Al-Rafidain Journal of Computer Sciences and Mathematics (RJCM)

www.csmj.mosuljournals.com

BLOCK CIPHER PERFORMANCE AND RISK ANALYSIS

Amina khaled Alregabo[1], * Yaseen Hikmat[2]

The General Directorate of Education in Nineveh Governorate, Mosul, Iraq [1],
Department of Computer Science, College of computer science and mathematics, Mosul University, Mosul, Iraq [2]

Article information

Article history:
Received :30/6/2022
Accepted :13/11/2022
Available online:

Abstract

Block cipher algorithms are a very important issue in the field of information security. Their simple structure and software-based encryption allow users to implement them in several applications such as: data security and cloud computing. In this paper, we reviewed 8 block ciphers that had been presented in the recently five years and were used in different applications. The 8 block ciphers are: DES, 3DES, Blowfish, Twofish, PRISENT, KLEIN, IDEA and AES. All of them are symmetric block ciphers with different designs. The comparative results showed that the block ciphers can still be used in different applications and fields. They showed that many modifications had been presented in which, chaotic maps had been implemented in key generation to enhance the robustness of the block ciphers and its randomness. The comparative results also showed that the AES is one of the block ciphers that is still unbroken algorithm and still modified to suit other new applications. Since less robust ciphers have continuous modification and enhancement in order to be more robust against some of probable attacks, the length of the key and its complexity and the structure of the ciphers are essential directions for improving block ciphers.

Keywords:
Data Encryption, Cryptography, Block Cipher, Performance Analysis.

Correspondence:
Author: Amina Khaled Alregabo
Email:amina.20csp64@student.uomosul.edu.iq

I. INTRODUCTION

Today, we live in the era of information technology and the wide widespread of network and Internet applications, where the process of exchanging information has become easy to use for everyone. As a result, it is necessary to implement an effective and efficient method to protect our data transmitted over the network, and thus prevent unauthorized persons from accessing them [1].

Several cipher systems had been invented and developed to enhance the security level of networks and applications. Block ciphers as important encryption systems were implemented to achieve data security. Many algorithms had been developed based on the main principles of Block Ciphers. In those algorithms, many thoughts and modifications had been presented and improved to reach higher performance and robustness [2]. Thus, the performance analysis most be performed to evaluate their performances. The analysis allows the researcher to develop the weakness of the previous algorithms against the attacks and to build new robust algorithms [3]. Among these algorithms is the block ciphers which have the most important role in many network applications. Many algorithms of block ciphers had been presented to increase their performance level and to strengthen their potentials against any attack.

Data encryption as a security solution converts plain data into encrypted data in the encryption or ciphering phase. On the other hand, the reverse process is called decryption or deciphering which converts the encrypted data into plain ones. The ciphering algorithms usually aim to retrieve the original data after decryption phase without loss. Other important issue is the robustness of these algorithms against deferent types of attacks. This would secure transmitted data via any communication method [4].

The encryption system consists of three main categories: Symmetric Keys which contain a single Secret Key, and Asymmetric keys which contain two keys, Public Key that is used to encrypt plain data and Private Key that is used to decrypt encrypted data. The third category is protocols that secure data transmission. The Symmetric Keys algorithms are divided into two categories: Stream cipher which encrypts/decrypts the whole data and Block Cipher which encrypts/decrypts blocks of the data in each step [5]. Fig.1 illustrates the classification of encryption system.

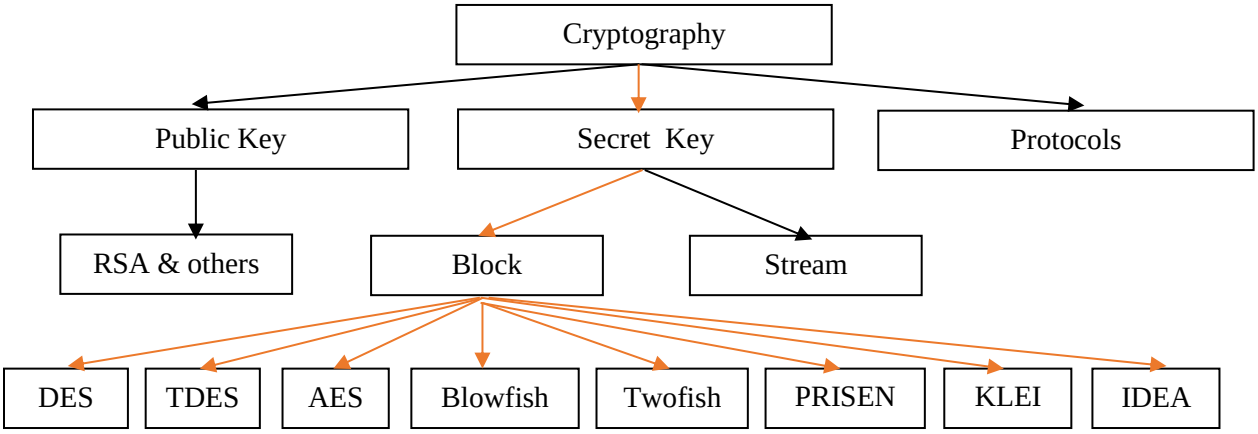


Fig.1: Classification of Encryption system [5].

