞	0	∞
chessboard	0	∞	0	∞	0	∞
city block	196	25.2082428951143	196	25.2082428951143	81	29.0459534198926
Euclidean	23.2235105946375	34.4715249014074	33.7605145774771	32.8467130335103	10.4307708004678	37.9476395828789
Shahad. A.H	5338.63733683551	10.856499414074	623.36145441012	20.1834041672006	113.118542069761	27.5954656179078

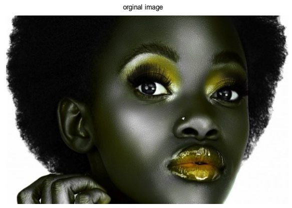
Table2: Efficiency of the proposed method of coding with Correlation Coefficient and Structural Similarity Index(SSIM).

						
	SSIM	**Coralation Coefficient**	**SSIM**	**Coralation Coefficient**	**SSIM**	**Coralation Coefficient**
Original	1	1	1	1	1	1
chessboard	1	1	1	1	1	1
city block	0.42500100948725	0.575759749984599	0.573786245326249	0.688547616336875	0.566104395917543	0.61703581692421
Euclidean	0.947334006967885	0.990635992943151	0.955362892270954	0.991843097922171	0.945289232739296	0.991726064416956
Shahad. A.H	0.178959110580514	0.0194845942730301	0.36029683383587	0.0506777176381649	0.241952832794539	0.0321563703417517

Journal of Theoretical and Applied Information Technology
30th April 2018. Vol.96. No 8

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table3: Structural Similarity Index(SSIM) between the Portrait photography and Encrypted images .

orginal image 					orginal image 					orginal image 			
SSIM					**SSIM**					**SSIM**			
Chessboard	**Euclidean**	**Cityblock**	**Shahad.A.H**		**Chessboard**	**Euclidean**	**Cityblock**	**SHAHAD.A.H**		**Chessboard**	**Euclidean**	**Cityblock**	**Shahad.A.H**
1	**0.9227**	**0.2852**	**0.0211**		**1**	**0.9208**	**0.1316**	**0.0790**		**1**	**0.9262**	**0.2807**	**0.0237**