ISSN: 0067-2904

Modified Blowfish Algorithm for Image Encryption using Multi Keys based on five Sboxes

Nada Hussein M. Ali[1*], Suaad Ali Abead[2]
[1]Department of Computer Science, College of Science, University of Baghdad, Baghdad, Iraq
[2]Department of Computer Science, College of Science for women, University of Baghdad, Baghdad, Iraq

Abstract

In this paper, a new modification was proposed to enhance the security level in the Blowfish algorithm by increasing the difficulty of cracking the original message which will lead to be safe against unauthorized attack. This algorithm is a symmetric variable-length key, 64-bit block cipher and it is implemented using gray scale images of different sizes. Instead of using a single key in cipher operation, another key (KEY2) of one byte length was used in the proposed algorithm which has taken place in the Feistel function in the first round both in encryption and decryption processes. In addition, the proposed modified Blowfish algorithm uses five Sboxes instead of four; the additional key (KEY2) is selected randomly from additional Sbox5, the fifth Sbox is formed in GF(2^8) and it is variable to increase the complexity of the proposed algorithm. The obtained results were tested using many criteria: correlation criteria, number of pixels change rate (NPCR) and mean square error (MSE). These tested factors were approved by the output results which demonstrated that the correlation of image elements in the proposed algorithm was significantly reduced during the encryption operation. Also, the algorithm is very resistant to attempts of breaking the cryptographic key since two keys were used in the encryption/ decryption operations which lead to increase the complexity factor in the proposed algorithm.

Keywords: Blowfish, MSE, Encryption, Decryption, NPCR, Correlation, Gray scale images.

تعديل لخوارزمية السمكة المنتفخة لتشفير الصور باستخدام مفاتيح متعددة بالاعتماد على خمسةSboxes

ندى حسين محمد علي[1*]، سعاد علي عبيد[2]
[1]قسم علوم الحاسبات ، كلية العلوم، جامعة بغداد، بغداد، العراق
[2]قسم علوم الحاسبات، كلية العلوم للبنات، جامعة بغداد، بغداد، العراق

الخلاصة

في هذا البحث، اقترح تعديل جديد لتعزيز مستوى الأمان في خوارزمية السمكة المنتفخه.هذه الخوارزمية تعتبرمن ذوات المفاتيح المتناظرة والمتغيرة الاطوال،وذات 64 بت كتلية الشفرات. والهدف من هذا النهج الجديد والذي يتم تنفيذه باستخدام الصور الرمادية ذات أحجام مختلفة، هو لزيادة صعوبة تكسير الرسالة الأصلية التي من شأنها أن تؤدي إلى تكون آمنة ضد نوع الهجوم الغير مخول به. فبدلا من استخدام مفتاح واحد في عملية التشفير، تم استخدام مفتاح آخر (KEY2) يتكون طوله من بايت واحد في الخوارزمية المقترحة والتي تم التحديث فيها في دالة Feistel في الدورة الأولى في كل من عمليات التشفير وفك التشفير. وبالإضافة إلى ذلك، تستخدم خوارزمية السمكة المنتفخة المقترحة خمسة Sboxes بدلا من أربعة .يتم تحديد مفتاح إضافي

*Email: nada husn@yahoo.com

(KEY2)بشكل عشوائي من Sbox5 الاضافية، ويتم تشكيل Sboxالخامس في GF (2^8) ويكون متغير وذلك لزيادة تعقيد الخوارزمية المقترحة. تم اختبار النتائج التي تم الحصول عليها باستخدام العديد من المعايير : معايير الارتباط، ونسبة عدد البكسل المتغيرة (NPCR) ومعدل مربع الخطأ (MSE) .وتم التأكد من خلال الاختبار لهذه العوامل من قبل نتائج الإخراج التي أثبتت أن الترابط بين عناصر الصورة في التقنية المقترحة انخفض بشكل ملحوظ خلال عملية التشفير. وأيضا، فإن هذا النظام مقاوم لمحاولات كسر مفتاح التشفير وذلك لاستخدام مفتاحين في عمليات التشفير /فك التشفير التي تؤدي إلى زيادة عامل تعقيد في الخوارزمية المقترحة.

