Proposed Algorithm for Encrypting the(JPEG)Compressed Image

Abdul Monem S. Rahma*,Ph.D.(Prof.) Zainab J. Hanash*

Abstract

In image encryption algorithms, encryption security and encryption speed are important aspects in the field of data transmission (including digital image transmission) via the Internet, the need arises to protect data by encrypting it, in this paper proposes an algorithm that is characterized by precision and safety. It works in 15 rounds and applies encryption to the compressed image (JPEG), Taking into consideration data image of loss after the decryption process. The goal is to supply a highly secure encryption algorithm with increase the speed significantly based on field GF (P) that adopted in the algorithm advance encryption standard (AES).

Keywords: cryptography, key generator, randomness, symmetric key, AES, block cipher, JPEG.

*University of Technology

1. Introduction

Joint Photographic Experts Group (JPEG) is an advanced lossy compression method for color or grayscale still images (not videos). It does not manage bilateral level images (black and white) extremely well it works best on continuous tone images. Where neighboring pixels like colors, the various features of the JPEG format allow the user to set the resolution of the missing data (as well as the compression ratio) over a wide range. Thus, the eye cannot see any image degradation, even at pressure factors of 10 or 20.

The main objectives of JPEG compression are high compression ratios; the use of multiple parameters; achievement of good results with any type of continuous tone image; the ability to obtain compression/quality trade-off, no matter what the image dimension, color spaces, pixel aspect ratios, or other image features. The (JPEG) compression method is sophisticated, but not too complex, and it permits software and hardware applications on many platforms and in several modes of operation: sequential, hierarchical, and progressive modes.

The JPEG standard has proved successful and has become widely used for image compression, particularly in web pages [1]. The algorithm proposed in this paper this type of digital image used.

2. Related works:

At the last year several symmetric cipher can be proposed, so that the list of the last proposed as follow:

1. Kawl et al. (2014) introduced a new AES algorithm by reducing the calculation and computation overhead. To reduce the problem of a high number of calculations, they replace the Mix column step by a permutation step. The Mix column stage gives a high level of security, but it takes a long time for calculation, which makes the encryption algorithm slow. The other transformations in AES remain unchanged [2] .

2. Ali A. et al, in this researcher used a new AES cipher method which can be depended on shift register in addition to the chaotic map for encryptiing the image. The aim of this new method was, to reduce time and to increase encryption of image [3] .

3. Li (2004) proposed a new design of the S-Box. In this algorithm, the original S-Box table has been partitioned into 32 small S-Box look-up tables. These partitioned tables are used to substitute the bytes in the State matrix in parallel, while the original AES design is sequential. The new results show a good improvement in time compared to the original AES. The obtained improvement speedup of the proposed design is about eight times faster than the original S-Box look-up table through the substitution process [4] .

4. Omar A. Dawood, et al. (2015) proposed a cipher that uses the SPN structure and what is known as the Galois Field (GF) [2^8]. It is an iterated cipher that has a conservative design which is easily implemented in both hardware and software [5] .

5. Atheer M. Abbas Al-Abbass (2015) provide a state of balance between time and complexity of encrypted documents by using multiple irreducible polynomials with order of 8, 4, and 2 (high, medium, and low complexity, respectively) depending on the importance of the document [6] .

6.Hala Bahjat.,and May A. Salih (2014 proposed " Speed Image Encryption Scheme using Dynamic Galois Field GF(P) Matrices ",The studied case showed in this paper works on GF(7) and for encryption key sizes varying from 3X3 to 12X12. The goal was to provide a highly secure encryption algorithm with a wide space for encryption speed [7] .

3. The objective of encryption:

"Cryptography" is the term can be connected with the design problem and encryption and schemes of analyzing [8] . Cryptography is the science, which is writing secret. This art or science

involve information transform into unintelligible garbage, so that unwanted eyes will be unable to comprehend [9] . Cryptography involved number theory of dive willy– nilly, so that, natural numbers study, most mathematics areas that is beautiful. The number of involvement cryptography theory is not limited, to these area mathematicians important made [10] .

