International Journal of Current Engineering and Technology
©2017 INPRESSCO®, All Rights Reserved

E-ISSN 2277 – 4106, P-ISSN 2347 – 5161
Available at http://inpressco.com/category/ijcet

Research Article

High Performance Encryption Algorithm

Mariam Raheem*and Ivan A. Hashim

University of Technology/ Department of Electrical Engineering, Baghdad-Iraq

Received 01 Oct 2017, Accepted 02 Dec 2017, Available online 11 Dec 2017, **Vol.7, No.6 (Nov/Dec 2017)**

Abstract

*Cryptographic algorithms are utilized in various environments in which security is a key requirement. The widespread use of large data storage networks and information technology has led to an increase in demand of high speed, low power and low area consumption cryptographic systems. The established cryptographic systems which have existed for a long period of time are having a difficult time to come up with ever increasing performance requirements. In this work, a cipher generator for encryption algorithm is proposed based on different methods and techniques (Central spiral technique, outer spiral technique, transpose array method and exclusive –OR operation) to increase the strength of proposed algorithm system by making the cipher of encryption system more robust and more reliable. This system is able to encrypting any input data such as text message, image and audio. The simulation results show that the proposed encryption algorithm has best values in three tests(ARE, maximum deviation analysis and peak signal to noise ratio) comparing with the traditional schemes(Lorenz, Chua, Rössler and Nien) flow sequences when it has been implemented on 256*256 images, while getting very close results for other tests, and the proposed algorithm system has excellent results compared with the performance of the traditional encryption systems in which has passed most of the FIPS PUB 140-1 statistical tests successfully.*

Keywords: *Encryption, Decryption, Central spiral technique, Cryptanalysis.*

Introduction

Encryption can be provided either using symmetric (secret) key algorithms, such as DES, or asymmetric (public) key algorithms, such as RSA. Because asymmetric-key algorithms are computationally much more intensive than symmetric-key algorithms, they are not typically used for bulk encryption. Instead, they are mostly used for digital signature and key exchange. Symmetric- and asymmetric-key algorithms usually operate on blocks of fixed size. Often it's required to encrypt a long plaintext block using a short-block encryption algorithm. This is not such a big problem when symmetric-key cryptosystems are used, since . They operate at much higher speed. However, it is highly impractical to use a public key cryptosystem, such as RSA or Elliptic Curves, to encrypt a very large block of data. [M. Matyas and M. Peyravian et al ,1998], In this paper we propose the following alternative: we will covering between the secret bits of the plaintext and symmetric key after applying many methods and techniques on them to provide a strong guardianship for the content of the secret part of the plaintext.

Cryptography: The encryption and decryption techniques are a set of algorithms that convert the plaintext to the ciphertext in the sender side (encryption). The decryption process is done in the receiver side by using the agreement key to acquire the plain text again. When discussing strength in terms of encryption, it generally signifies the level of difficulty by which it is possible to decipher the key or algorithm, which is not disclosed. Thus, decoding a key must involve processing a large number of probable values in order to attain a value which can be employed so as to decrypt a particular message. In other words, non-repudiation services, authenticity, confidentiality, and integrity can be provided by means of cryptography. [J. Katz and L. Yehuda,2007, W. Stallings,2009].In cryptography, encryption is the process of transforming information (referred to as plaintext) using an algorithm (called cipher) to make unreadable to anyone except those possessing special knowledge, usually referred to as a key. The result of the process is encrypted information (in cryptography, referred to as ciphertext). In many contexts, the word encryption also implicitly refers to the reverse process, decryption (e.g. software for encryption can typically also perform decryption), to make the encrypted information readable again (i.e. to make it unencrypted)[R. Hosseinkhani1 and S. Hamid,2012].

The classification of Cryptography

1) ***Symmetric Key:*** Symmetric cryptography, commonly called secret or conventional encryption,

*Corresponding author's ORCID ID: 0000-0003-3938-530X refers to the type of encryption where the keys of encryption and decryption have the same equivalent values. Another definition of symmetric encryption describes it as well as a shared key cryptography or shared secret cryptography due to the fact that it applies to only one shared key which is employed in encrypting and decrypting the message. Application of symmetric has numerous benefits and disadvantages actually, the advantages of employing symmetric encryption include: providing authentication that the key remain secret, encryption of data is performed instantly, and key symmetry permits encryption and decryption while using the same key [W. Stallings,2005].

