

A New Random Sequence using Descriptor of Fourier for Image Encryption

¹N. Benmessaoud, ¹N. Hadj-Said, ¹A. Ali-Pacha and ²M. Benmessaoud

¹Department of Electronic, Laboratory of Coding and Security Information,
Université des Sciences et de la Technologie d'Oran («MB»), Algérie, Algeria

²Department of Electronic, Ecole Nationale Polytechnique d'Oran, Algérie, Algeria
nabila.benmessaoud@univ-usto.dz

Abstract: The digital revolution has created the much easier ways for treatment, storage and transmission of digital images. However, it has also created the means of forgery, counterfeit and highly advanced spy. The increasing use of images in industrial processes has become necessary to secure and protect the confidentiality of these images against unauthorized access before transmitting. In this study, we propose an image encryption method based on the use of Fourier descriptor and Chaos theory. In this method, a chaotic noise is applied to the image and a series of operations are performed in order to generate a new random sequences based on Fourier descriptor which will be used after for image encryption.

Key words: Encryption, Fourier descriptor, logistic map, random sequence, Chaos theory, industrial

INTRODUCTION

Securing information is a research topic for which there is currently a renewed interest it is the main concern in today's world, so, it is important to secure data from unauthorized access. Data encryption is often used to ensure security in open networks such as the internet. Each type of data has its own features, therefore, different techniques should be used to protect confidential image data from unauthorized access (Abugharsa *et al.*, 2011). In recent years, access to image stream through the world has become possible via. modern means of communication (Internet), so, it has become very essential to protect them against all attacks and leaks. Several applications such as military bases of images, confidential video conference, medical imaging systems, personal photos, etc., require reliable, robust and fast security systems to ensure their privacy (Pareek *et al.*, 2006). Encryption is the favorable technique for the protection of transmitted data.

There are various encryption systems for encrypting and decrypting the image data, however, it can be said that there is no single encryption algorithm that satisfies the various types of images (Li and Zheng, 2002). An optical encryption methods have been proposed by researchers Unnikrishnan and Singh (2000), Al-Qaheri *et al.* (2010), Refregier and Javidi (1995), Unnikrishnan and Singh (2001) among them, the

optical encryption system very widely used and successful. This system which is proposed by Refregier and Javidi (1995) is twice random phase encoding. The method uses two random phase masks, one in the entrance plane and the other in the Fourier plane to encrypt the primary image. Younes and Jantan (2008) presented an image encryption algorithm which was the combination of permutation technique followed by encryption. They introduced a new permutation technique based on the combination of image permutation and the well known encryption algorithm called Rijndael. The original image was divided into 4 by 4 pixels blocks which were rearranged into a permuted image using a permutation random process and then the generated image was encrypted using the Rijndael algorithm. The results showed that the correlation between the image elements was significantly decreased by using the combination technique and higher entropy was achieved. Kushwaha and Roy (2010) proposed a scheme to encrypt data for secure image using a combination of double encryption process based on the combination of encryption by pixel position (x, y) and another encryption for blocks. The transformation process used is meant to divide the original image into a number of blocks which are then encrypted by their position with another pixel in the image. The resulted image then becomes the input of the algorithm for public key encryption. By transferring the correlation and the entropy as the security setting,

encryption process is performed using their pixel position (x, y) and the AES encryption algorithm encrypts each block using the recipient's public key. Bu and Wang (2004) and Chee *et al.* (2004) have used the chaotic encryption schemes chaotic systems have many important properties such as sensitivity to initial conditions and system parameters, pseudo-random property not periodicity and transitivity topology, etc. (Gao *et al.*, 2006). By Ashutosh (2013) the continuous FFT has been proposed with the double random phase coding method for improving data security. The image encryption is based on FFT and DFT and decryption with the same transformed order. Zhang and Xiao (2014) have proposed a novel image encryption scheme based on rotation matrix bit-level permutation and block diffusion. Firstly, divide plain image into non-overlapping 8×8 pixels blocks with a random matrix then transform each block into an 8×8×8 3-Dimensional (3-D) binary matrix which has six directions just as a cube. Permutation is performed by multiplying the 3-D matrix by the rotation matrix that relies on plain image, according to different direction. Secondly, use block diffusion to further change the statistical characteristics of the image after confusion. Xu *et al.* (2016) presented a novel bit-level image encryption algorithm that is based on Piecewise Linear Chaotic Maps (PWLCM). First, the plain image is transformed into two binary sequences of the same size. Second, a new diffusion strategy is introduced to diffuse the two sequences mutually. Then they swapped the binary elements in the two sequences by the control of a chaotic map which can permute the bits in one bitplane into any other bit plane. Zhen *et al.* (2016) proposed a secure image encryption scheme based on logistic and spatiotemporal chaotic systems. The extreme sensitivity of chaotic system can greatly increase the complexity of the proposed scheme. Furthermore, the scheme also takes advantage of DNA coding and eight DNA coding rules are mixed to enhance the efficiency of image confusion and diffusion. To resist the chosen-plaintext attack, information entropy of DNA coded image is modulated as the parameter of spatiotemporal chaotic system which can also guarantee the sensitivity of plain image in the encryption process.