II. CONCEPTS OF BLOCK CIPHER

There are common concepts that had been recognized in all Block Ciphers. These concepts are implemented in the design to perform encryption and decryption processes. They are:

a. Iteration

One of the most common concepts is the iteration of the block cipher. The steps of the algorithms are repeated for a number of iterations. The block of the plan-text is encrypted via several invertible transformations. The iterations are known as Rounds. The Round Function R produces a key that usually would be used in the next round [6].

b. Substitution box (S-box)

The S-box substitutes a block of the plain bits with a block of encrypted bits. The substitution process has to be one-to-one in order to invert the process (Decryption). In a given secure S-box, changing one bit of the input would change 50% of the output. This property is called The Avalanche Effect. This means that the output bit depends on all the input block. The design of algorithm may use one or more S. boxes; either in the same or on nested rounds. They also may be used in parallel [7].

c. Permutation box (P-box)

The P-box permutates all the bits. The bits of the plain data would be permutated to form the encrypted data. In modern block cipher, the output's bits of S-boxes for a round would be permuted and would be fed to the next S-boxes at the next round. As P-box can manipulate with output of S-boxes, it is a good property to cover all the output, then permutated them and fed them again [8].

d. Substitution–Permutation Network (SPN)

SPN is a network of S-boxes and P-boxes which were arranged to perform an encryption in a block cipher. SPN ciphers are important type of iterated block cipher. SPN cipher encrypts a block of the plain data by the key and several rounds. Each round consists of a substitution stage followed by a permutation stage. At the final round, the encrypted data would be produced [9].

III. IMPROVEMENT OF BLOCK CIPHER ALGORITHMS

In this section, the most important block cipher algorithms would be illustrated that the researchers had proposed their studies to improve their performance.

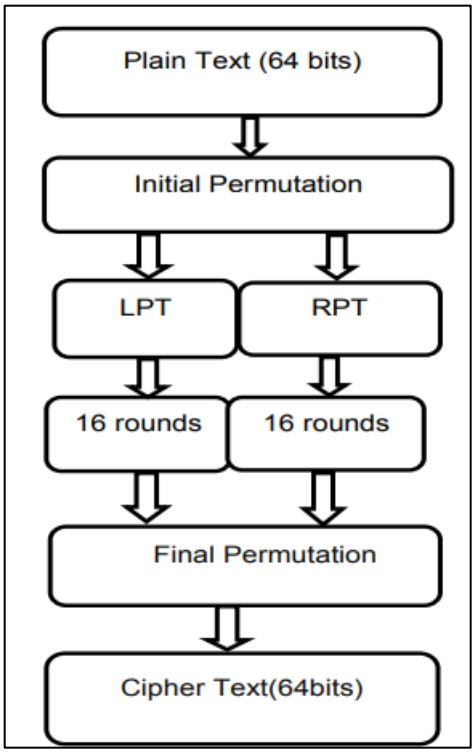
a) The Data Encryption Standard (DES)

The DES had been presented since 1975 and

standardized by IBM in 1977. Then, it was broadcasted by the National Institute of Standards and Technology (NIST) [10]. DES Algorithm has a number of steps that are called (Round Algorithm) as shown in Fig.2. The following are the steps of this algorithm:

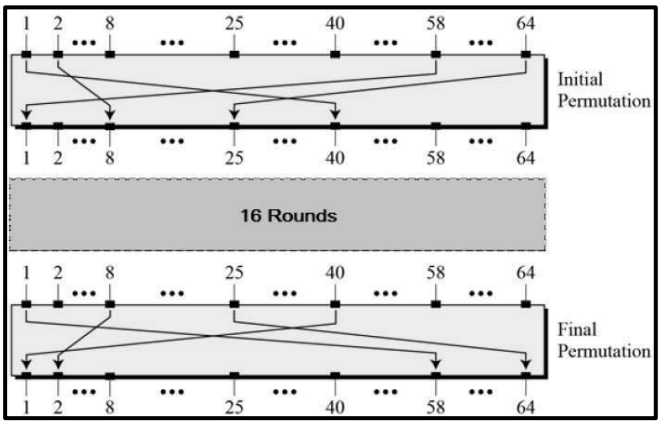
1. In the beginning step, 64-bit block of plain text initially went through Initial Permutation.
2. The initial permutation is performed for the given plain text.
3. Permutation yield permuted blocks consist of 2 parts: Left and Right plain texts.
4. Then, the right part is shifted and left part goes through encryption steps in 16 rounds. Each round has its own key:

- Key transformation used different 48-bit sub-key is generated from the 56-bit key.
- Expansion permutation is implemented, the 32-bit right part is enlarged to 48-bits.
- The 32-bits are permuted by P-box permutation.
- The output of 32-bits P-box is XORed with the 32-bits left part.
- The XORed output of 32-bits turns out to be the new Right part and the older Right part turns to be Left part. This processing is known as swapping.
- Again, Right plain text applied to next round and more than 15 rounds are performed.
- At the end of the 16 rounds, the final permutation is performed [11].



a. DES Structure

Several works had been recently presented as a modification of DES. The following are some of those works.



b. DES Rounds

Fig.2: DES Algorithm [12].

In [13], the authors presented a new model of DES based on higher entropy in image encryption. The implementation of entropy increased the strength of the standard DES and reduced the risk of system broken. It also supposed to override the shortcomings of high complexity of the standard DES. SHA-256 algorithm and Logistic map had been used to generate a 256-bit key. The results showed that the proposed algorithm had been enhanced; its security was verified by the analysation of the information entropy, image correlation. The proposed algorithm passed both noise attack and occlusion attack tests. As a result, it may resist common attacks.