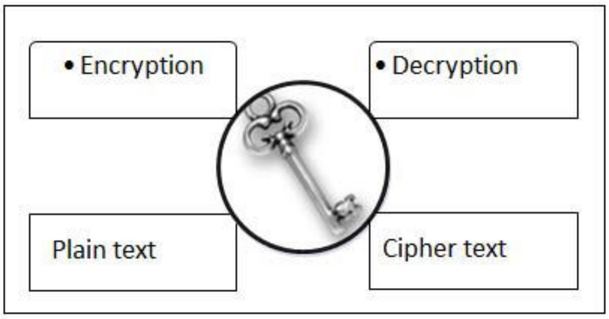


Figure 1: Symmetric key

2) ***Asymmetric Key***: The term Asymmetric encryption, which is commonly referred to as public key encryption, is the type of asymmetric encryption which employs two varied keys for the purpose of encryption and decryption. One of the two keys in cryptography is a public key which can be made available for anyone. On the other hand, the second key, known as a secret or a private key is a mathematically-related one.

This is cryptography key is the one which has to be kept confidential from others [P. hristof and P. Jan,2009].

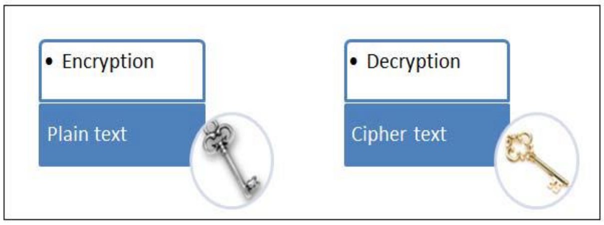


Figure 2: Asymmetric key.

C. Types of symmetric key algorithms

1) Stream cipher: The stream cipher idea is simply dividing the text into relatively small blocks, for example, 1bit and allowing every block encoding to be based on numerous preceding blocks [P. hristof and P. Jan,2009].

2) Block cipher*:* The concept of a block cipher is to divide the text into fairly bulky, for instance 128 bits, blocks, then encode every block individually. Normally, each block encoding is based on at the maximum a block of the former ones. The key remains unchanged when applied with every block [L.R. Jan,2001].

Related Work

In the literature, various approaches have been proposed by researchers to provide the best level in data security. In general, researchers have many methods and techniques for providing their proposed algorithm system by powerful protection For example [B. Katz,2016], suggested using physical (PHY) layer techniques for the generation of encryption keys on the fly without the use of vulnerable key sharing. While these PHY layer techniques had been demonstrated to work in controlled settings with offline processing, little work had been done to integrate them into existing wireless standards. In this work, an integration of PHY layer channel state-based encryption key generation was presented into a real-time 802.11 compliant software-defined radio.

[J. Majumder and P. Bankura,2013]proposed two algorithms, one for image encryption process and other for decryption. Spiral encoding and spiral decoding technique were used for creating confusion of neighboring pixel correlation. Symmetric key and shared secret number were used which enhanced the overall encryption technique. Several experiments showed that proposed algorithms were good enough to prevent differential attack and statistical attack

Proposed encryption algorithm

Encryption is the process of transforming plaintext to the cipher text so it is unintelligible to anyone but the intended recipient. Decryption is the process of transforming encrypted information (ciphertext) to the original information (plaintext) so that it is intelligible again as shown in Fig.3

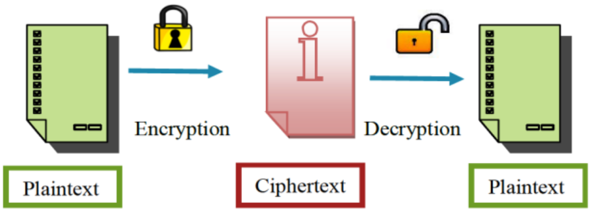


Figure 3: Encryption and Decryption process.