In this communication, we propose a method of encryption and decryption based on the use of logistic map which is used to confuse the pixels of plain image by a chaotic noise then a series of operations are applied to an image gallery to extract the contours contained in these images then we apply the Fourier descriptor on the coordinates of these contours to get a complex representation coordinates that will be used for generating a new ideal random sequences which are used

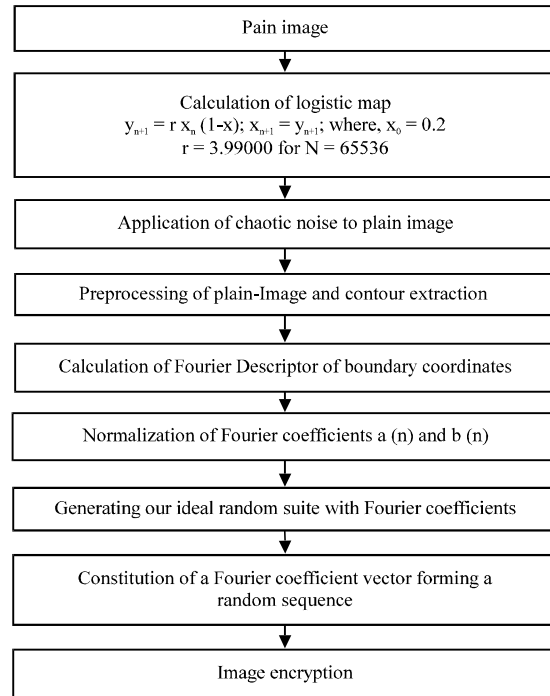


Fig. 1: Diagram of the steps of the proposed encryption method

finally for encrypting and decrypting process. Figure 1 shows the proposed architecture of our image encryption/decryption system.

MATERIALS AND METHODS

Figure 1 shows the steps used for our image encryption method. For decryption, the restitution of information is done through a series of reverse operations to those proposed above.

Image preprocessing: A set of operations are performed on the original image to improve its quality and then a step of extracting the contours and the coordinates (x, y) is made. The following diagram shows the various stages of pretreatment (Fig. 2).

Filtering and thresholding: The first step in the pretreatment is thresholding. An image binarization is performed by applying a simple threshold after many tests we took a threshold of 130 to get to convert the original images to binary images. The images obtained are filtering to make a noise suppression that eliminates isolated pixels and smaller areas or isolated segments. So, we used the average filter; example in Fig. 3.

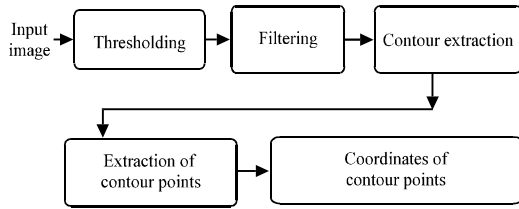


Fig. 2: Preprocessing steps

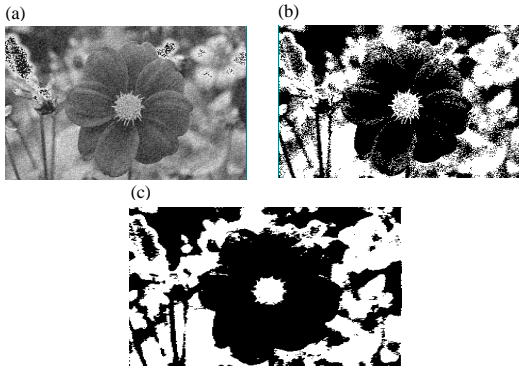


Fig. 3: a) Original image after the chaotic noise; b) Binary image without filter and c) binary image with filter

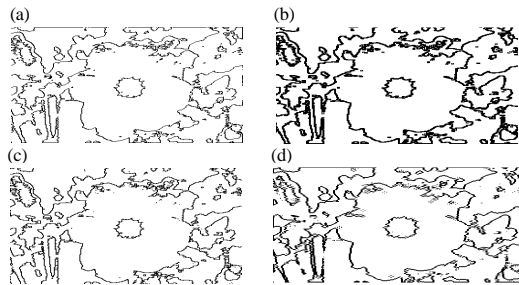


Fig. 4: a) Gradient contour; b) Sobel; c) Laplacian and d) White Rohrer

Contour extraction: In our method, we have extracted the containing contours in the image by applying several convolution filters (Gradient, Sobel, Laplace, White Rohrer) (Fig. 4).

Extraction of the coordinates of contour points: After extracting the contours of an image using different approaches, we perform a step of extracting the coordinates of these contours, so, we sweep the whole picture column by column starting with the first column to the last and each time we find a black pixel that means we have to find a contour pixel, so, we keep these spatial coordinates (x, y) and we continue in this way until the last column.

Table 1: The Fourier coefficients a (n) and b (n)

n	Values					
	0	1	2	3	4	5
a (n)	83	252	105	178	8	177
n	6	7	8	9	10	11
a (n)	207	182	196	35	119	194
b (n)	220	172	25	99	36	92
n	6	7	8	9	10	11
b (n)	127	110	84	95	48	114

Fourier descriptor application: The contour points extracted in the previous step are considered as discrete description by a set {Mi} points represented in the complex plane then the Fourier descriptor (Zhang and Lu, 2006) is applied to the coordinates (x, y) to calculate Fourier coefficients. An example of few Fourier coefficients of image in Fig. 3a is shown in Table 1. A norm alization step is applied to the Fourier coefficients in order to generate a random sequence.

An ideal random sequence: Following $u_i = x_i/m$, $i = 1, \dots, n$ is a random number uniformly distributed in the interval $[0, 1]$ [(Shannon, 1949). An ideal random sequence should find the three values:

$$\text{Average} = \bar{u} = \frac{1}{n} \sum_{i=1}^n u_i = \frac{1}{2} \quad (1)$$

$$\text{Variance } v = \frac{1}{n} \sum_{i=1}^n u_i^2 - (\bar{u})^2 = \frac{1}{12} \quad (2)$$

Autocorrelation factor:

$$E(u_i, u_{i+1}) = \frac{1}{n} \sum_{i=1}^{n-1} u_i u_{i+1} = \frac{1}{4} \quad (3)$$

To test whether, if the suite of Fourier coefficients forms an ideal random sequence, we have to calculate three characteristics mentioned above but before, we need to normalize these values to belong to the interval $[0, 1]$, so, we have devised each Fourier coefficient on max value as follow:

$$\text{Coefnorm}_i = \text{coef}_i / 255, i = 0, \dots, N$$

where, N is the number of Fourier coefficients. In the next paragraph, we give the values of the characteristics of the random sequence of Fourier coefficients calculated in the preceding part (image in Fig 3a).