In [14], the authors proposed an enhanced DES used f-function and incorporating striding technique in addition to the XOR operation between sub keys and the plaintext. The results showed that the enhanced DES gain 55% of average of avalanche effect comparing with standard DES. It is resistant to known exhaustive and cryptanalysis attacks.

In [15], the authors presented an enhanced key DES. The enhancement is based on premutation of the odd and even bits of the key to generate more complex keys during the 16 rounds. It supposed to be more robust against attacks especially short key attack because it enhanced key generation.

In [16], the authors presented an improved DES based on increasing Key length to 128-bit. It consists of two parallel implementations of the standard DES with permutations. The 128-bit key is divided into two subkeys to be used on each DES 16 rounds. The result showed that the improved DES is faster more efficient than 3DES.

b) Blowfish

Schneier invented Blowfish algorithm in 1993. It was implemented in several encryption domains and ciphers. Blowfish encrypts 64-bits as a block size and 32-448 bits key length. It was a promising alternative to DES. It suits to be used in hardware applications [11]. Fig.3 illustrates this algorithm.

In [18], the authors presented a hybrid encryption system based on Blowfish algorithm with 3D Henon and Chen chaotic maps. This system was implemented to encrypt and decrypt transmitted satellite images and other images transmission. The results showed that the proposed system is efficient with large images. It also showed that it has a good robustness according to performance analysis.

In [19], the author presented a modified Blowfish encryption algorithm to secure the user's data in the cloud. It is based on clustering the user's data that are stored in the cloud into groups of similar measures. A 448-bit key is generated by the Blowfish key generator with Xor operations in 16 rounds. The clustered data are encrypted by Blowfish in a modified procedure to gain encrypted text. Indeed, S-boxes had been effectively implemented in this algorithm. The results showed that the proposed algorithm has better performance than the standard Blowfish, RSA and AES.

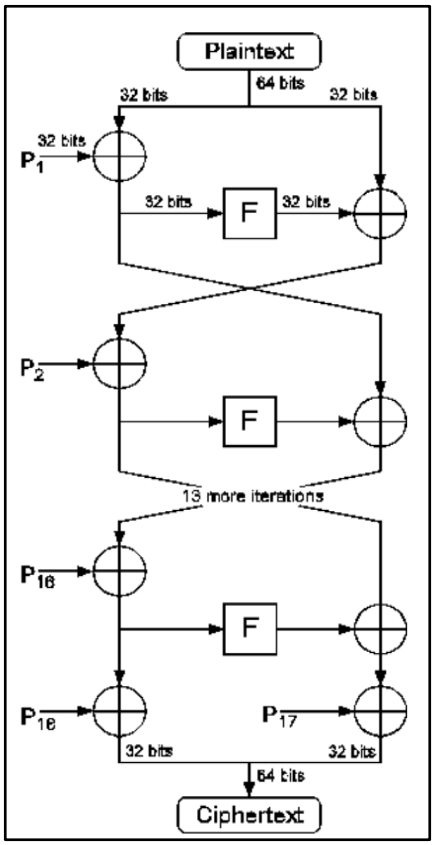


Fig.3: Blowfish Algorithm [17].

In [20], the authors presented a modified blowfish algorithm that based on increasing both block size and key length. The block size was increased to 128bit and the key length was increased to 128bit too. The structure of the standard Blowfish was re-designed to maintain the new block size and key length. The algorithm implements a F function to generate key. The results showed that the modified Blowfish has better security than standard Blowfish but it is slower.

In [21], the authors presented a modified Blowfish based on Quadratic map in image encryption. The modification allows to implement the Blowfish in image encryption by overriding the big size problems. The plain image is divided into 8 areas. Then, Quadratic map is performed for each area. The input key of Blowfish (64bit) would be selected from the 8 areas. The results showed that the modified Blowfish is better in security and in performance than traditional Blowfish.

c) Triple DES (3DES) or (TDES)

DES Algorithm had been derived from standard DES in 1995. It is three times DES ciphering for each block of plain data. It has 64 bits block sizes and 56, 112 or 168bits as a key size. The encryption process (Fig.4) can be performed according to the following major steps:

1. DES algorithm encrypts the plain data primary key K1.
2. Next, DES decrypts the output of step1 by secondary key K2.
3. Finally, DES algorithm encrypts the output of secondary key by third key [11].

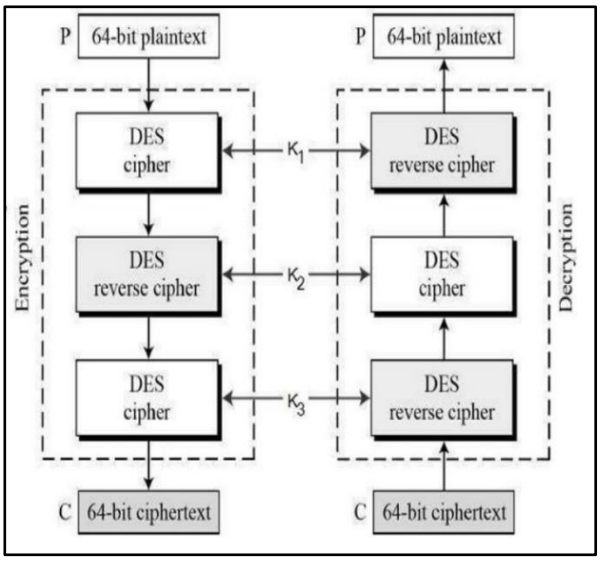


Fig.4: 3DES Algorithm [22].