Introduction

In the symmetric cipher systems, the sender and receiver use identical key in the cipher operation (encryption and decryption). Symmetric key methods can be categorized into two sets; either block ciphers or stream ciphers [1]. Blowfish is a symmetric block cipher that can be effectively used for encrypting and safeguarding of data. It takes 64-bit block size and a variable key length from 32-bit up to 448 bit and it is a 16-round Feistel cipher and uses large key-dependent S-boxes [2].

Finite fields are fields with only finitely many elements, these are also called Galois Fields GF, in honor of Evariste Galois (1811-1832) who in his study of roots of polynomials discovered many of their fundamental properties. Too many cryptographic algorithms are based on finite field arithmetic (such as: Diffie and Hellman, 1976; ElGamal, 1985; Miller, 1986; Kravitz, 1993 and the Advanced Encryption Standard, AES) [3]. Arithmetic in a finite field is different from standard integer arithmetic. There are a limited number of elements in the finite field; all operations performed in the finite field result in an element within that field [1]. Finite fields of order p, where p is a prime number, is denoted as GF(p). The $GF(2^n)$; for $n > 1$; is another representation for prime numbers were all arithmetic operations are mod over irreducible polynomials [4].This paper presents a proposed modification of the Blowfish algorithm in Feistel function based on finite fields $GF(2^n)$ to increase the complexity degree in encryption and decryption processes.

Related works

In [5] suggests an improvement to the blowfish algorithm, the modifications made inside the F-Function and the key generated process to increase the complexity and the confusion for the s-boxes. The achieved results proved that the time needed to attack the proposed algorithm was increased compared to the Blowfish algorithm. [6]introduce a new method to enhance the security level in key expansion layout in Blowfish algorithm. This enhancement was done using multiple keys, these keys generated by Cellular Automata (CA) randomly. The CA produces numbers as a pseudo number generator (PSNG) which represent multiple keys used in different rounds of the algorithm. The obtained results shown the proposed algorithm was resistant to breaking cipher key. In [7] proposed a new method to derive the encryption key in the Blowfish algorithm from a color image chosen by the sender and receiver users. The key is selected from a specific position in the image, the goal of the proposed algorithm is to overcome the weakness of the Blowfish algorithm key since it is symmetric. The results of the suggested method lead to increase the difficulty of cryptanalyst against cracking the key. In [8] Focus of this research is to optimize the four S-boxes into two S-boxes in original Blowfish algorithm to increase the speed and examine the effectiveness and limitations of some Block cipher algorithms. The program simulation result provides better performance as well as security. The main advantage of optimized Blowfish is that the execution time is reduced to 0.2 milliseconds and the throughput is increased to 0.24 bytes/milliseconds compare than original algorithms.

Blowfish Algorithm

In 1993, Bruce Schneier designed the Blowfish algorithm that has many benefits. It is considered fast, free alternative to existing encryption algorithms and it is also appropriate to implement on hardware in an efficient manner, beside that no license is required [9]. The Blowfish algorithm is a 64-bit block cipher and has three basic operators include XOR, addition and lookup tables; such tables are four S-BOXES and P-array used for mapping operations. This algorithm is based on a Feistel structure design on each round and the strategy of F-function uses the same DES principles. The security level of the Blowfish algorithm is the same as DES but it offers more speed and greater easy implementation on software for such characteristics, it is proposed as an alternative to the DES [10]. The implementation of the Blowfish algorithm in 32-bit microprocessors is faster than DES, especially when the caches are large, for example Pentium and the PowerPC. The Blowfish algorithm involves

two phases: the first phase; the 448- bit key at most are converted into totaling 4168 bytes of many subkey arrays. While the second phase; data encryption; lies in 16-rounds of Feistel structure network and each round has its own key permutation and data substitution operations. All operations of addition and XOR are implemented with word of 32-bit length in each round. The only additional operations are four indexed array data lookups per round [11].

Digital Color Image Processing Concepts

An image can be defined as two-dimensional array of integer numbers, the height and the width which are represented by rows and columns respectively. Each element in this array is denoted point of color called pixels by which the size of an image is specified. Each pixel in the image is indexed by x and y coordinates and stored as 24-bit in color images and 8-bit in gray scale images. The 24-bit images are extended over three bytes which are RGB (red, green, blue) colors respectively. The colors are found by mixing these three RGB colors in different properties [12].

Each pixel has its own properties in the digital image; address indexing as row and column, size and color value. The digitization operation could be defined as an electronic conversion of the photographic image through a digital camera or scanner devices [13]. Figure-1 shows the Blowfish encryption algorithm to encrypt the gray image file.