After several tests carried out using different images, we can deduce that the random sequence composed of Fourier coefficients have an ideal random behavior.

Frequencies test: To prove that a random sequence of Fourier coefficient ensure really an randomization, we

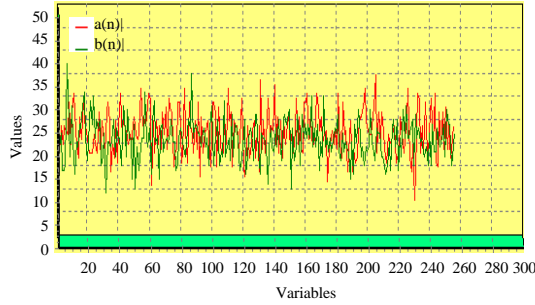


Fig. 5: Frequencies histogram of the random sequence

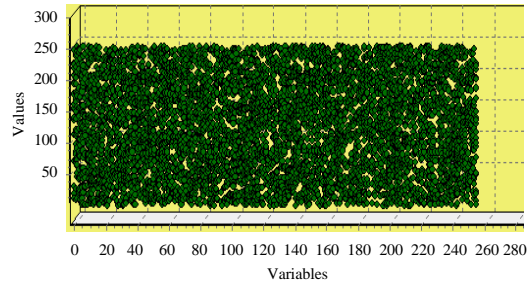


Fig. 6: Frequencies histogram of the ideal random sequence

Table 2: The characteristics of FC a (n) and b (n)

a (n)	Values
Average	0.495070
Variance	0.083048
Correlation	0.245466
b (n)	Values
Average	0.494893
Variance	0.082755
Correlation	0.246159

Table 3: Entropy comparison of generated sequence and character sequence

Nature of source	Entropy in bit/symbol
Sequence generated	7.9684
Source of that equiprobable character	8.0000

have applied a test of frequencies which represents the relative frequencies of occurrences of each value of random sequence and we have traced an histogram of these frequencies an examples of such histogram of the same image (Fig. 3a) is shown in the next Fig. 5 and 6.

It is noted in this graph that all the values of a (n) and b (n) coefficients from 0-255 are represented approximately with the same proportion. This results shows that our generator of random sequence of Fourier coefficients have passed this test.

Entropy of frequencies: After calculating of the frequencies of each value of a random sequence, we have also calculated the entropy which is an important characteristic. Entropy is a very important quantity of information theory. The information entropy $H(S)$ is a statistical measure of uncertainty in communication theory it is defined as follows (Shannon, 1949):

$$H(S) = -\sum_{k=1}^K P_k \log_2 P_k \text{ bits/pixel} \quad (4)$$

Where:

S = A discrete random variable

P_k = The Probability density function of the occurrence of the symbol k

After calculating the values of entropy for a basis of images used in our experimentation, we found it to be over 7.9684.

On the other hand, consider a source that has an alphabet of 256 characters, if all this characters are equiprobable, the entropy associated with each character is $\log_2(256) = \log_2(2^8) = 8$ bits which means that it takes 8 bits to transmit a character, thus, its entropy is equal to 8 bits.

For our random sequence of Fourier coefficients there is a ratio of 99.60% of a source that delivers equiprobable characters. So, we can say that a generated random sequence have satisfied a condition on the information entropy (Table 2 and 3).

Spectral analysis: The spectral test is described by Knuth (1981) as the most discriminating of all. Very simple, the method consists in studying the distribution of the values generated in a dimension k to verify the quality (21). We have applied 2D spectral test.

Dimension 2 (2D): Two consecutive values will be the coordinates of a point on the plane. We see if the points are uniformly distributed in a square. An example of the image in Fig. 3a is shown in the figure.

In general, the spectral test makes it possible to determine the difference between two lines. At most this gap is small the generator is of good quality. We find that our generator of random sequences have passed this spectral test.

Through the randomization tests done, we can see clearly that our random sequence composed of the Fourier coefficients a (n) and b (n) satisfies very well its tests and gives a good results, so, we can confirm that our sequence constitutes an ideal random sequence which will be used in the next step for image encryption.

Application of the proposed method for image encryption:

We will use the ideal random sequence calculated in the previous steps to encrypt our data (images). The principle of encryption is simple (Fig. 7).

The principle of this scheme is to perform a simple addition between the plaintext data M_i (original images) and the random sequence generated S_i the result is an

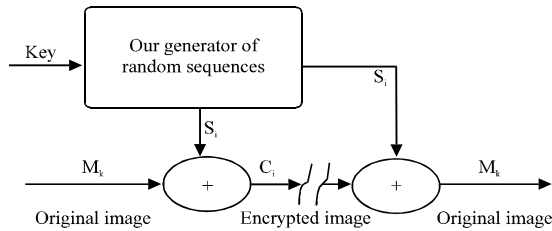


Fig. 7: Encryption scheme

encrypted images C_i . The information is then retrieved by subtracting the output (encrypted images) with the generated random sequence:

$$M_i = (C_i + S_i) \text{ mod } 256 \quad (5)$$

The key parameters: The key is divided into six parts:

- K_1 : Applying or not the average filter on the image (1 bit)

0	Apply the average filter on image
1	Don't apply the average filter on image

- K_2 : Image binarization threshold in our case we have taken a threshold between 50 and 180 (8 bits)

00110010	50
10110100	180

- K_3 : The contour extraction method (Gradient, Sobel, Laplace, White Rohrer) (2 bits)

00	Gradient method
01	Sobel method
10	Laplace method
11	White Rohrer method

- K_4 : The number of selected images to extract their Fourier coefficients (1024 images) (10 bits), we have constructed a set of 1024 images between transmitter and receivers
- K_5 : The parameter μ used for the normalization of Fourier coefficients $10 \cdot 10^7$ (24 bits)
- K_6 : The type of Fourier coefficients used to encryption/decryption: a (n) or b (n) (2 bits)

00	a (n) and b (n)
01	a (n)
10	b (n)
11	b (n) and a (n)

RESULTS AND DISCUSSION

Hardware configuration: To implement our method of encrypting and decrypting images, we have opted for a PC (SONY VAIO) 4 GB of RAM, Processor Intel (R) Core (TM) i3 CPU M330@2.13 GHz 2.13 GHz, Windows 7 64-bit for programming our software, we have used C++ language with Embarcadero RAD Studio 2010.

Experimental results and statistical analysis:

Experimental results of our random sequence generator and the new algorithm presented in this study has been done with several images. Figure 8 shows the experimental results with Flower BMP image. Figure 8a is plain-image. Figure 8b is its encrypted image with the encryption key (1130120100000001). As we can see, the encrypted image is rough-and-tumble and unknowable. Figure 8c is the decrypted image by use of the decryption algorithm with the same key.

Security analysis: A good encryption procedure should be robust against all kinds of cryptanalytic, statistical and brute-force attacks. In this study, we discuss the security analysis of the proposed image encryption scheme such as statistical analysis, sensitivity analysis with respect to the key and plaintext, key space analysis etc. This is to prove that the proposed cryptosystem is secure against the most common attacks (Pareek *et al.*, 2006).

Statistical analysis: It is well-known that many ciphers have been successfully analyzed with the help of statistical analysis and several statistical attacks have been devised on them. Therefore, an ideal cipher should be robust against any statistical attack. To prove the robustness of the proposed image encryption procedure, we have performed statistical analysis by calculating the histograms, the correlations of two adjacent pixels in the encrypted images and the correlation coefficient for several images and its corresponding encrypted images of an image database (Pareek *et al.*, 2006).

Histogram analysis: The histogram of an image represents the relative frequencies of occurrences of gray

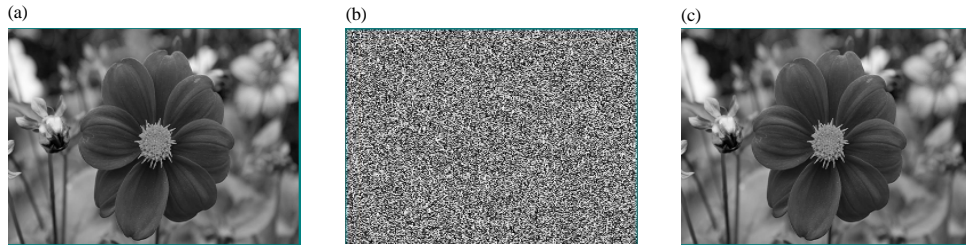


Fig. 8: Image encryption and decryption experimental result: a) Plain-image; b) Encrypted image and c) Decrypted image with correct key

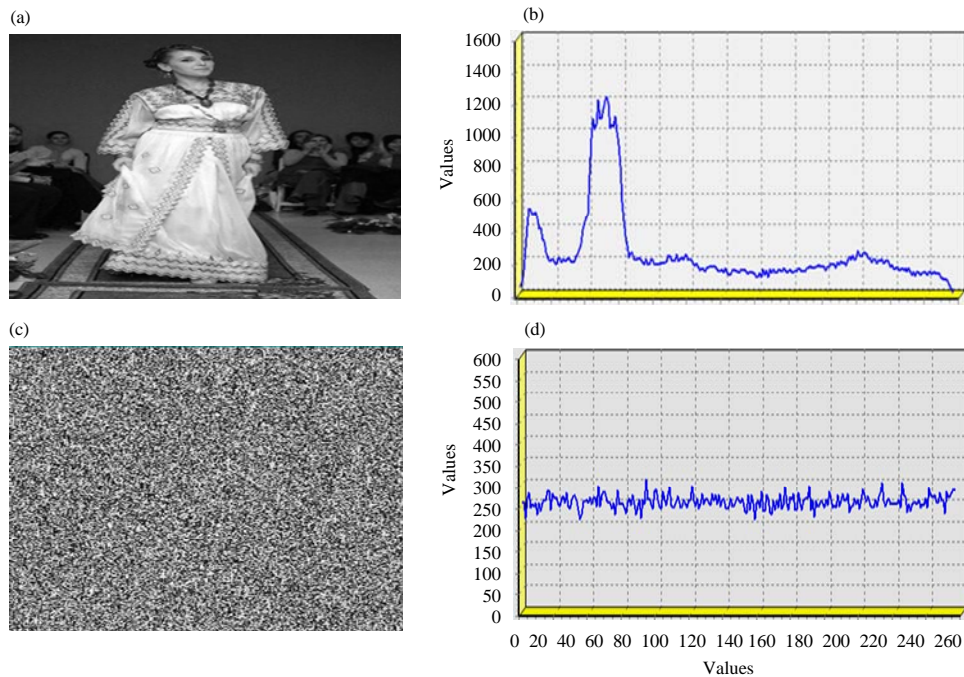


Fig. 9: a) Original image; b) Histogram of the original image; c) Encrypted image and d) Histogram of encrypted image

levels. In the case of a digital image, it is a discrete function $h(r_k) = n_k$ where, r_k is the k th gray level and n_k the number of pixels in the image with that level. We have traced the gray level histogram of both the original and encrypted image to see the distribution of their pixels which have no statistical similarity. The histograms of the original image as well as the corresponding encrypted image illustrate how the pixels are distributed. We have calculated and analyzed the histograms of several encrypted and original images that have widely different content. Two examples of such histogram analysis are shown in Fig. 9 and 10.