Encryption

In the proposed system used many technique and method as (Central spiral technique and transpose array method) on the stream bits of plaintext after making reshaping and subgrouping to the plaintext Whether (text message or image) and applying (Outer spiral technique) on the key to provide the proposed algorithm system with randomize and strength, Fig. 4 shows the proposed encryption algorithm block diagram.

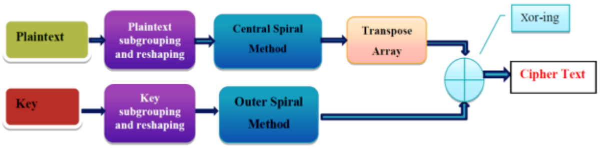


Figure 4: Proposed algorithm system

A. Encryption Plaintext

In the proposed algorithm system, the plaintext should be converted into a stream of bits whether it contains text, images or audio as the first step in the encryption process.

B. Plaintext Sub-Grouping and Reshaping

The second stage in proposed encryption process is dividing the stream bits of plaintext into sub-groups, each sub-group consist of 25 bits, The second step in this stage is reshaping the sub-group from one dimension vector to two dimension array, Using the reshaping in the encryption process is very important to prepares it for the next stage (central spiral technique), because it depend on the arrangement position of input data bits in its work.

C. Central Spiral Array

In the proposed encryption algorithm the central spiral technique are adopted. By applying a central spiral method on the two dimension matrix, which produced by previews step the position of bits will be changed in order to make scrambling on input data input.

D. Transpose Array

In transposition systems, plaintext values are rearranged without otherwise changing them. All the plaintext bits that were present before transposition are still present after transposition. Only the order of the bits is changed.

So as to increase the randomize of bits array in the proposed encryption algorithm system , will used one of the important type of the transposition system called the transpose technique (T) after applying the central spiral method on the previous stage.

E. Encryption Key

A symmetric key is used in the proposed encryption algorithm system that created a randomly (variable value ad size) for each input data. The key has different size may be shorter or longer than input data. If the key (K) shorter than data (D) therefore resizing the key should be done in order to produce anew key which is the same as the first key but doubling it until it becomes as the same size of the input data. However, if the key is longer than input data should trim part of key size to become equal with the input data size. The key resizing process is explained in the following example.

The key in the encryption process may be on the form of a text, image, or audio, if in any case it should be converted to the stream of bits after which apply the stages of the algorithm with the plaintext.

A similar procedure that is done on plaintext in second stage well be done for key in this stage. Where the stream bits of key is splits to 25 bits sub-groups. Therefore, reshipping each sub-group to 5×5 array as shown below to prepare the sub-groups to the next stage, which is applying the outer spiral method for the produced array.

F. Outer Spiral Array

In order to increase the randomize of key the outer spiral techniques are employing that changes the bits positions of the key sub-group array

G. Encryption Cipher Text

The last step in encryption process produces a ciphertext , when applying the exclusive OR between the Transpose of central spiral array (Plaintext) and the outer spiral array (key) the ciphertext (C) will be composed Exclusive-OR operation has many advantages when used for cryptography; very fast computable, especially in hardware, not making a difference between the right and left site (being commutative), it doesn't matter how many and in which order you XOR values (being associative), easy to understand and analyses.

1. Encryption for text message

Plaintext usually means un-encrypted information pending input into cryptographic algorithms and as a data input to the proposed algorithm, this data (e.g. file contents) may represent only characters of readable material, However, nor its graphical representation neither objects (images, etc.). It may also include a limited number of characters that control simple arrangement of text, such as line breaks or tabulation characters. Plaintext is different from formatted text, where style information is included, and from binary files in which some portions must be interpreted as binary objects (encoded integers, real numbers, images, etc.).In the proposed algorithm system, the plaintext and key should be converted into a stream of bits by sub-grouping and reshaping as shown below, then applying the central spiral technique and transpose array method to plaintext to increasing the randomize and outer spiral technique to key then used Xor-ing between them.

b_0	b_1	b_2	…………	b_{25}

2. Encryption for image

The image should be passing through the same steps that text is passed to be encrypted by the proposed encryption system except the first stage that prepares the input data. Image is composed of a set of pixels and generally the RGB image consists of three matrices; for red, green and blue color. In the proposed algorithm, image will be treated in order to convert the image to stream of bits. Firstly, each pixel in image will be replaced with the equivalent binary values as shown in Fig.5. Therefore, the three binary values of the pixel will be constructed to be one vector. Finally, combine all pixels vectors to produce the input bit stream.