In [23], the authors presented a modified 3DES based on chaotic maps. This implementation had been performed by using three all-pole IIR filters to 16 characters (128-bit) to generate the key sequence of 3DES in 16 rounds. The results showed that using all-pole IIR filters can increase the performance speed with the small complexity algorithm.

In [24], the authors developed 3DES algorithm. They re-designed the structure of the three nested DESs to be parallels. Thus, three keys were used in the same time to produce the ciphered text. A generation key kernel is used to generate three (16-bits) subkeys in 16 rounds that results a (48-bits) key. The results showed that the proposed algorithm is faster three times than the traditional 3DES.

In [25], the authors implemented the genetic algorithm in key generation process in 3DES algorithm. The proposed algorithm is supposed to have more complex key by the property of genetic algorithm. The result showed that the proposed algorithm is more robust than the traditional 3DES.

In [26], the authors proposed a system to secure network by encrypting messages then to apply a fuzzy model to the encrypted messages. 3DES as an encryption algorithm is used to encrypt the plain message. The output (encrypted message) is an input to the Takagi-Sugeno (T-S) Fuzzy Model. The results showed that the fuzzy model applied more complexity to the encrypted messages.

d) PRESENT

In 2007, Orange Labs had developed PRESENT algorithm at technical university of Denmark and Ruhr University Bochum. This algorithm has a 64-bit block size, light-weight type and a varied key length (80 and 128) bits. This algorithm is used in high efficiency chip and low power consumption [11]. Fig.5 illustrates the steps of this algorithm.

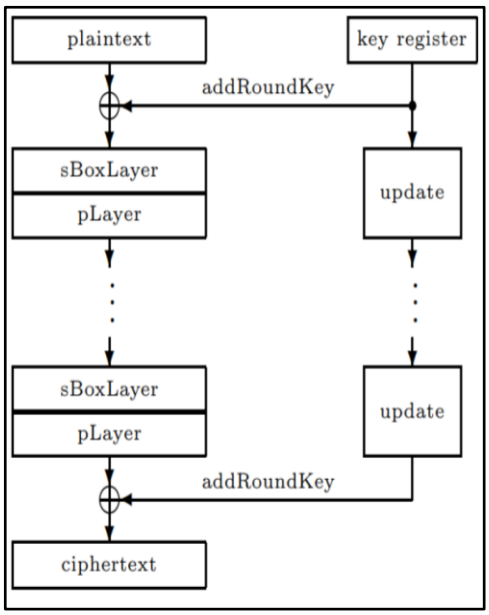


Fig.5: PRESENT Algorithm [27].

In [28], the authors proposed a modified S.box structure for the PRESENT block cipher. The proposed cipher had the same block size of 64-bytes, and the same key length. In fact, the structure of the S.boxes had been modified to reduce the number of rounds. The proposed cipher divided the block into 4x2 and this would decrease the number of S.boxes to 8 and the required rounds to 16 rounds.

In [29], the authors proposed a dynamic key PRESENT cipher in which the key had been rotated in varied sequence and permutate the values of the key bits. So, the generated key had been rotated for 61times till be used. Only, one of the keys in the array of keys would be used in each round. S.box had been used with the selected key during each round too. The results showed that the proposed cipher had better performance than the original cipher.

In [30], the authors presented an optimal quantum circuit based on symmetric key cryptography by an optimized PRESENT and GIFT block ciphers. The proposed design aimed to minimize qubits, quantum gates, and circuit depth. The results showed that the proposed optimization of those two ciphers had been compared with other ciphers. The results showed that the implementation of both ciphers together minimized the number qubits, quantum gates, and circuit depth. It also strengthens the proposed cipher against Brut force attack and Quantum attack.

e) KLEIN

Klein is a block cipher that is used in compact hardware to achieve a high performance based on software. It was presented by Gong et al, in 2011[31]. It has 64-bit block of plain data and 64,80, and 96-bit keys. The key length variation may increase the randomness of the KLEIN cipher. In fact, the KLEIN cipher is based on SPN structure to perform both substitution and permutation as known in other block ciphers. A KLEIN encryption process can be described as follows [31]:

- $SK^1 \leftarrow KEY$
- State ← Plaintext
- For i =1 to NR do
- Add Round Key (State, Sk^i);
- Sub Nibbles (State);
- Rotate Nibbles (State);
- Mix Nibbles (State);
- Sk^{i+1} = Key Schedule (SK^i, i);
- end for
- Ciphertext Add Round Key (State, SK^{NR+1});

The structure of KLEIN algorithm is shown in Fig.7.

In [32], the authors proposed an optimized KLEIN cipher. Their proposal is based on the original KLEIN SPN structure but it implemented 3 layers of S-box after performing original algorithm. In those three layers of S-box, a 4-bit permutation is applied to 16 nibbles steps after Rotate Nibble Algorithm. The initial state is XOR 'd with key once before each of the three layers of S-boxes. 3-layer S-box enhanced the software

capabilities that perform in high quality level.

In [33], the author proposed an enhanced algorithm of KLEIN block cipher. This algorithm is similar to the original algorithm with one modified step. The (MixNibble) step had been replaced with 3-stage S-box of four bytes. The optimized algorithm showed higher performance than the original one, with low time and memory usage. The optimized algorithm is suitable to be used in low hardware devices.