Correlation of adjacent pixels: In addition, to the analysis of the histogram, we also analyzed the correlation between two horizontally adjacent pixels and two vertically adjacent pixels as well as two diagonally adjacent pixels in the several imager and their encrypted

images, respectively Fig. 11 and 12. For calculating this correlation, we chose randomly a large number of pixels of the original and the encrypted images. If the calculated correlation of two adjacent pixels approaches to zero it means that the original image and the encrypted image are completely different and independent. In Fig. 13, we have shown the distribution of two adjacent pixels in the original and encrypted images shown in Fig. 11a-c, we have depicted the distributions of two horizontally adjacent pixels in the original and encrypted images. Moreover, we have also calculated the correlation between two diagonally as well as vertically adjacent pixels in the original and encrypted images. Equation 6 is used to calculate the correlation of the two adjacent pixels:

$$r_{xy} = \frac{\text{Cov}(x,y)}{\sqrt{D(x)D(y)}} \quad (6)$$

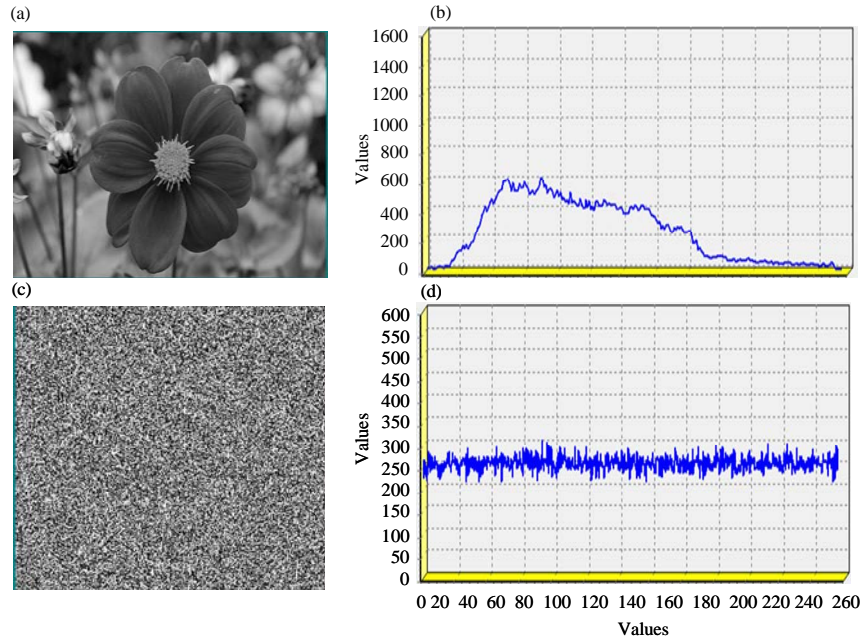


Fig. 10: a) Original image; b) Histogram of the original image; c) Encrypted image and d) Histogram of encrypted image

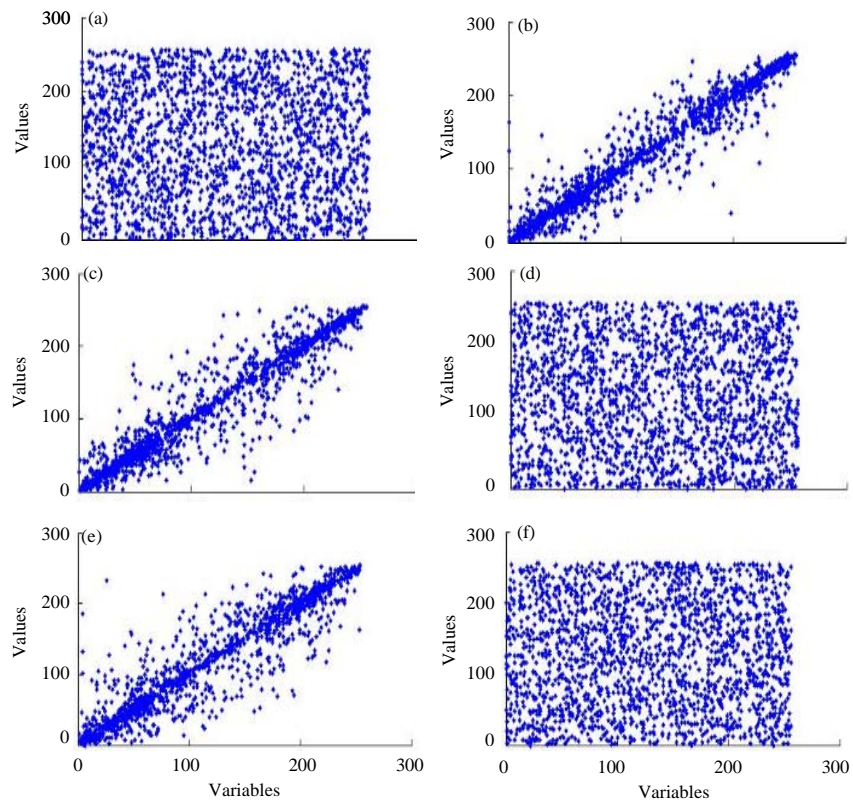


Fig. 11: The distribution of two horizontally, vertically, diagonally adjacent pixels in the plain and encrypted images shown in: a) Horizontal d' image originale; b) Horizontal d' image cryptee; c) Vertical d' image originale; d) Vertical d' image cryptee; e) Diagonal d' image originale and f) Diagonal d' image cryptee