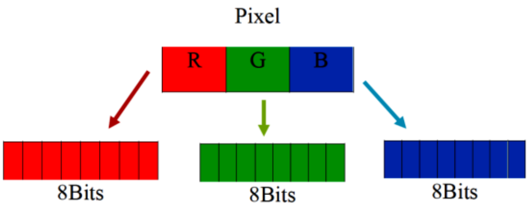


Figure 5: Pixel component.

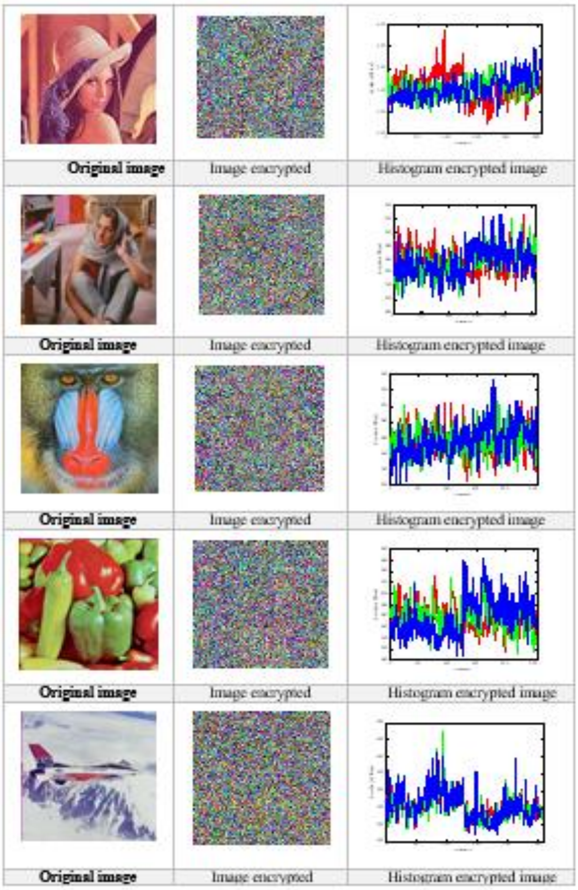


Figure 6: Simulation results of the proposed system for different images

Fig.6 shows the original images of size 256*256 with the resultant encrypted images when encrypted by the proposed algorithm system. As it is shown in this figure, the histogram is obtained for the image after it is encrypted.

It is very important to note that the encrypted image has changed completely from the original image and is not recognizable or detected. In addition, the histogram of the encoded image has changed from the original image histogram and this is the result of a strong type of algorithm that has a strong cryptographic. Also this is what distinguishes strength of the cryptography from Scrambling which, does not change the histogram of the new image from the old image. Figure 7 shows the flowcharts of proposed real time algorithm system steps.

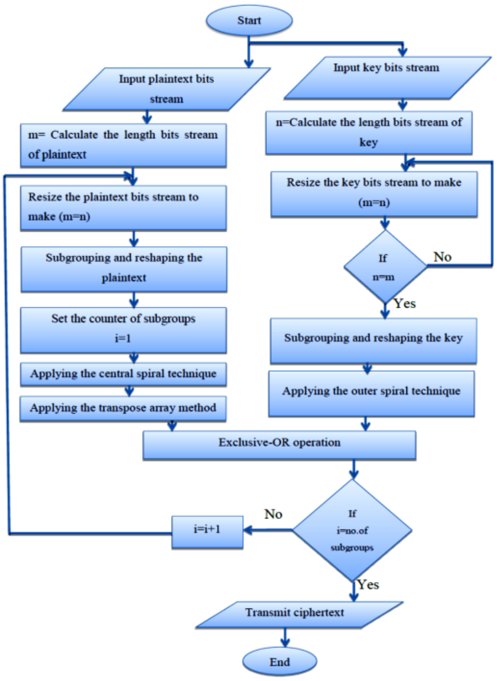

Start
Input plaintext bits stream
Input key bits stream
m= Calculate the length bits stream of plaintext
n=Calculate the length bits stream of key
Resize the plaintext bits stream to make (m=n)
Resize the key bits stream to make (m=n)
If n=m
No
Yes
Subgrouping and reshaping the plaintext
Set the counter of subgroups i=1
Subgrouping and reshaping the key
Applying the central spiral technique
Applying the transpose array method
Applying the outer spiral technique
Exclusive-OR operation
If i=no.of subgroups
No
i=i+1
Yes
Transmit ciphertext
End