To secure system, there are many factors must be combined. For example, it should not be possible for hackers to exploit bugs, break into a system, and use an account they shouldn't be able to buy off your system administrator. They shouldn't be able to steal your back-up. These things lie in the realm of system security. The cryptographic protocol is just one piece of the puzzle. If it poorly designed, the attacker will exploit that. For example suppose the protocol transmit a password in the clear (that is, in the way that any way watching can understand what it is). That is a protocol problem not a system problem, in addition it will certainly be exploited [11] .

4. Basic requirement of block cipher

In a block cipher, a group of plain text elements greater than one charterer are encrypted together creating a group of cipher text. A block cipher is one in which a block of plain text is treated as a whole and used to produce cipher text blocks of equal length. Successful block cipher designs often integrate the concepts of confusion and diffusion [12] .

5. Finite Fields

Let p be a prime number. The integers mod p, consisting of the integer {0, 1,2, . . ., p−1} with addition and multiplication performed mod p, is a finite field of order p [12] . This paper was adopted for the field GF (P).

6. The AES structure and implementation

This algorithm is not a Feistel structure. One noticeable feature of this structure. Recall that, in the classic Feistel structure, half of

the data block is used to modify the other half of the data block, and then the halves are swapped. AES uses substitutions and permutation as a replacement for processes the entire data block as a single matrix during each round.
The key that is provided as input is extended into an array of forty-four 32-bit words, w[i]. Four distinct words (128 bits) serve as a round key for each round. Four various stages are used, three of substitution and one permutation:

1. Substitute bytes**:** byte-by-byte substitution of the block, using an S-Box to implement it.

2. Shift Rows: A simple permutation.

3. Mix Columns: A substitution that makes use of arithmetic over GF(2^8).

4. Add Round Key**:** A simple bitwise(XOR) of the current block with a part of the expand key produces a very simple structure. For both encryption and decryption, the cipher starts with an Add Round Key phase, and then it continues with nine rounds that each contains all four phases, and it ends with a tenth round of three phases.

Only the Add Round Key phase makes use of the key. Therefore, the cipher starts and ends with an Add Round Key phase. Any other stage, applied at the start or end, is reversible without knowledge of the key and so would add no security.
The Stage of Add Round Key is, in fact a form of Vernam cipher and by itself would not be remarkable. The other three phases together provide diffusion, confusion, and nonlinearity. However, by themselves they would not provide security because they do not use the key. We can view the cipher as alternating operations of (XOR) [13] .

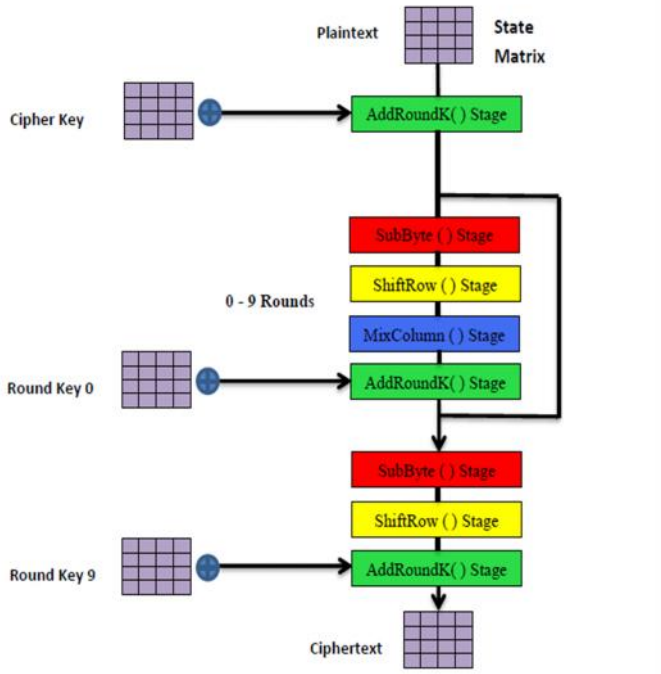

Figure 1. Block Diagram for the AES Structure.