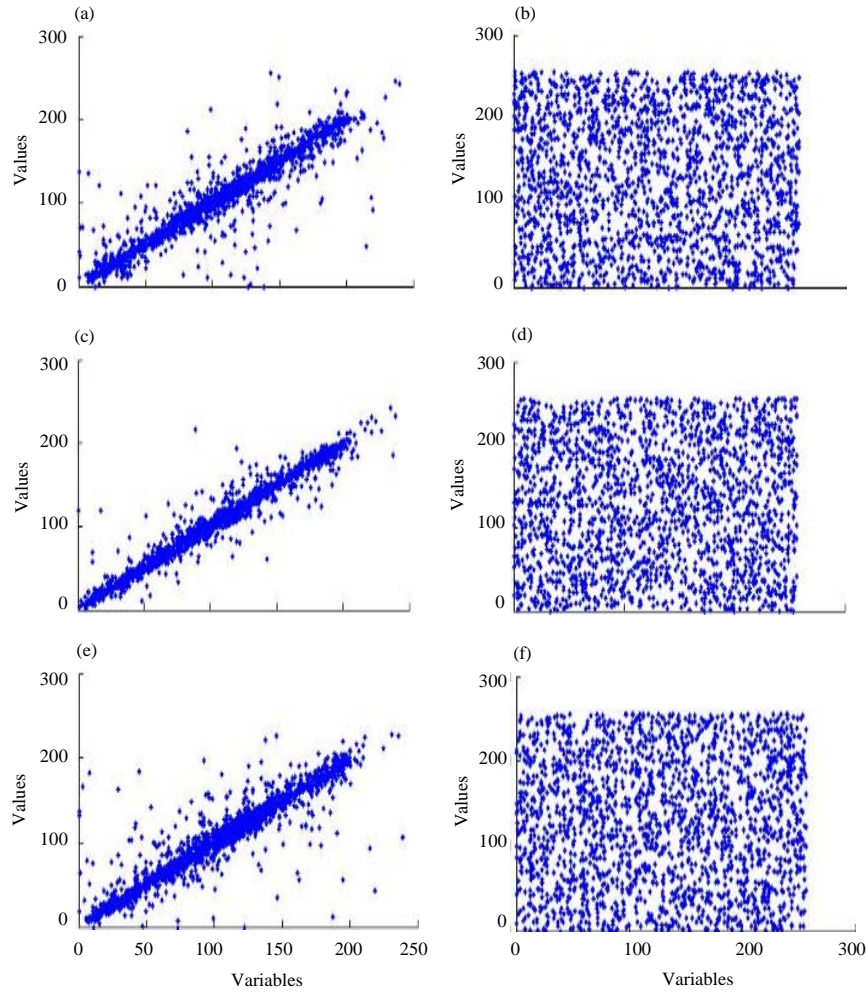


Fig. 12: Distribution of two horizontally, vertically, diagonally adjacent pixels in the plain and encrypted images shown in Fig. 10a-d: a) Horizontal d’image originale; b) Horizontal d’image cryptee; c) Vertical d’image originale; d) Vertical d’image cryptee; e) Diagonal d’image originale and f) Diagonal d’image cryptee

Table 4: Correlation coefficients of adjacent pixels of the original image and encrypted image

Adjacent pixels direction	Original image	Encrypted image
Horizontal	0.9686	0.000320
Vertical	0.9572	0.000324
Diagonal	0.9475	0.003610

Table 5: Correlation coefficients of adjacent pixels of the original image (e) and encrypted image (g)

Adjacent pixels direction	Original image (e)	Encrypted image (g)
Horizontal	0.9370	-0.00112
Vertical	0.9812	0.00008
Diagonal	0.9353	0.00139

$$\text{Cov}(x, y) = \frac{1}{N} \sum_{i=1}^N [(x_i - E(x))(y_i - E(y))] \quad (7)$$

$$D(x) = \frac{1}{N} \sum_{i=1}^N [x_i - E(x)]^2 \quad (8)$$

$$D(y) = \frac{1}{N} \sum_{i=1}^N [y_i - E(y)]^2 \quad (9)$$

$$E(x) = \frac{1}{N} \sum_{i=1}^N x_i \quad (10)$$

$$E(y) = \frac{1}{N} \sum_{i=1}^N y_i \quad (11)$$

Here, x and y are the gray level values of two adjacent pixels and N is the number of adjacent pixels selected from the image. Table 4 gives the correlation coefficients for the original and encrypted images shown in Fig. 9a and c, respectively, Table 5 gives the correlation coefficients for the original and encrypted images shown in Fig. 10a and g, respectively.


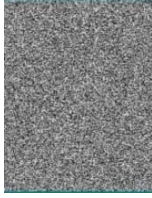

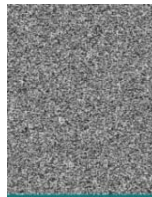

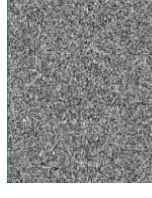
Original image	Entropy original image	Encrypted image	Entropy encrypted image
(a) 	7.5692	(b) 	7.9972
(c) 	7.5645	(d) 	7.9975
(e) 	7.4874	(f) 	7.9970

Fig. 13: The entropy of the original images and their encrypted

Calculation of entropy: Information entropy is defined to express the degree of uncertainties in the system (Shannon, 1949), so, the entropy equation $H(S)$ is defined by Eq. 4 and P_k is defined as follow:

$$P_k = \frac{\text{No of pixels equals to } k}{\text{Total number of pixels of the image}}$$

In this part, we have to calculate the entropy information for the plain-image and its corresponding cipher image. We show in the following table the calculated values of the entropy of the original images mentioned above and encrypted images.