Figure 7: Flowchart of proposed Encryption Algorithm

Decryption

The decryption process of the proposed algorithm system has approximately the same stages of the encryption algorithm process with the same initial values and parameters.

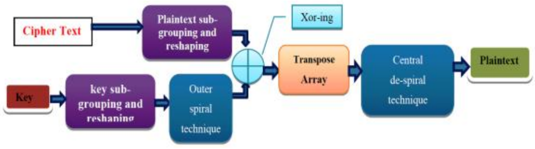

Cipher Text
Plaintext sub-grouping and reshaping
Xor-ing
Key
key sub-grouping and reshaping
Outer spiral technique
Transpose Array
Central de-spiral technique
Plaintext

Figure 8: Proposed Real Time decryption Algorithm

At receiver the recipient should receive the same quality of original data without delay. So the proposed algorithm system should build the decryption process according to high quality and precision with the stages shown in Fig (8).

A. Received Cipher Text

The received ciphertext should be converted to stream if bits at the first stage in order to be capable to read by the proposed system. Where, the same steps that used to translate the plaintext to stream of bits are used to evaluate the stream bits of the received ciphertext. Therefore, this stream bits will be passed through the sub-grouping and reshaping stage that divide the cipher bits into 5×5 arrays.

B. Decryption Key and Decryption Recovering

The key used in the decryption stages should be the same one that used in encryption stage (symmetric key). After the key is converted to stream of bits, the stream of bits will be sub-grouping and reshaping to produce two dimensions array that used to remove the effect of the key from cipher bits.

In the decryption process, the effect of the key should be removed using the exclusive-OR operation between the ciphertext and the key as the first stage to recovery the plaintext.

C. Decryption Transpose Array

The next stage of the proposed encryption algorithm in the decryption process is transposing array in order to retrieve the plain text properly and sequentially. Therefore, by applying the transpose array method on the previous stage.

D. Central De-spiral Method

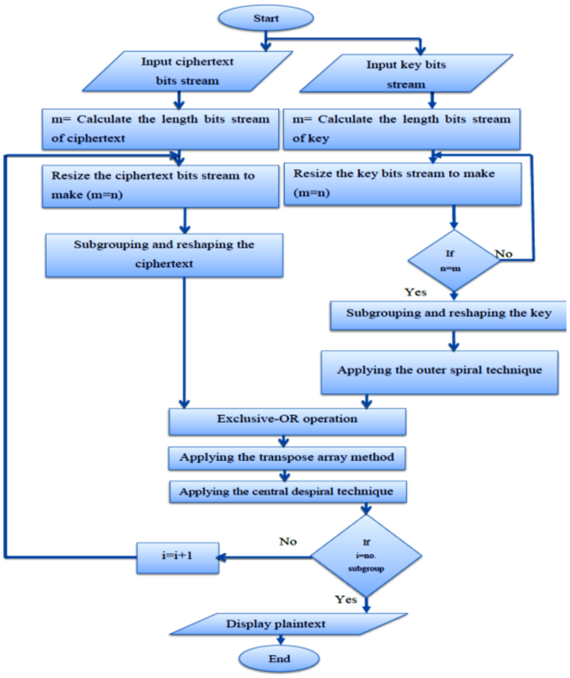

Start
Input ciphertext bits stream
Input key bits stream
m= Calculate the length bits stream of ciphertext
m= Calculate the length bits stream of key
Resize the ciphertext bits stream to make (m=n)
Resize the key bits stream to make (m=n)
Subgrouping and reshaping the ciphertext
If n=m
No
Yes
Subgrouping and reshaping the key
Applying the outer spiral technique
Exclusive-OR operation
Applying the transpose array method
Applying the central despiral technique
If i=no. subgroup
No
i=i+1
Yes
Display plaintext
End