7. Five Basic Tests

Five statistical tests are used to determine whether the binary sequences possess some specific features. If a truly random sequence would appear, it confirms that the result of the test is not specific, but, rather, is probabilistic. If a sequence passes all five tests, it does not ensure that the sequence actually resulted from a random bit generator [14] .

8. The proposed algorithm

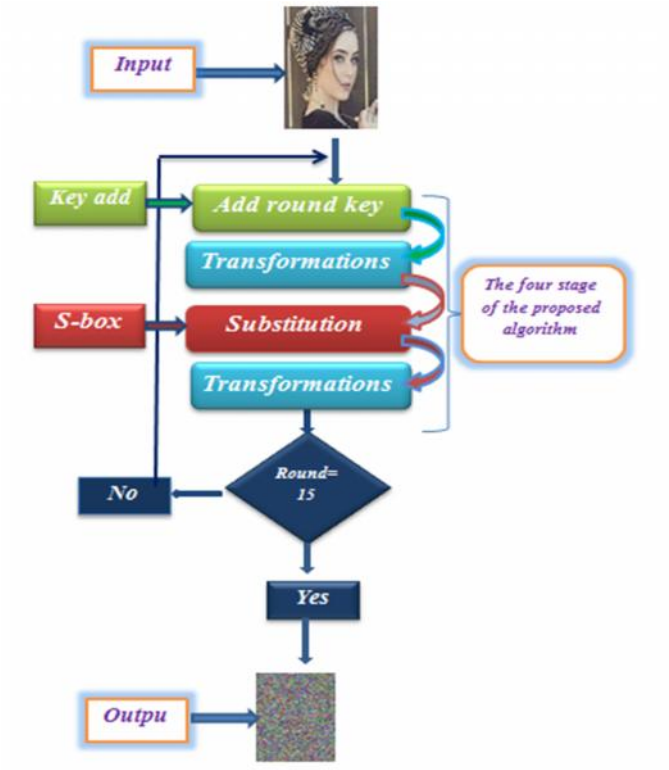

Figure 2. Block Diagram for the proposed algorithm

8.1 Characteristics of the proposed algorithm

- Execution algorithm in (15) round.
- Implemented in a prime number.
- Dividing the input image into four blocks (25*25).
- The key size is (5*5).
- This algorithm based on a random encryption of the blocks.

8.2 Description of the Proposed Algorithm

The proposed algorithms are similar to the (AES) of the structural hand and stages. And the difference are in the number of rounds (since the proposed algorithm (15) round), key generator where the key is generating randomly within the range (0-255), as well as deleting one stage (Mix Column). With a repeating another stage (shift row), to increase the complexity and reduce the time. In the proposed

algorithm return the process (transformation) in different directions in the second and the fourth phase for each round.

8.3 Illustrate the proposed algorithm

Implementation of the above-mentioned of the four operations algorithm during the 15 round, in the first round will be executed of the four operations on all blocks. In the rest of the rounds will be selected random blocks according to random matrix within the range (1 -15) this matrix corresponds to another matrix that generates random numbers within the range [1-4].
The first step chooses an image size [100*100] was divided into four equal-sized blocks, each block size [25*25]. For example:

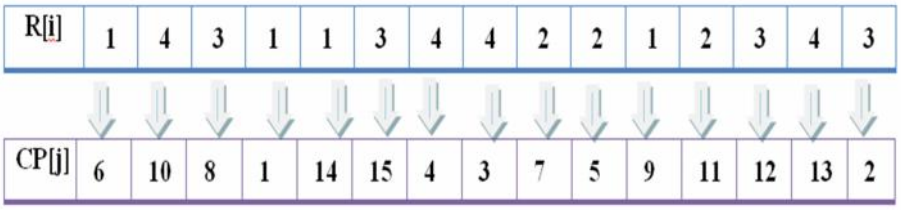

Figure 3. Illustration of the method of selecting blocks randomly

R[i] : The random matrix containing fifteen cell, that determines any Block will be selection to encrypt. And will be within the range [1-4], according to a number of blocks of the image.