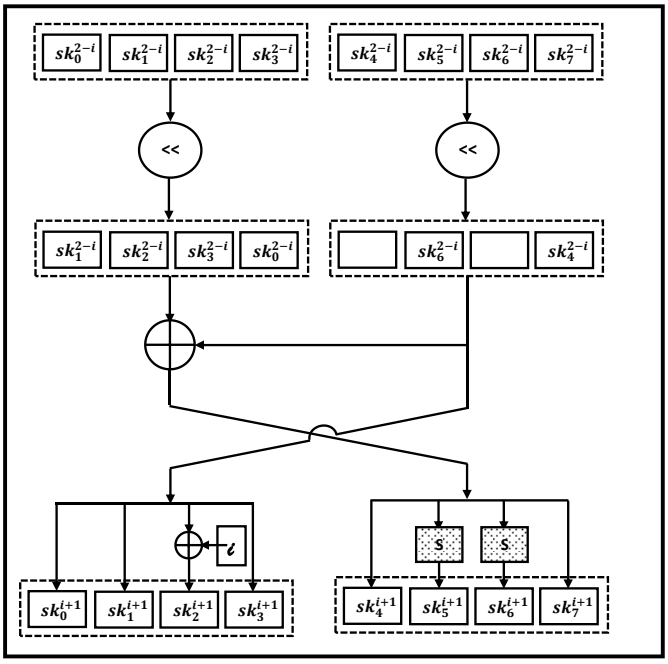


Fig.7: KLEIN cipher structure[31].

f) Twofish

Twofish is an improved block cipher. It has 128-bits as block size combined with a key. It has three variable keys of 128, 192, and 256-bits. Twofish is based on the Feistel network with 16 rounds. Plaintext is broken into four blocks (W0, W1, W2, and W3) of 32-bit. Each word is Xored with four words (K0, K1, K2, and K3) of 32 bits as an input in whitening process. The outputs of whitening passes into the F directive function which consists of five operations based on four dependent keys and four S-boxes with an 8-bit input. The output followed by a mathematical code called a fixed maximum distance separable (MDS) matrix. The pseudo-Hadamard transform is a straight forward 32-bit mixing operation with an addition mode of 232. After the 16th round, Twofish performs output whitening. Fig.8 shows the structure of Twofish algorithm [34].

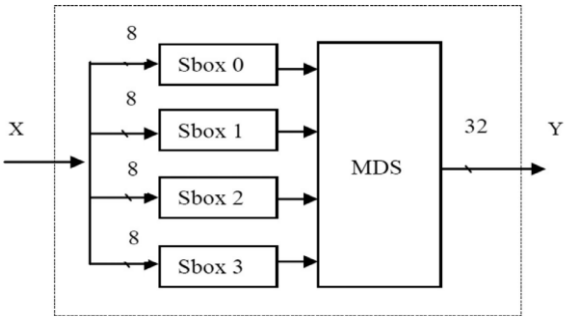


Fig.8: Twofish Algorithm [35].

In[35], the authors presented a modified Twofish algorithm in image encryption. The modification was to replace the XOR operation of each round with a (#) operation by dynamic block sizes and multi-state tables. This modification allows more complexity and fast retrieving of plain text.

In [36], the authors presented a modified TWOFISH algorithm in image encryption. They add more mathematical complexity via S-boxes drawn from a multiplicative group of units of chain ring $\sum_{i=0}^{7} u^i F_2$ .Those S-Boxes add more algebraic complexity to the Twofish.

g) International Data Encryption Algorithm (IDEA)

IDEA is a block cipher with 64-bit block size and 128-bit key. The 64-bit block is divided into four 16-bit sub-blocks. Those sub-blocks go through 8 rounds with repeated sequences of operations. Each round output is an input for the next round. Indeed, the system needs six unique keys, that are generated from the 128- bit original key. The output of the 8th round is an input to output transformation phase that consists of arithmetic operations with four keys. The output transformation phase produces the final cipher key. The entire encryption requires 52 keys. Fig.9 illustrates that [37].

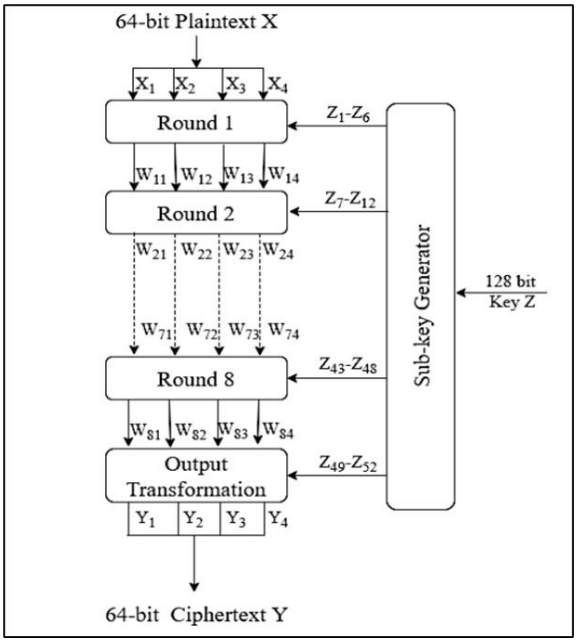


Fig.9: IDEA Algorithm [38].

h) AES

Advanced Encryption Standard (AES) is a block cipher that had been adopted in October 2000 by the National Standards and Technology (NIST) as a substitution for DES. The structure of AES is based on the round transformation that consisted of three distinct invertible uniform transformations, known as layers that simulate the Wide Trail Strategy. This structure strengthens the AES against linear and differential cryptanalysis. Three functions are represented in the three layers: The linear mixing layer provides high diffusion during rounds; The nonlinear layer consisted of S-boxes that have optimum worst-case nonlinearity properties. Finally, there the key addition layer. Although this algorithm has not broken yet but there are some studies that try to enhance its performance. AES has 128, 192 or 256 key length and 10 to 14 rounds. It has 128-bit block size distributed on its four arrays [40].