Figure 9: Flowchart of proposed algorithm system in decryption process

The last stage in the decryption process at receiver is applying the central de-spiral technique on the transposed array, then converting the array to stream of bits [b] and take every 8 bits from the stream to return as character if the input data is text, pixel if the input data is image, sample if the input data is audio, After the conversion of all the bits to the original input data, the recipients read and understand the encrypted data clearly with high quality and super-fast**.** Figure (9) shows the flowcharts of proposed decryption algorithm system steps.

Comparative Analysis

A scientific examination for the correlation of regular and proposed calculation is displayed in this area. In this work, the size of key is 25 bits, so the aggregate key space will comprise of 2^{25}combinations that equivalents to**(33554432)**.A system that able toperform1 combination for every unit time will acquire **(33554432)** time units to discover the key via power attack. Additionally, the size of the data input (plaintext) is of 25 bit, the total input data space will be same as key space which is equal to**(33554432)** in addition to the same quantity of time units that needs to discover the data by brute power assault. Furthermore, there are 8 attempts to identify and detect one of four type of spiral four attempts for the central spiral in terms of if starting from the center and move right or left movement or move the bottom or the top and four attempts to the outer spiral if it appeared from the top, but on the left or right and if it appeared from the bottom but from the right or the left. So there are2^8combinationsof additional attempts that increase complexity, where will capture **256**time units to find out the type of spiral. Moreover, there are 2 attempts to find a transpose array. Therefore, the total space will be consisting of 2^2combinations that equal **4.** The Xor-ing will be consisting of 2^1combinations that equal **2** operations. Table (1) shows the result combination of brute force attack

As illustrated in this Table the maximum attempt to discover the cipher by force attack per second are (33,554,432) which is very large number in comparison with the other algorithm system.

Table 1 : Comparative analysis of the proposed real time encryption algorithm

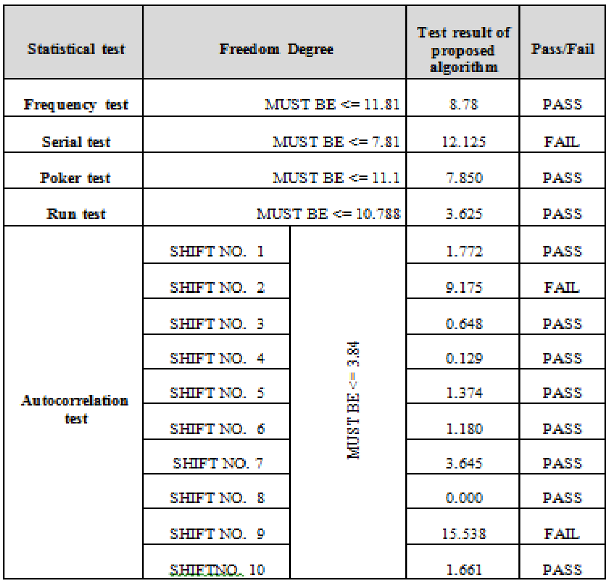
S.No	Reference type	Bits size(n)	Types Techniques(n)	No. of Attempt(2^n)	No. of Attempt/Sec (Complexity)
1	Input Data	25		2^{25}	33554432
2	Input Key	25		2^{25}	33554432
3	Central Spiral Technique		8	2^8	256
4	Outer Spiral Technique		8	2^8	256
5	Transpose Method		2	2^2	4
6	Exclusive –OR operation		1	2^1	2
sum					33,554,432/s

Statistical tests for the proposed system

Many testing techniques are used to calculate system performance and encryption quality. The testing technique results are testing the randomness behavior by using the FIPS PUB 140-1 statistical tests.

Table (2) shows the result of implementing of the FIPS PUB 140-1 statistical tests to check the system randomness. The results obtained in the Table strongly prove that the proposed algorithm system fulfills the randomness requirements needed for reliable encryption algorithm.