CP[j]: The random matrix containing fifteen cell that, determines how often processing, of the block who was chosen from the previous matrix R[i]. It will be within the range [1-15] depending on the number of proposed algorithm rounds.

For example: Let's take the first position in the matrix R[i], which means any block will be selected, it is contains a number 1, This means in the first round will be selected first block .
Now, let's take the first position in the matrix CP[j]. Then the first location of the matrix R[i] was 1, and the first location of the matrix CP[j] is 6. This means first block will encrypts six times.

Then the second location of the matrix R[i] is 4, and the second

location of the matrix CP[j] was 10, this means fourth block will encrypts ten times, and so on.

8.4 Modified algorithm:

Algorithm 1 The Proposed algorithm Encryption/Decryption.
Input: Image [100,100] size, key add. Output: cipher image.
BEGIN **Step1:** input image is split into equal Block - four Blocks each block [25, 25]. **Step2:** for each blocks of step1 applied the following operations: 1. The Round Key Addition function.(As it is the AES) 2. Transformations function. 3. Sub Byte Transformation function. (As it is the AES) 4. Transformations function. **Step2.1:** make addition function between blocks and key matrix. **Step2.2:** implement transform function on the output of step 2.1 **Step2.3:** applied substation function on output of step 2.2. **Step2.4:** applied step 2.2 again. **Step3:** select random block there is of step and save into [K] matrix. **Step4:** for all R application step 2.1 to 2.4 based on a random encryption of the blocks matrix, with the exception of the first round, the four operations will be implemented for All the blocks in the image. **Step5:** repeat step 3 to step 4 until 15 round. END

8.5 The four stages of the proposed algorithm

8.5.1 The proposed AddRoundkey stage

In this proposed the size of element is fixed as well as the key matrix is constant in all (15) rounds. In this stage, the key matrix is provided with the same size of the block image, where the pro-

cess (XOR) between the elements of the block (5 * 5) and the key random generated (5 * 5), as shown in the following algorithm (2):

Algorithm2:TheProposed Add Round key Encryption/Decryption Transformation Function
Input: block image
Output: State1 matrix
Begin Step1: The dimension of block matrix is 5*5 Step2: Each cell in the matrix of block is added with the cell key matrix and the results are stored in state1 matrix. End.

8.5.2Transformations function:

Transport can be operated in this stage. It can be done within the blocks in different directions for each block to increase the complexity, without changing the element values. It will be explained in detail, shown in the following algorithm (3).

There are three types of transport:

1. Main diagonal (transport).
2. Upper (left to right).
3. Lower (top to bottom).

The process will be applied on the results of the previous stage on all blocks during the 15 round, at this stage (the second stage of the algorithm), which is implemented in each round.

$$R[I] = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 \end{pmatrix} \quad >> \text{ Matrix before transport}$$

1. Main diagonal (transport)

Diffusion matrix, that resulting from previous operations (add), where transport is to convert rows to columns. At this stage, it will be transferred to each row and a column, as shown in the example, as the row (1 2 3 4) turned into a column, and so on for the rest of rows, so the resulting matrix will be R[i]1.

R[I]1 =

1	**5**	**9**	**13**
2	**6**	**10**	**14**
3	**7**	**11**	**15**
4	**8**	**12**	**16**

>>first transport

Main diagonal (transport)

2. Upper (left to right)

At this stage, it will be moving in each line from left to right. That is to say, the top row of the matrix (1 2 3 4) will be (4 3 2 1) , (5 6 7 8) will be (8 7 6 5), (9 10 11 12) will be (12 11 10 9) and the bottom row of the matrix (13 14 15 16) will be (16 15 14 13), as shown in the example R[i]2.