Compute subkeys K_0, K_1, ..., K_n from the key K

1- $S=B \oplus K_0$
2- For i = 1 to nr – 1
   3.1 S = ByteSub(S)
   3.2 S = ShiftRow(S)
   3.3 S = MixColumn(S)
   3.4 $s = K_i \oplus S$
3- S = ByteSub(S)
4- S = ShiftRow(S)
5- $S = K \oplus S$

Fig.10 illustrates the structure of AES algorithm

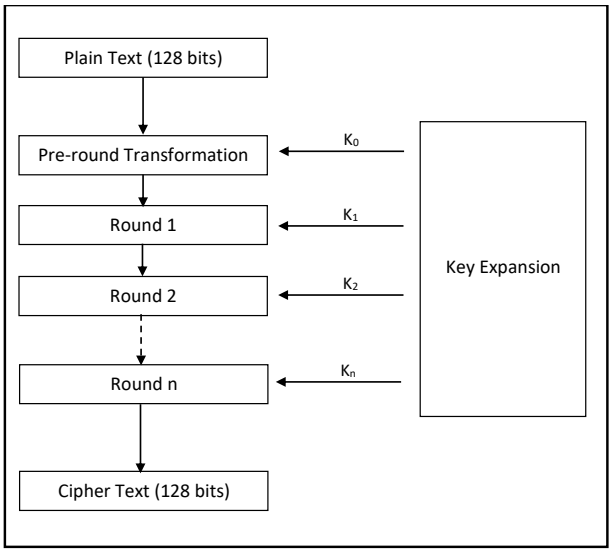


Fig.10: The structure of AES Algorithm [40].

In [41], the authors presented an enhancement to the original AES by adding 3 rounds of randomization to the initial key before encryption process. This modification has been implemented to secure data in cloud computing.

In [42], the authors presented an enhancement to encrypt images as a heavy load by AES in parallel encryption mode. This enhancement allows to implement the GPU to generate four tables known as T-table for image data that stored in shared memory. Thus, the memory access time has been reduced.

IV Comparison and Discussion

The block cipher algorithm had several properties and features that can be compared in addition to their performance. Table.1 showed some of these features that allow to determine which of these algorithms is better to be implemented or it may enhance.

It is obvious that AES algorithm still unbroken, but other algorithms with long key are difficult to be broken too. Some of researchers had modified weak algorithm to be strong as shown in Table 1.

Table.1: The comparison among the previous presented modification of the block cipher algorithms.

Ref. No.	Original algorithm	Block Size(bits)	Key length(bits)	Modification	Rounds Number	Advantages
14	DES	64	256bit	-Entropy -SHA256 -Logistic map	16	-Resist statistical attacks
15	DES	64	64bit	-F function -Incorporating striding techniques	16	-Resist brute force. -Resist cryptanalysis attack
16	DES	64	64	-Enhanced Key generation. -K-D function.	16	-just more robust than DES
17	DES	64	128	-increasing key length -implementation of two DES	16	-Faster than 3DES
19	Blowfish	64	64-384	-Henon map. -Chen chaotic map	2	-Gives good encryption Strength
20	Blowfish	64	448bit	-K-medoid clustering method -F function	16	-better performance than standard Blowfish, RSA and AES
21	Blowfish	128	128	-Increase Block size -increase key legth -F function	8	-better robustness than standard Blowfish - Slower -better performance than stand and Blowfish but faster than Twofish
22	Blowfish	64	64-384	-Entropy - Quadratic map	16	-Better security and performance than traditional Blowfish.
24	3DES	64	128	all-pole IIR filter	16	-Better performance than traditional 3DES -small additional complexity
25	3DES	64	48	Key generation Kernel.	16	Three times faster than traditional 3DES
26	3DES	64	64	Genetic algorithm	N-rounds	More robust than 3DES
27	3DES	64	64	Takagi-Sugeno (T-S)	16	More complex encrypted message
29	PRISENT	64	80 or 128	Quantum Circuit Logic gates SPN	16	- Minimize qubits, quantum gates, and circuit depth. - Robust against Brut force attack and Quantum attack
30	PRISENT	64	80 or 128	Dynamic Key Selected from Key array. SPN	16	
31	PRISENT	64	80 or 128	SPN	16	- reduced number of S.boxes and the number of rounds
33	KLEIN	64	64, 80, 96	SPN	64	Enhance the software-based cipher
34	KLEIN	64	64, 80, 96	SPN 3 Stage S.box.	12,16, 20 and 32	Enhance the software-based cipher
36	Twofish	128bit	128, 192, and 256-bits	S-boxes Directive function # operation	16	Increase complexity
37	Twofish	128bit	128, 192, and 256-bits	Mathematical complex operation with 4 keys	16	Increase complexity
39	IDEA	64	128-bit	Algebraic operations S-boxes	8	Increase complexity
40	IDEA	64	128-bit	Sub keys	10	Increase complexity
42	AES	128-bit	128, 192 or 256	3 randomization rounds for key	10 or 14	More randomness
43	AES	128-bit	128, 192 or 256	Four table of data Parallel encryption	10 or 14	Reduce access time to memory Encrypt big data

Most of the reviewed ciphers have 64-bit block size except Twofish and AES. Both ciphers have 128-bit of block size. The larger block gives more robustness for the cipher against cryptanalysis and attacks. The rest have smaller size but some of them had been modified to reduce the vulnerabilities of the probable attacks.