Analysis of the sensitivity to the secret key: An ideal image encryption procedure should be sensitive with respect to the secret key, i.e., the change of a single bit in

the secret key should produce a completely different encrypted image. We have performed two types of tests to observe the sensitivity of our secret key encryption algorithm.

Test 01: The encrypted image generated by the cryptographic system should be very sensitive to the secret key, i.e., if two slightly different keys are used to encrypt the same image, the two images generated (encrypted) should be completely independent of each other or in other words they should have a negligible correlation.

Test 02: The encrypted image cannot be deciphered correctly despite the presence of a slight difference between the key of encryption and decryption. For testing the key sensitivity of the proposed image encryption procedure, we have performed the following steps:

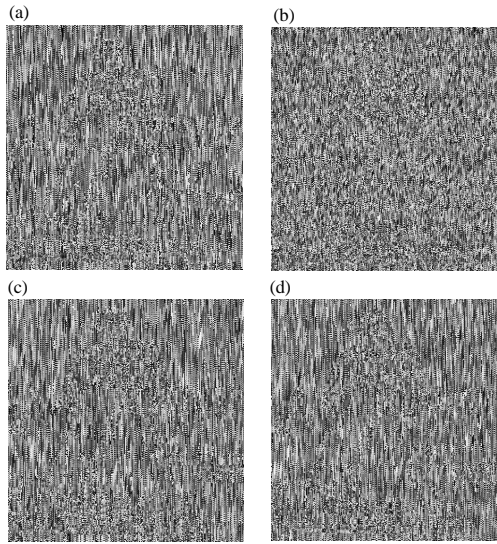


Fig. 14: a-d) Test 1 sensitivity of the secret key, respectively shows the encrypted images of the original image with the words ‘1130120100000001’, ‘0130120100000001’, ‘0130121100000001’, ‘1130121100000001’

- An original image (Fig. 9a) is encrypted by the key ‘1130120100000001’ (in decimal) and the resulting image is referenced encrypted image Fig. 14a
- The same image is encrypted by making the slight modification in the secret key, i.e., ‘0130120100000000’ and the resulting image is encrypted Image referenced Fig. 14b
- Again the same image is encrypted by making the slight modification in the secret key, i.e., ‘0130121100000001’ and the resulting image is referenced encrypted image Fig. 14c
- Again the same image is encrypted by making the slight modification in the secret key, i.e., ‘1130121100000001’ and the resulting image is encrypted image referenced Fig. 14d
- Finally, the four encrypted images are compared

In Fig. 14, we have shown the original image and the four encrypted images produced in the in the aforesaid steps. It is not easy to compare the encrypted images by simply observation of these images. So, for comparison, we have calculated the correlation between the corresponding pixels of the four encrypted images. For this calculation we have used the same formula given by Eq. 7 except that in this case x and y are pixels values of the two encrypted images to be compared. In Table 6, we have given the results of the correlation coefficients between corresponding pixels of four images Fig. 14a-d.

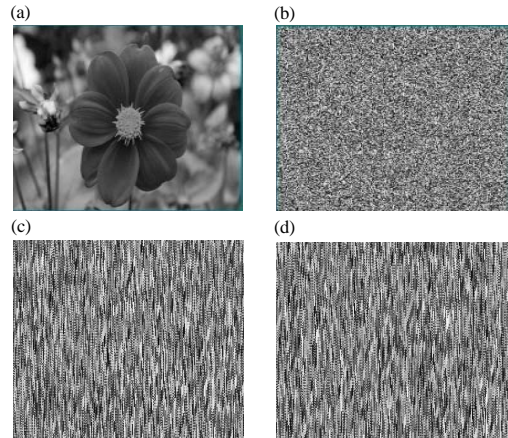


Fig. 15: Test 2, sensitivity of the secret key; (a) and (b), respectively shows the original image and its encrypted image with key ‘1130120100000001’. Images (c) and (d), respectively shows the images after the decryption of the encrypted image (e) Using the key ‘0130120100000001’, ‘0130121100000001’, ‘1130121100000001’

Table 6: Correlation coefficients between the corresponding pixels of the four encrypted images obtained using slightly different keys

Encrypted image		
Image 1	Image 2	Correlation coefficients
B	C	0.00860
C	D	-0.00560
D	B	0.01610
B	E	0.01490
E	D	-0.00310
C	E	-0.00440

It is clear from the table that no correlation exists among four encrypted images even though these have been produced by using slightly different secret keys.

In Fig. 15, moreover, we have shown the results of some attempts to decrypt an encrypted image with slightly different secret keys than the one used for the encryption of the original image. Particularly the image (a) and (b), respectively, the original image and the encrypted image generated by using the secret key ‘1130120100000001’ are shown whereas the image (c) and (d), respectively are the images after decryption of the encrypted image (shown b) applying the secret keys ‘0130120100000001’, ‘0130121100000001’. It is clear that the decryption with slightly different keys has completely failed and hence, the proposed image encryption procedure is highly key sensitive.