R [I] 2=

4	**3**	**2**	**1**
8	**7**	**6**	**5**
12	**11**	**10**	**9**
16	**15**	**14**	**13**

>> second transport

Upper (left to right)

3. Lower (top to bottom)

At this stage, it will be move to the first row; this will turn down to the last row and will turn to the top of each block [4 * 4]. That is to say, the top row of the matrix (1 2 3 4) will turn to the last row (1 2 3 4)). As well as for the last row, the same approach is intended. Then, (13 14 15 16) turns to the top and so on, as shown below for R[i]3.

$$R[I]3=\begin{pmatrix} 13 & 14 & 15 & 16 \\ 9 & 10 & 11 & 12 \\ 5 & 6 & 7 & 8 \\ 1 & 2 & 3 & 4 \end{pmatrix} >> \text{Third transport}$$

Lower (top to bottom)

The results are considered as shown in the following algorithm (3):

Algorithm 3: The Proposed Shift Rows Encryption/Decryption Transformation Function
Input: State1 matrix
Output:State2 matrix
Begin Step1: Apply the first operation on the blocks (Main diagonal(transport)) Step2: Apply the second operation on the blocks (Upper (left to right)) Step3: Apply the third operation on the blocks (Lower (top to bottom)) End.

8.5.3The proposed Substitution stage.

SubBytes: The modified algorithm S-Box supplies a permutation of a group of 256 possible input bytes and is provided as a look-up table. The operation SubBytes Switching the old value with the new value, as shown in the following algorithm:

Algorithm 4: The Proposed substitution Encryption/Decryption Transformation Function
Input: state2 matrix
Output: state3 matrix
Begin Step1: It generated S-Boxes. Step2: The dimension of state2 matrix is (5*5). Step3: pass any cell of the state2 matrix to the chosen (S-Box) in step1 and store the result of the element in the state3 matrix, and so on for the other cases. End.

8.5.4Transformations function:

Transport operations in the fourth phase are different from-transport operations in the second phase as described follows:

1. Left right then top to bottom.
2. Transport then left right.
3. Transport then top to bottom.

$$R[I] = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 \end{pmatrix}$$ >> Matrix before transport

1. Left right then top to bottom

At this stage, it will be move to the first row(1 2 3 4) to the right will be (4 3 2 1) and turn to the last and the last row (13 14 15 16) will turn to the top of each block [4 * 4], the same approach is intended. Then, and so on, shown below for R[i]1.

$$R[I]\,1 = \begin{pmatrix} 16 & 15 & 14 & 13 \\ 12 & 11 & 10 & 9 \\ 8 & 7 & 6 & 5 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$ >>first transport

Left right then up down

2. Transport then left right

in this stage columns converted to rows., it will be trans-ferred to each column switch row with move left to right , for example the row (1 5 9 13) turned into a column, with turn from left to right will be (13 9 5 1), (2 6 10 14) will be (14 10 6 2) , (3 7 11 15) will be (15 11 7 3), (4 8 12 16) will be (16 12 8 4), as shown below for R[i]2.

$$R[I]2=\begin{pmatrix} 13 & 9 & 5 & 1 \\ 14 & 10 & 6 & 2 \\ 15 & 11 & 7 & 3 \\ 16 & 12 & 8 & 4 \end{pmatrix} >> \text{second transport}$$

Transport then left right

3. Transport then top to bottom

In this stage columns converted to rows., it will be transferred to each column switch row with move top to bottom, for example the colomn (1 5 9 13) turned into a row, with switch in the last row and so on, as shown below for R[i]3.

$$R[I]3=\begin{pmatrix} 4 & 8 & 12 & 16 \\ 3 & 7 & 11 & 15 \\ 2 & 6 & 10 & 14 \\ 1 & 5 & 9 & 13 \end{pmatrix} >> \text{Third transport}$$

Transport then top to bottom

The results are considered as shown in the following algorithm (5):

Algorithm 5: The Proposed Shift Rows Encryption/Decryption Transformation Function
Input: State3 matrix
Output:State4 matrix (cipher block)
Begin Step1: Apply the first operation on the blocks (Left right then top to bottom) Step2: Apply the second operation on the blocks (Transport then left right) Step3:Apply the third operation on the blocks (Transport then top to bottom) End.