Table 2 The FIPS PUB 140-1 statistical tests of the proposed algorithm system



Statistical test	Freedom Degree		Test result of proposed algorithm	Pass/Fail
Frequency test	MUST BE <= 11.81		8.78	PASS
Serial test	MUST BE <= 7.81		12.125	FAIL
Poker test	MUST BE <= 11.1		7.850	PASS
Run test	MUST BE <= 10.788		3.625	PASS
Autocorrelation test	SHIFT NO. 1	MUST BE <= 3.84	1.772	PASS
	SHIFT NO. 2		9.175	FAIL
	SHIFT NO. 3		0.648	PASS
	SHIFT NO. 4		0.129	PASS
	SHIFT NO. 5		1.374	PASS
	SHIFT NO. 6		1.180	PASS
	SHIFT NO. 7		3.645	PASS
	SHIFT NO. 8		0.000	PASS
	SHIFT NO. 9		15.538	FAIL
	SHIFTNO. 10		1.661	PASS

The proposed system has many results in the last test, it is able to achieve success in most results, while failed in some of them because it depends on the checking for correlations between the sequence of bit stream and (non-cyclic) shifted versions of it and this is not always achieved in the sequence bit stream of the proposed system.

Encryption's Quality Measurement Tests for the Proposed System

Many testing techniques are used to calculate system performance and encryption quality. The testing technique results are testing the encryption system based on proposed system and comparing the results with the one of the strong image encryption algorithm which is the traditional chaotic system results.

It is important to obtain the system performance on different kinds of images and compare the results with that of the traditional chaotic system results. To evaluate the system performance, ARE, EQ, correlation coefficient, entropy, irregular deviation analysis, maximum deviation analysis and peak signal to noise ratio are used.

According to the tests results in Table (3), it could be noticed that:

1) In most cases, the proposed algorithm performance is either very near to the best test result of the traditional system and in the three cases it has the best result.
2) The proposed algorithm performance is the best system for image encryption in quality.

The testing results are evaluated after the proposed algorithm is applied on these images and comparing the results with the applying results of the traditional systems as shown in Table (3).

Table 3: Proposed algorithm and traditional system evaluation performance tests results