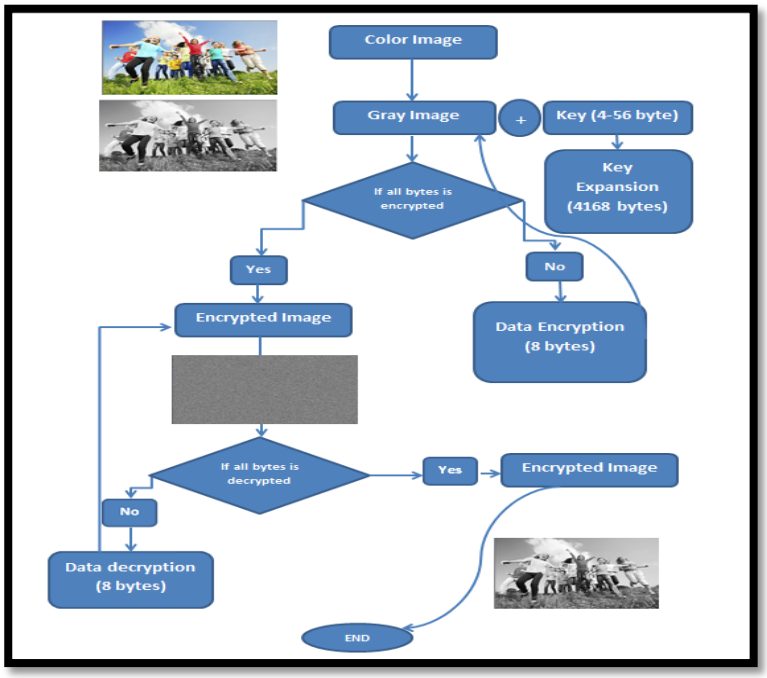

Figure 1- The image encryption by Blowfish algorithm.

Encryption Quality Evaluation

The image encryption operations are defined as the change of pixel value in the image file which could be irregular. The quality of an image encryption means the higher difference between each pixel value before and after the cipher operation. The encryption measurement can be expressed numerically of the total changes, or deviation, in pixel value between the original and encrypted images [14]. In this study, three different factors will be used to measure the encryption quality as in following:

The Correlation Coefficient

The image correlation coefficient measures the relationship, or correlation, between adjacent pixels in the image. This coefficient clarifies the matching between the adjoining pixels. For the encrypted image, this coefficient should be small to make the recognition of any pixel from its neighbor so hard. For example, x_i and y_i are two pixel pairs, then the correlation coefficient can be obtained by the equation [15]:

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

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

$$cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}\left(x_i - E(x)\right) - E(y)\left(y_i - E(y)\right) \quad (3)$$

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(y)}\sqrt{D(y)}} \quad (4)$$

Where $\sqrt{D(x)} \neq 0$ and $\sqrt{D(y)} \neq 0$

where x_i and y_i are gray level value of two adjacent pixels, N is the number of pairs (x_i, y_i) and E(x) is the mean of xi and E(y) is the mean of y_i.

Mean Square Error

Mean Square Error (MSE) is one of the most widely used quality degradation metrics. Let **X** and **Y** two images of size N*M for each one, representing the plain image and encrypted or decrypted images. The mean square error between the two images is thus defined as in the following equation [16]:

$$MSE = \frac{1}{N\times M}\sum_{i=0}^{N-1}\sum_{j=0}^{M-1}[X(i,j) - Y(i,j)]^2 \quad (5)$$

The more Y is similar to X, the more MSE is small. Obviously, the greatest similarity is achieved when MSE equal to 0.

The Number of Pixels Change Rate

The Number of Pixels Change Rate (NPCR) is criteria to assess the differences between the original image and the encrypted image, the mathematical formula of the NPCR measure is formulated as in the following equation [16]:

$$NPCR = \frac{\sum_{i=1}^{N}\sum_{j=1}^{M} Dif(i,j)}{N*M} * 100$$

$$Dif(i,j) = \begin{cases} 1 & I(i,j) \sim = I'(i,j) \\ 0 & I(i,j) \sim = I'(i,j) \end{cases} \quad (6)$$

I(I,j) and I'(i,j) represent the source and encrypted images respectively. As large obtained as possible for NPCR value is considered better to reach the ideal encryption scheme for the digital image performance.