1. **The process of generation of keys:**
   The key provider is characterized by the ability to generate keys for all rounds of algorithm. Where it certain keys are generated for the Add Round stage and have been stored in the (key matrix1).

2. **Decryption for the proposed algorithm:**
   It may be noted to the decryption process the same steps the decryption for the proposed algorithm works through implementing the inverse of all four operations which were described previously, but by using the inverse of key.

9. The result of the Modified algorithm:

Table (1) Comparison of Time between the Proposed Algorithm and the AES

Algorithms	No. of image	Block Size	Key Size	Time Encryption (M.S.ms)	Time Decryption (M.S.ms)
Original-AES (Rijndael) (10 rounds)	text	240128 -bit	128-bit	1.27.796	-
The Proposal algorithm (15 rounds)	1. JPEG image (a)	240128 -bit	128-bit	0.0.493	0.0.546
	2. JPEG image (b)	240128 -bit	128-bit	0.0.528	0.0.522
	3. JPEG image (c)	240128 -bit	128-bit	0.0.488	0.0.529
	4. JPEG image (d)	240128 -bit	128-bit	0.0.488	0.0.520

In this table, the elapsed time is examined to encrypt a given block between the proposed algorithm and the AES algorithm. The time elapsed in the proposed block encryption algorithm is less than is spent in the algorithm (AES). And it should be noted for the time in the proposed algorithm which is attributed to the uneven time despite the uniform size of the image. Using a random key for each image, as shown in Table1.

Table (2) Randomness Test to the Image (JPEG)

No. of image	Frequency test	WITH FREEDOM DEGREE & MUST BE	Run test		WITH FREEDOM DEGREE & MUST BE	
I1. mage (a)	0.952	1	T0	30.732	27	<=39.829
		<=3.84	T1	29.119	21	<=32.386
2. Image (b)	2.183	1	T0	13.207	14	<=23.401
		<=*3.84*	T1	26.588	16	<=26.012
3. Image (c)	0.062	1	T0	23.109	26	<= 38.601
		<=3.84	T1	27.193	19	<= 29.859
4. Image (d)	0.032	1	T0	30.728	20	<= 31.126
		<=3.84	T1	9.831	16	<= 26.012

Table (3) Randomness Test to the Image (JPEG)

No. of image	Poker test	WITH FREEDOM DEGREE & MUST BE	Serial test	WITH FREEDOM DEGREE & MUST BE
1. Image (a)	10.439	5	5.697	3
		<=11.1		<=7.81
2. Image (b)	12.018	5	4.677	3
		<=11.1		<=7.81
3. Image (c)	4.652	5	5.346	3
		<=11.1		<=7.81
4. Image (d)	0.883	5	0.314	3
		<=11.1		<=7.81

Table (4) Randomness Test to the Image (JPEG)

	Image (a)	Image (b)	Image (c)	Image (d)
Shift 1	8.366	3.147	0.072	2.795
Shift 2	6.784	0.058	1.242	0.000
Shift 3	3.046	0.179	3.103	2.048
Shift 4	1.033	5.960	1.179	2.535
Shift 5	3.564	2.396	3.284	3.176
Shift 6	3.494	2.386	3.322	3.183
Shift 7	0.128	3.219	0.189	0.002
Shift 8	0.001	1.815	0.742	0.621
Shift 9	0.368	0.670	0.200	0.193
Shift 10	0.089	0.499	1.728	0.874

Figure 4. illustrates the image encryption.

10. Security complexity analysis

Algorithm can be based design to offer the security with high level. So that the cipher can be designed with large security aspects. It based on the encryption blocks to increase the complexity by the following functions. Can be calculated the number of each block and then multiply the possibilities in the 15 round.