The length of the secret key is varied among the studied ciphers between 48 to 384 bits. This variation is associated to the modification of most of the studied ciphers. Increasing length of the key overrides the short key

problem. Thus, the authors increased the length of their proposed cipher for this reason. Thus, the robust ciphers are enhanced by increasing the key length because it adds more complexity in cryptanalysis and increases its time.

Most of the studied ciphers had been modified by adding either chaotic maps, Entropy, SHA256, clustering, or other functions and mathematical operations. Other strategies like modified SPN must be increase key length. It is obvious that the authors had discussed several matters related with robustness of their presented attacks.

The number of rounds is an important feature of the design of block ciphers. Most of the studied ciphers had 16 rounds. But some of the ciphers had less than 16 rounds as a try to reduce the required rounds in high performance condition such as Blowfish and IDEA ciphers. Thus, in some other ciphers, the number of rounds had been increased as an enhancement strategy of the cipher robustness such as KLEIN. While in the proposed cipher 3DES, the number of rounds was variable that can be selected according to condition of the ciphered text.

For most of the studied ciphers, execution time that is required for encryption or decryption was not mentioned. Thus, time measure was excluded from comparison in this study.

V. Conclusion

The block ciphers are a type of symmetric key encryption that has several types of algorithms. They have deferent performance, complexity and randomness. AES is one of the robust algorithms that had not broken yet. Some others are robust but may be broken either for its short keys or by applying some types of attacks.

The recently proposed block ciphers showed the capability of improving the known algorithms to add more complexity and robustness via increasing the length of keys or modifying the structure of the cipher. More function and operations can be used and other additional techniques. Some of the proposed ciphers implemented chaotic map as solution for the randomness of the secret key.

In the future, the time must be considered for the proposed ciphers. It is important to determine the performance of the block ciphers and to define the faster one specially for communications.

Acknowledgment

The authors would like to express their gratitude to the Department of Computer Science, the University of Mosul for their support that led to the successful accomplishment of this study.

References

[1] Hussain, S., Jamal, S. S., Shah, T., & Hussain, I. (2020). A power associative loop structure for the construction of non-linear components of block cipher. IEEE Access, 8, 123492-123506.

[2] Shetty, V. S., R., A., M. J., D. K., & Hegde N., P. (2020). A Survey on Performance Analysis of Block Cipher Algorithms. 2020 International Conference on Inventive Computation Technologies (ICICT).

[3] Ali, K. M., & Khan, M. (2019). A new construction of confusion component of block ciphers. Multimedia Tools and Applications. doi:10.1007/s11042-019-07866-w.

[4] Hendi, A. Y., Dwairi, M. O., Al-Qadi, Z. A., & Soliman, M. S. (2019). A novel simple and highly secure method for data encryption-decryption. International Journal of Communication Networks and Information Security, 11(1), 232-238.

[5] Ramesh, G., & Umarani, R. (2012). Performance analysis of most common encryption algorithms on different web browsers. International Journal of Information Technology and Computer Science, 4(12), 60-66.

[6] Junod P. & Canteaut A. (2011) Advanced Linear Cryptanalysis of Block and Stream Ciphers, Cryptology and information security series 7ed, IOS Press.

[7] Cusick, Pantelimon Stanica (2009). Cryptographic Boolean Functions and Applications

[8] Katz J. & Lindell Y. (2008). Introduction to modern cryptography. CRC Press.

[9] Keliher, L., Meijer, H., & Tavares, S. (1999, August). Modeling linear characteristics of substitution-permutation networks. In International Workshop on Selected Areas in Cryptography (pp. 78-91). Springer, Berlin, Heidelberg.

[10] Shetty, V. S., Anusha, R., MJ, D. K., & Hegde, P. (2020, February). A survey on performance analysis of block cipher algorithms. In 2020 International Conference on Inventive Computation Technologies (ICICT) (pp. 167-174). IEEE.

[11] S. Singh , Sunil Maakar , Kumar, "Enhancing the security of des algorithm using transposition cryptography techniques", International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE). Volume3, Issue 6, june 2013.

[12] Gunjan Gupta, Rama Chawla, "Review on Encryption Ciphers of Cryptography in Network Security", Review on Encryption Ciphers of Cryptography in Network Security. Volume 2, Issue 7, July 2012.

[13] Zhang, X., Wang, L., Cui, G., & Niu, Y. (2019). Entropy-based block scrambling image encryption using DES structure and chaotic systems. International Journal of Optics, 2019.

[14] Amorado, R. V., Sison, A. M., & Medina, R. P. (2019). Enhanced Data Encryption Standard (DES) Algorithm based on Filtering and Striding Techniques. Proceedings of the 2019 2nd International Conference on Information Science and Systems - ICISS 2019.

[15] Reyad, O., Mansour, H. M., Heshmat, M., & Zanaty, E. A. (2021). Key-Based Enhancement of Data Encryption Standard For Text Security. 2021 National Computing Colleges Conference (NCCC).

[16] Yihan, W., & Yongzhen, L. (2021). Improved Design of DES Algorithm Based on Symmetric Encryption Algorithm. 2021 IEEE International Conference on Power Electronics, Computer Applications (ICPECA).

[17] Bruce Schneier, "The Blowfish Encryption Algorithm", Dr Dobbs Journal April 01, 1994.