The Proposed Modified Blowfish Algorithm

Instead of using a single key (KEY1) in cipher operation, another key (KEY2) of one byte length was used in the proposed algorithm, this modification was taken place in the Feistel function. The proposed modified Blowfish algorithm uses five Sboxes instead of four; the additional key(KEY2) is selected randomly from additional Sbox5, the new Sbox5 is a nonlinear substitution table that gets a number and returns another number, this table is built in GF(2^8). Equations (7) and (8) clarify the mathematical model to compute each value in various Sbox5 and Sbox5^{-1} respectively. The additional fifth Sbox is variable, this means different Sboxes (Sbox5) are created in GF(2^8). Three initial keys are needed for generating Sbox5 as follows:

1. **Value1**: This key is one byte long; it is used to create the Sbox5 on condition that this key has its associated inverse value for building its inverse table Sbox5^{-1} to retrieve the decrypted values.
2. **Value2**: This key also has one byte long and is used as affine additive value to increase the randomness of the created Sbox5.
3. **Value3 ($poly$):** This key represents 30 different irreducible polynomials [17] used to module the addition and multiplication operations to normalized the output results in GF(2^8).

Equations 7 and 8 had shown the mathematic formulas to build the fifth $Sbox5$and its inverse as in follow:

$$Sbox5[i][j] = \{Value1 * MI[i][j] + Value2\} Mod\ poly \quad (7)$$

$$Sbox5^{-1}[i][j] = \{Value^{-1} * MI[i][j] + Value2^{-1}\} Mod\ poly \quad (8)$$

where MI represents the Multiplicative Invers table in GF(2^8) [13]. Table-1 clarifies the suggested three keys to create three different Sboxe5 tables, the values in first and second columns are variables and depend on user selection. Figures- 2 and 3 clarify the proposed Sbox5 and Sbox5^{-1} tables formed using the keys in the first row of Table-1. Both sender and receiver agree in advance to select any

value from Sbox5 which represents KEY2 to encrypt each pixel in the image. The inverse $KEY2^{-1}$ can be obtained from Equation 8 or $Sbox5^{-1}$ to decrypt the pixels.

The additional key used in encrypted operation is Exclusive OR with Least Significant Byte (LSB) of the plaintext. Each formed Sbox5 has 256 elements, the additional key is selected depending on its row and column indexes, for example; if KEY2=0xA7 selected from Figure-2, where its row index is 0x06 and column index is 0x0C, while in Figure-3 row=0x0A and column=0x07 is the reverse value of KEY2.

Table 1- Three different keys to form various Sbox5 in the proposed algorithm**.**

Value1	Value2	Irreducible polynomial
0x4C	0xC1.	$x^8 + x^4 + x^3 + x + 1$
0x67	0x82	$x^8 + x^7 + x^5 + x + 1$
0x85	0x45.	$x^8 + x^6 + x^5 + x^2 + 1$

The purpose of the second key (KEY2) in cipher operation is to increase the complexity and difficulty of cracking the cipher text as explained below:

1- The second key (KEY2) is variable that depends on its row and column indexes (both ended parties satisfy in advanced on them), the total number of KEY2 space in single Sbox5 is:

$$K_{Space} = 256 \quad (9)$$

2- Different Sbox5 could be created in GF(2^8) from the initial three values, the maximum total space for Sbox5 that could be created is clarified as in follow:

$$Sbox_{Space} = 256(value1) * 256(Value2) * 30(Value3) \quad (10)$$

3- The total KEY2 space in multiples Sbox5 as declared in equations 9 and 10 will be:

$$KEY_{Total_{Space}} = 256 * 256 * 256 * 30 \quad (11)$$

This complexity degree obtained from the proposed algorithm compared to Blowfish algorithm is considered high، this added complexity was achieved using the KEY2 and Sbox5, the modification was applied both in the first round of encryption and decryption operations. Figure-4 shows the block diagram for the proposed modification in Feistel function, while Figure-5 demonstrates the modified Blowfish algorithm. The block of 32- bit is divided into 8-bit blocks a, b, c, and d, the operations inside Function $F(X_L)$ are modified and given by the following steps:

1. $F(X_L)= ((S\ 1,a + S2,d\ ) mod\ 2^{32}) \oplus ((S3,b + S4,c\ ) mod\ 2^{32})$
2. Split the last byte of block $F(X_L)$ as L
3. L $\oplus$ KEY2 (8-bit)
4. Merge the L with block $F(X_L)$, where key2 represent the second key (8-bit length *)*

	Y															
X		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
	0	C1	A5	25	79	65	56	9D	C8	45	C6	0A	EA	39	02	93	A7
	1	83	A8	94	57	F2	C2	54	80	BD	15	F6	58	3E	D8	1C	F1
	2	E0	2E	75	44	6B	0E	5C	AD	8E	2A	96	72	0B	49	B7	22
	3	FF	2D	7D	E6	8C	4C	0D	10	E8	FE	4D	4A	2F	B6	D9	C0
	4	51	5A	36	69	9B	6F	D5	13	42	C5	F0	2B	0F	B8	21	86
	5	B0	2C	34	01	6A	DC	CE	27	A4	71	85	20	FA	D4	30	BA
	6	DE	E4	61	00	9F	26	52	74	B1	E5	D1	B2	A7	19	29	84
	7	55	04	88	06	87	CC	D2	B9	60	12	AC	98	1B	CB	97	3B
	8	5F	68	0C	F3	EC	BE	43	C7	3A	CF	40	EB	1D	09	7E	EE
	9	D6	BF	C3	82	8F	18	62	DA	A6	16	AB	D0	67	1E	B4	5E
	A	AF	A0	37	46	ED	1A	A1	FB	14	C9	4F	33	90	5B	64	9C
	B	73	66	99	78	E3	E7	31	76	8A	89	4B	DD	EF	8B	AA	A3
	C	4E	6E	53	D3	47	3D	F7	DF	38	70	32	50	08	92	CD	3F
	D	F9	FC	05	F8	1F	23	AE	8D	34	7C	7B	59	63	03	B5	DP
	E	5D	17	F5	E9	B3	BB	F4	A9	E2	A2	91	CA	48	9E	FD	95
	F	11	E1	28	9A	77	81	6D	41	7A	07	C4	7F	3C	6C	BC	35

Figure 2- Sbox5 of Value1=0x4C and Value2=0xC1**.**

	Y															
X		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
	0	63	53	0D	DD	71	D2	73	F9	CC	8D	0A	2C	82	36	25	4C
	1	37	50	79	47	A8	19	99	E1	95	6D	A5	7C	1E	8C	9D	D4
	2	5B	4E	2F	D5	D8	02	65	57	F2	6E	29	4B	51	31	21	3C
	3	5E	B6	CA	AB	52	FF	42	A2	C8	0C	88	7F	FC	C5	1C	CF
	4	8A	F7	48	86	23	08	A3	C4	EC	2D	3B	BA	35	3A	C0	AA
	5	CB	40	66	C2	16	70	05	13	1B	DB	41	AD	26	E0	9F	80
	6	78	62	96	DC	AE	04	B1	9C	81	43	54	24	FD	F6	C1	45
	7	C9	59	2B	B0	67	22	B7	F4	B3	03	F8	DA	D9	32	8E	FB
	8	17	F5	93	10	6F	5A	4F	74	72	B9	B8	BD	34	D7	28	94
	9	AC	EA	CD	0E	12	EF	2A	7E	7B	B2	F3	44	AF	06	ED	64
	A	A1	A6	E9	BF	58	01	98	6C	11	E7	BE	9A	7A	27	D6	A0
	B	50	68	6B	E4	9E	DE	3D	2E	4D	77	5F	E5	F2	18	85	91
	C	3F	00	15	92	FA	49	09	87	07	A9	EB	7D	75	CE	56	89
	D	9B	6A	76	C3	5D	46	90	0F	1D	3E	97	DF	55	BB	60	C7
	E	20	F1	E8	B4	61	69	33	B5	38	E3	0B	8B	84	A4	8F	EC
	F	4A	1F	14	83	E6	E2	1A	C6	D3	D0	5C	A7	D1	EE	39	30

Figure 3- Inverse Sbox5 $^{-1}$ of Value1=0x4C and Value2=0xC1.