Differential analysis: We have also measured the Number of Pixels Change Rate (NPCR) to see the influence of changing a single pixel in the original image on the encrypted image by the proposed algorithm. The NPCR

measure the percentage of different pixel numbers between the two images. We take two encrypted images, C1 and C2 whose corresponding original images have only one-pixel difference. We define a two-dimensional array D having the same size as the image C1/C2. The D (i, j) is determined from C1 (i, j) and C2 (i, j). If C1 (i, j) = 2 (i, j) then D (i, j) = 1 otherwise D (i, j) = 0. The NPCR is defined by the following Eq. 12 (Abugharsa *et al.*, 2011):

$$NPCR = \frac{\sum_{ij} D(i, j)}{wh} \times 100\% \quad (12)$$

where, w and h are the width and height of encrypted image. We obtained NPCR for a large number of images by using our encryption scheme and found it to be over 99% showing thereby that the encryption scheme is very sensitive with respect to small changes in the plaintext. UACI is the difference in the average intensity between two encrypted images. It is defined as follow:

$$UACI = \frac{1}{h \times w} \sum_{i=1}^h \sum_{j=1}^w \frac{|C1_{i,j} - C2_{i,j}|}{2^8 - 1} \times 100 \quad (13)$$

We obtained UACI for an important number of images by using our encryption algorithm and found it to be over 33.4635%.

Key space analysis: For a secure image cipher, the key space should be large enough to make the brute force attack infeasible. From the key parameters, we can see clearly that the key space can be up to (2^{47}). Thus, the pattern with such a large key space can effectively resist all attacks brute force.

Analysis of the execution time: Apart from security, running speed of the algorithm is also an important aspect for a good encryption algorithm. The execution time of our encryption method using Chaos theory and Fourier descriptors is estimated by a few minutes.

CONCLUSION

In this study, a new method for image encryption have been proposed which utilizes Fourier descriptor as an ideal random numbers function with external key of 47-bit as we have applied a chaotic noise to make our method more complex. We have carried out statistical analysis, key sensitivity analysis and key space

analysis to demonstrate the security of the new image encryption/decryption procedure. Finally, we conclude with the remark that the proposed method is expected to be useful for real time image encryption and transmission applications.

REFERENCES

- Abugharsa, A.B., A.S.H. Basari and H. Almangush, 2011. A new image encryption approach using block-based on shifted algorithm. *Intl. J. Comput. Sci. Netw. Secur.*, 11: 123-130.
- Al-Qaheri, H., A. Mustafi and S. Banerjee, 2010. Digital watermarking using ant colony optimization in fractional Fourier domain. *J. Inf. Hiding Multimed. Sign. Proc.*, 1: 179-189.
- Ashutosh, D.S., 2013. Image encryption using discrete Fourier transform and fractional fourier transform. *Intl. J. Eng. Adv. Technol.*, 2: 886-890.
- Bu, S. and B.H. Wang, 2004. Improving the security of chaotic encryption by using a simple modulating method. *Chaos Solitons Fractals*, 19: 919-924.
- Chee, C.Y., D. Xu and S.R. Bishop, 2004. A zero-crossing approach to uncover the mask by chaotic encryption with periodic modulation. *Chaos Solitons Fractals*, 21: 1129-1134.
- Gao, H., Y. Zhang, S. Liang and D. Li, 2006. A new chaotic algorithm for image encryption. *Chaos Solitons Fractals*, 29: 393-399.
- Knuth, D.E., 1981. *The Art of Computer Programming: Semi-Numerical Algorithms*. 2nd Edn., Pearson Education, London, England, UK., ISBN:9780201038224, Pages: 688.
- Kushwaha, J. and B.N. Roy, 2010. Secure image data by double encryption. *Intl. J. Comput. Appl.*, 5: 28-32.
- Li, S. and X. Zheng, 2002. Cryptanalysis of a chaotic image encryption method. *Proceedings of the IEEE International Symposium on Circuits and Systems*, May 26 29, 2002, Phoenix-Scottsdale, AZ., USA., pp: 708-711.
- Pareek, N.K., V. Patidar and K.K. Sud, 2006. Image encryption using chaotic logistic map. *Image Vision Comput.*, 24: 926-934.
- Refregier, P. and B. Javidi, 1995. Optical image encryption based on input plane and Fourier plane random encoding. *Opt. Lett.*, 20: 767-769.
- Shannon, C.E., 1949. *Communication theory of secrecy systems*. *Bell Syst. Tech. J.*, 28: 656-715.

- Unnikrishnan, G. and K. Singh, 2000. Double random fractional Fourier domain encoding for optical security. *Opt. Eng.*, 39: 2853-2860.
- Unnikrishnan, G. and K. Singh, 2001. Optical encryption using quadratic phase systems. *Opt. Commun.*, 193: 51-67.
- Xu, L., Z. Li, J. Li and W. Hua, 2016. A novel bit-level image encryption algorithm based on chaotic maps. *Opt. Lasers Eng.*, 78: 17-25.
- Younes, M.A.B. and A. Jantan, 2008. An image encryption approach using a combination of permutation technique followed by encryption. *Intl. J. Comput. Sci. Netw. Secur.*, 8: 191-197.
- Zhang, D. and G. Lu, 2006. A comparative study on shape retrieval using Fourier descriptors with different shape signatures. Master Thesis, Gippsland School of Computing and Information Technology, Monash University Clayton Campus, Melbourne, Australia.
- Zhang, Y. and D. Xiao, 2014. An image encryption scheme based on rotation matrix bit-level permutation and block diffusion. *Commun. Nonlinear Sci. Numer. Simul.*, 19: 74-82.
- Zhen, P., G. Zhao, L. Min and X. Jin, 2016. Chaos-based image encryption scheme combining DNA coding and entropy. *Multimedia Tools Appl.*, 75: 6303-6319.