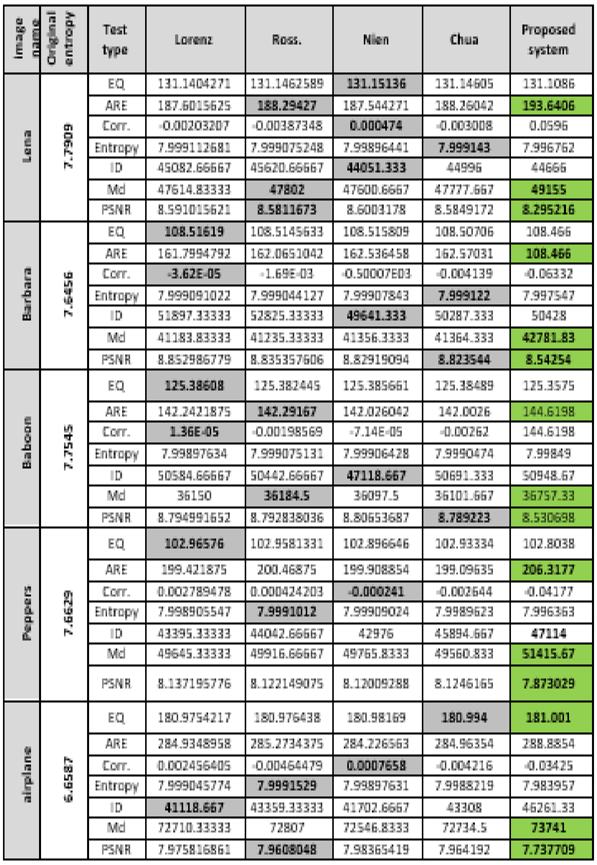


Image name	Original entropy	Test type	Lorenz	Ross.	Nlen	Chua	Proposed system
Lena	7.7909	EQ	131.1404271	131.1462589	131.15136	131.14605	131.1086
		ARE	187.6015625	188.29427	187.544271	188.26042	193.6406
		Corr.	-0.00203207	-0.00387348	0.000474	-0.003008	0.0596
		Entropy	7.999112681	7.999075248	7.99896441	7.999143	7.996762
		ID	45082.66667	45620.66667	44051.333	44996	44666
		Md	47614.83333	47802	47600.6667	47777.667	49155
		PSNR	8.591015621	8.5811673	8.6003178	8.5849172	8.295216
Barbara	7.6456	EQ	108.51619	108.5145633	108.515809	108.50706	108.466
		ARE	161.7994792	162.0651042	162.536458	162.57031	108.466
		Corr.	-3.62E-05	-1.69E-03	-0.50007E03	-0.004139	-0.06332
		Entropy	7.999091022	7.999044127	7.99907843	7.999122	7.997547
		ID	51897.33333	52825.33333	49641.333	50287.333	50428
		Md	41183.83333	41235.33333	41356.3333	41364.333	42781.83
		PSNR	8.852986779	8.835357606	8.82919094	8.823544	8.54254
Baboon	7.7545	EQ	125.38608	125.382445	125.385661	125.38489	125.3575
		ARE	142.2421875	142.29167	142.026042	142.0026	144.6198
		Corr.	1.36E-05	-0.00198569	-7.14E-05	-0.00262	144.6198
		Entropy	7.99897634	7.999075131	7.99906428	7.9990474	7.99849
		ID	50584.66667	50442.66667	47118.667	50691.333	50948.67
		Md	36150	36184.5	36097.5	36101.667	36757.33
		PSNR	8.794991652	8.792838036	8.80653687	8.789223	8.530698
Peppers	7.6629	EQ	102.96576	102.9581331	102.896646	102.93334	102.8038
		ARE	199.421875	200.46875	199.908854	199.09635	206.3177
		Corr.	0.002789478	0.000424203	-0.000241	-0.002644	-0.04177
		Entropy	7.998905547	7.9991012	7.99909024	7.9989623	7.996363
		ID	43395.33333	44042.66667	42976	45894.667	47114
		Md	49645.33333	49916.66667	49765.8333	49560.833	51415.67
		PSNR	8.137195776	8.122149075	8.12009288	8.1246165	7.873029
airplane	6.6587	EQ	180.9754217	180.976438	180.98169	180.994	181.001
		ARE	284.9348958	285.2734375	284.226563	284.96354	288.8854
		Corr.	0.002456405	-0.00464479	0.0007658	-0.004216	-0.03425
		Entropy	7.999045774	7.9991529	7.99897631	7.9988219	7.983957
		ID	41118.667	43359.33333	41702.6667	43308	46261.33
		Md	72710.33333	72807	72546.8333	72734.5	73741
		PSNR	7.975816861	7.9608048	7.98365419	7.964192	7.737709

Conclusions

In this work, the proposed encryption algorithm as per the suggested encryption system and their outcomes, the accompanying conclusions can be recapitulation: The suggested algorithm is able to encrypting any input data such as text message, image and audio, In addition, using the spiral and transposing techniques of the bits stream in the proposed algorithm system increases the system complexity. As well the proposed algorithm system has excellent performance results compared with the performance of the traditional encryption systems in which passed all the FIPS PUB 140-1 statistical tests successfully. and the test results of ARE, maximum deviation analysis and peak signal to noise ratio test of the proposed real time encryption algorithm are better than the testing results of the traditional chaotic flow sequences.

References

M. Matyas, M. Peyravian (1998); Reversible procedure public-key data mixing for efficient encryption

J. Katz and L. Yehuda (2007) Introduction to Modern Cryptography.

R. Hosseinkhani1 and S. Hamid (2012) Using image as cipher key in AES

W. Stallings (2009); Cryptography and Network Security Principles and Practices; Fourth Edition; Pearson Education; Prentice Hall.

P. hristof, P. Jan, Stream Ciphers (2009), Chapter 2 of Understanding Cryptography, A Textbook for Students and Practitioners.

L.R. Jan (2011)The Block Cipher Companion. Springer. ISBN 9783642173417.

B. Katz and C. Sahin (2016.),,Real-Time Wireless Physical Layer Encryption

J. Majumder and P. Bankura (2013) Color Image Encryption Using Spiral Encoding Technique and Symmetric key