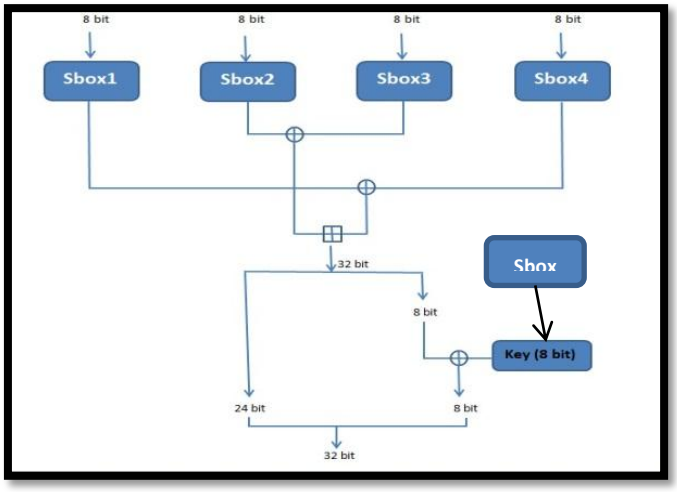

Figure 4- Modified Blowfish Feistel function.

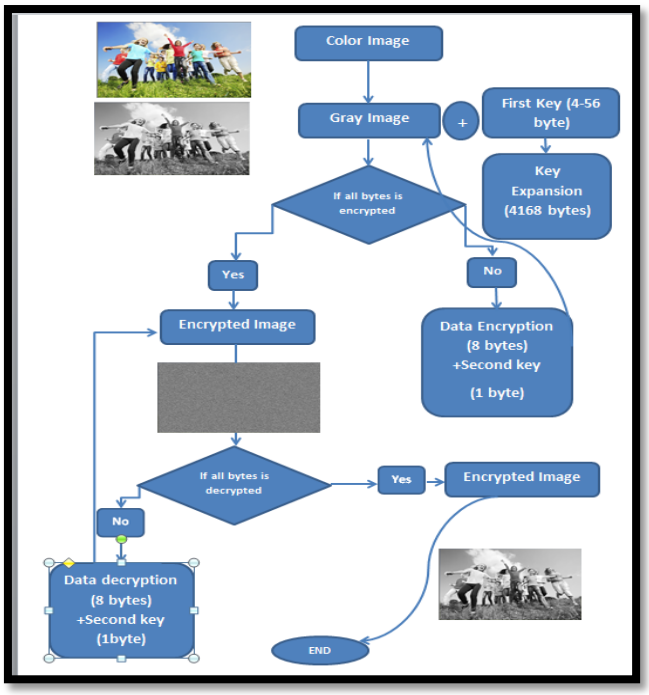

Figure 5- The proposed modification of the Blowfish encryption algorithm.

Experimental results and discussions

The proposed system has been established using Visual Basic.NET programming language, Windows 7 with 64-bit operating system, Intel(R) Core(TM) i5. Three BMP files each of size(300* 300) pixels are used to test the proposed system for the encryption quality as shown in Figure- 6. The proposed modification was applied both in encryption and decryption operations, while Figure- 7, for example, shows the results of execution of the Blowfish algorithm.

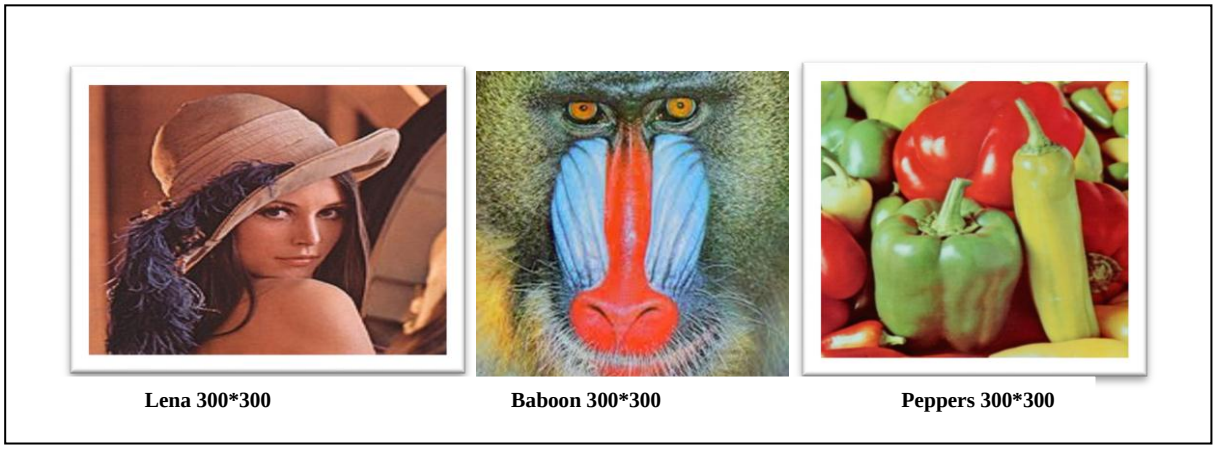

Figure 6- Three different BMP images used to test the encryption quality.