Table (5) Illustration of Security Complexity Analysis

The operation	In 15 round
• The Round Key Addition function	(5*5*256)*15
• Transformations function	(3*5*5*256)*15
• Sub Byte Transformation function	(5*5*256)*15
• Transformations function	(3*5*5*256)*15

11. Comparing the work with previous work:

The comparison of the work will be held with the algorithms (advance encryption standard).The comparison to the time required for encryption between the (AES) and the proposed algorithm with the same image size, where the proposed algorithm is faster than (AES). As shown in the table(1).

12. Conclusion

The implementation of using a set of block-encrypting functions (The Round Key Addition function, Sub Byte Transformation function, Transformations function) based on field GF (P), on the compressed image (JPEG), Depending on the random encrypting of blocks, led to a reduction in the encryption time. Randomizing block selection combined with randomizing the selection of a fixed number within the range of rounds (15) raised the complexity of the algorithm. The proposed algorithm has achieved a high speed compared to the (AES).

References

[1] Salomon, D, "Data Compression", Fourth Edition ,Springer- Verlag London Limited 2007.

[2] Kawle, P., Hiwase, A., Bagde, G. , Tekam, E. and Kalbande, R. , Modified Advanced Encryption Standard, International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-4, Issue-1, March , 2014.

[3] ALI ABDULGADER et al, “ENHANCEMENT OF AES ALGORITHM BASED ON CHAOTIC MAPS AND SHIFT OPERATION FOR IMAGE ENCRYPTION”, Journal of Theoretical and Applied Information Technology 10th January 2015. Vol.71 No.1© 2005 - 2015 JATIT & LLS.

[4] Li, H., A Parallel S-box Architecture for AES Byte Substitution, IEEE International Conference on communications, Circuits and Systems, June 2004, Vol.1, 2004.

[5] Omar A. Dawood, Abdul Monem S. Rahma and Abdul Mohsen J. Abdul Hossen,“The New Block Cipher Design (Tigris Cipher)”, I. J. Computer Network and Information Security, 2015

[6] Metaab, A.;" AUTOMATING SECURITY AND TIME BALANC ING IN INSTITUTIONAL DAILY WORK ON DATA TRANSFER ", 2015.

[7] Bahjat, H.; et al, " Speed Image Encryption Scheme using Dynamic Galois Field GF(P) Matrices ", International Journal of Computer Applications (0975 – 8887) Volume 89 – No.7, March 2014.

[8] David bishop, "introduction to cryptography with ™ applets", Grinn ell College," Jones and Bartlett
Publishers International", 2003

[9] Oded Gold Reich,"Foundations of Cryptography", Springer-Verlag, 1999

[10] Michael Welschenbach, "Cryptography in C and C++", second ed ition, by Springer-Verlag, 2005

[11] Information security. Retrieved from Wikipedia the free Encyclop edia http://en.wikipedia.org/wiki/Information _seaurity,2005.

[12] S, William ., "Cryptography and Network Security: Principles and Practice", Fifth Edition, Prentice Hall, 2011.

[13] NIST," Advanced Encryption Standard (AES)", Federal Information Processing Standards Publication (FIPS PUB) 197, Nov 2001.

[14] Andrew, R. & Juan, S. & Miles, S.," Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications" ,NIST Special Publication 800, 2001

الخوارزمية المقترحة لتشفير الصورة المضغوطة (JPEG)

أ.د. عبد المنعم صالح رحمة * زينب جواد حنش العابدي *

المستخلص

في خوارزميات التشفير, الأمن والسرعة من الجوانب الهامة في مجال نقل البيانات (بما في ذلك نقل الصور الرقمية) عبر الانترنيت, ولحماية البيانات يتم تشفيرها.
في هذا البحث تم اقتراح خوارزمية تتميز بالدقة والامان و تعمل على round(15) مع الاخذ بنظر الأعتبار الحفاظ على بيانات الصورة من الفقدان بعد عملية فك التشفير وتطبق على الصورة الرقمية (jpeg) وبالاعتماد على حقل GF(P) حيث حققت هذه الخوارزمية السرعة المطلوبة مع التعقيد, وذلك بالتعديل على خوارزمية (AES).

*الجامعة التكنولوجية