Figure 7- The output results of Blowfish algorithm.

The three encryption quality evaluation metrics were used to test the proposed modification algorithm for different images and various KEY2. Table-2 gives the details of KEY2 that is used to evaluate the implemented results for three criteria. The second column clarifies the different three values used in creating different two Sbox5 as explained in the previous section. While the third and fourth columns represent the second encrypted and decrypted keys and their indices in row and column respectively.

Table 2- Two KEY2 values from different Sbox5 and their initial values

Index	Three initial keys to create Sbox5	Encryption KEY_2 Value In Hex	Decryption KEY_2^{-1} Value In Hex
1-	Value1=0x4C	Row=0x0E Clo.=0x07	Row=0x0A Clo.= 0x09
	Value2=0xC1	0xA9	0x E7
	$x^8 + x^4 + x^3 + x + 1$		
2-	Value1=0x85	Row=0x06 Col.= 0x03	Row=0x0C Col.= 0x05
	Value2=0x45	C5	63
	$x^8 + x^6 + x^5 + x^2 + 1$		

Table- 3 presents the results using three images, two different KEY2 were selected randomly from two created Sbox5 in the proposed modified Blowfish algorithm. The details of each encrypted key were explained in Table-1. The correlation in encryption operation is considered better if the value closed to zero. The reduction value represents the obtained decrease ratio improvement when implementing the modified algorithm. It has been noticed that the correlation value obtained from the modified algorithm is less compared to Blowfish algorithm. The percentage improvement (Reduction) value is computed as in Equation 12, the original is the correlation value of the Blowfish algorithm while the new value is the correlation of the modified algorithm.

$$Reduction = \frac{original\ value - new\ value}{new\ value} * 100 \quad (12)$$

Table 3- Correlation values comparisons between the two algorithms.

Image file name	Blowfish	Modified Blowfish			
		First KEY2		Second KEY2	
		0xA9	Reduction	0xC5	Reduction%
Lena	0.0114	0.0073	36%	0.0099	13%
Baboon	0.0118	0.0091	23%	0.00643	46%
Peppers	0.0094	0.0045	52%	0.0076	19%

Table- 4 illustrate the MSE results of different images for both operations using different KEY2. In encryption operation, the largest MSE values lead to better encryption process. By comparing the results of the Blowfish and the modified algorithms, it has been observed that MSE increases when using the latest one. In decryption operation, this measurement represents the quality of the retrieval image in which lower value leads to the smallest error rate in the decrypted image. Also by comparing the results between the two algorithms, the MSE is decreased in the modified algorithm which is considered an improvement.

Table 4- Mean Square Error (MSE) in Encryption/Decryption operations.

Image file name	Modified Blowfish / Encryption			Modified Blowfish / Decryption		
	Blowfish	KEY2		Blowfish	KEY2	
		0xA9	0xC5		0xA9	0xC5
Lena	8593.52	8673.46	8594.96	157.737	150.917	34.325
Baboon	7142.71	7184.73	7164.40	112.359	107.509	24.452
Peppers	7876.53	7940.97	7879.82	112.359	107.509	24.452

The number of pixels change rate (NPCR) is considered good if this measurement value is high. Table-5 shows compassion between the two algorithms for NPCR values. From this table, it can be noticed that this value is increased when implementing the modified algorithm in the encryption process. While in decryption process, this metric is considered best if the obtained values are small. Thus, the results in modified algorithm are considered to be the best.

Table 5- The number of pixels change rate in Encryption/ Decryption operations.

Image file name	Modified Blowfish/ Encryption			Modified Blowfish/ Decryption		
	Blowfish	KEY2		Blowfish	KEY2	
		0xA9	0xC5		0xA9	0xC5
Lena	99.5943	99.6477	99.7064	0.4695	0.4522	0.4523
Baboon	99.5966	99.6383	99.62592	0.33442	0.3153	0.3143
Peppers	99.5966	99.6360	99.6202	0.33440	0.31534	0.3053

Conclusions

This paper suggests a new modification of the Blowfish algorithm to improve the security level using two keys in encryption operations, this will lead to increase the complexity level in modified algorithm. The aforementioned enhancement made the new suggested approach safe against unauthorized attack, instead of using a single key in cipher operation, another key of one byte length was used in the proposed algorithm. This modification has taken place in the Feistel function, where the second key has a length of 8-bit. The proposed modified Blowfish algorithm uses five Sboxes instead of four; the additional key is selected randomly from additional Sbox5 depends on its row and column indexes. Several criteria such as correlation, number of pixels change rate and mean square error (MSE) are used to evaluate both algorithms. The obtained results of the proposed algorithm were better compared to the Blowfish algorithm.

References

1- Ali , M. Nada .**2015.** An Improved AES Encryption of Audio Wave Files. Ph.D. Thesis submitted to the University of Technology, Baghdad, Iraq.

2- Rajender, K., Balwinder S. and Satish K. , **2014**, "A Novel Approach to Blowfish Encryption Algorithm. *International Journal of Advance Foundation and Research in Science & Engineering*, 1(2), pp: 26-34.

3- NIST .**2001.** *Advanced Encryption Standard (AES)*. Federal Information Processing Standards Publication (FIPS PUB) 197.

4- Stallings W. **2011**.*Network Security Essentials, Applications and Standards*. Fourth edition, Pearson Education, Inc., 417P.

5- Al-Hamami, A., Al-Hamami, M. and Hassan, S. **2006.** A Proposed Modifications To Improve the Performance of Blowfish Cryptography Algorithms. First National Information Technology Symposium (Nits 2006) , Bridging The Digital Divide: Challenge And Solutions, King Saud University, Riyadh, Kingdom Of Saudi Arabia.

6- Al-Neaimi, A. and Hassan, R. **2011**. New Approach for Modifying Blowfish Algorithm by Using Multiple Keys. *International Journal of Computer Science and Network Security*, 11(3), pp: 21-26.

7- Tahseen, I. and Habeeb, S. **2012**. Proposal New Approach for Blowfish Algorithm by Using Random Key Generator. *Journal of Madent Alelem College*, 4(1), pp: 1-10.

8- Christina, L. and Joe, Irudayaraj V. S. **2014**. Optimized Blowfish Encryption Technique. *International Journal of Innovative Research in Computer and Communication Engineering* , 2, (7), pp: 5009-5015.

9- Radhadevi, P. and Kalpana, P. **2012**. Secure Image Encryption using AES. *International Journal of Research in Engineering and Technology*, 1(2), pp: 15-117 .

10- Agrawal, M. and Mishra, P. **2012.** A Modified Approach for symmetric Key Cryptography Based on Blowfish Algorithm. *International Journal of Engineering and Advanced Technology (IJEAT)*, 1(6).

11- Sctmeier, B. **1994**. *Description of a new variable-length key, 64-Bit block cipher(Blowfish)*[J].Lecture Notes in computer Science, 809:191-204.

12- Ali, M., Nada, Rahma, A.M. and Jamil, A. **2015**. Text Hiding in Color Images Using the Secret Key Transformation Function in GF (2^n). *Iraqi Journal of Science*, 56(4B), 3240-3245.

13- Gonzalez, R. and Woods, R. **2008**. *Digital Image Processing*. 3rd edition, Pearson Education.

14- Mahalakshmi, J. and Kuppusamy, K. **2016**. An efficient Image Encryption Method based on Improved Cipher Block Chaining in Cloud Computing as a Security Service. *Australian Journal of Basic and Applied Sciences*, 10(2), 297-306.

15- Kumar M. and Chahal A. **2014**. Effect of Encryption Technique and Size of Image on correlation Coefficient in Encrypted Image. *International Journal of Computer Applications*, 97(12), pp: 23-27.

16- Alzubaidi1, A. and Al-Shakarchy N. **2014**. Color Image Encryption and Decryption Based Pixel Shuffling with 3D Blowfish Algorithm. *International Journal of Science and Research (IJSR),* 3(7), pp: 336-343.

17- Saeed, M. and Mian, M. **2008**. Methods of finding multiplicative inverses in GF (2^8). *Computer Communications,* 31(17), pp: 4117-4123.