[18] Abbas, S. Z., Ibrahim, H., & Khan, M. (2021). A hybrid chaotic blowfish encryption for high-resolution satellite imagery. Multimedia Tools and Applications.

[19] Hussaini, S. (2020). Cyber security in cloud using blowfish encryption. Int. J. Inf. Technol.(IJIT), 6(5).

[20] Quilala, T. F. G., Sison, A. M., & Medina, R. P. (2018). Modified blowfish algorithm. Indones. J. Electr. Eng. Comput. Sci, 11(3), 1027-1034.

[21] Jassem, A. H., Hashim, A. T., & Ali, S. A. (2019). Enhanced Blowfish Algorithm for Image Encryption Based on Chaotic Map. 2019 First International Conference of Computer and Applied Sciences (CAS).

[22] Akhil Arya., "Security Enhancement Using Triple DES Algorithm1", International Journal of Computer Science and Mobile Computing.Vol.6 Issue.4, April- 2017, pg 353- 355.

[23] Pich, R., Chivapreecha, S., & Prabnasak, J. (2018). A single, triple chaotic cryptography using chaos in digital filter and its own comparison to DES and triple DES. 2018 International Workshop on Advanced Image Technology (IWAIT).

[24] Altınok, K. F., Peker, A., & Temizel, A. (2020). Bit-level Parallelization of 3DES Encryption on GPU. arXiv preprint arXiv:2007.10752.

[25] Haithem, M., & Lateef, R. A. R. (2019). Intelligent TRIPLE DES with N Round Based on Genetic Algorithm. Iraqi Journal of Science, 2058-2066.

[26] Hsiao, F.-H., & Lin, P.-H. (2018). Applying Triple Data Encryption Algorithm to a Chaotic Systems: T-S Fuzzy Model-Based Approach. Lecture Notes in Electrical Engineering, 53–66.

[27] Andrey Bogdanov, Gregor Leander, Christof Paar and Lars Ramkilde Knudsen., "PRESENT: an ultra-lightweight block cipher", Cryptographic Hardware andEmbedded Systems- CHES 2007, 9th International Workshop, Vienna, Austria, September 10-13, 2007, Proceedings (pp.450-466).

[28] Sravya, G., et al. "Hardware lightweight design of PRESENT block cipher." Materials Today: Proceedings 33 (2020): 4880-4886.

[29] Labio, Ronniel D., and Enrique D. Festijo. "D-PRESENT: A Lightweight Block Cipher with Dynamic Key-Dependent Substitution Boxes." 2020 International Conference on Advanced Computer Science and Information Systems (ICACSIS). IEEE, 2020.

[30] Jang, Kyungbae, et al. "Efficient implementation of present and gift on quantum computers." Applied Sciences 11.11 (2021): 4776.

[31] Gong Z., Nikova S., and Law Y. W., "KLEIN: a new family of lightweight block ciphers," in International Workshop on Radio Frequency Identification: Security and Privacy Issues, 2011, pp. 1-18: Springer.

[32] Ghorashi, Seyed Ramin, Tanveer Zia, and Yinhao Jiang. "Optimisation of lightweight klein encryption algorithm with 3 s-box." 2020 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops). IEEE, 2020.

[33] Ghorashi, Seyed Ramin, et al. "Software Optimisation of Lightweight Klein Encryption in the Internet of Things." Journal of Information Security and Cybercrimes Research 4.2 (2021): 159-172.

[34] Apoorva, Yogesh Kumar. "Comparative study of different symmetric key cryptography algorithms." International Journal of Application or Innovation in Engineering & Management (IJAIEM) 2.7 (2013): 10-15.

[35] Kareem, Suhad Muhajer, and Abdul Monem S. Rahma. "A novel approach for the development of the Twofish algorithm based on multi-level key space." Journal of Information Security and Applications 50 (2020): 102410.

[36] Haq, Tanveer Ul, et al. "Improved Twofish Algorithm: A Digital Image Enciphering Application." IEEE Access 9 (2021): 76518-76530.

[37] Alenezi, Mohammed N., Haneen Alabdulrazzaq, and Nada Q. Mohammad. "Symmetric encryption algorithms: Review and evaluation study." International Journal of Communication Networks and Information Security 12.2 (2020): 256-272.

[38] Hendi, Amjad Y., et al. "A novel simple and highly secure method for data encryption-decryption." International Journal of Communication Networks and Information Security 11.1 (2019): 232-238.

[39] Prajwal, V. S., and K. V. Prema. "User defined encryption procedure for IDEA algorithm." 2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI). IEEE, 2018.

[40] Sanchez-Avila, C., and R. Sanchez-Reillol. "The Rijndael block cipher (AES proposal): a comparison with DES." Proceedings IEEE 35th Annual 2001 International Carnahan Conference on Security Technology (Cat. No. 01CH37186). IEEE, 2001.

[41] Adnan, Nur Afifah Nadzirah, and Suriyani Ariffin. "Big data security in the web-based cloud storage system using 3D-AES block cipher cryptography algorithm." International Conference on Soft Computing in Data Science. Springer, Singapore, 2018.

[42] An, Sang Woo, and Seog Chung Seo. "Study on optimizing block ciphers (aes, cham) on graphic processing units." 2020 IEEE International Conference on Consumer Electronics-Asia (ICCE-Asia). IEEE, 2020.

[43] Selvaraj, P., & Varatharajan, R. (2018). Whirlpool algorithm with hash function based watermarking algorithm for the secured transmission of digital medical images. Mobile Networks and Applications, 1-14.

[44] Nakamura, J. (2017). Image Sensors and Signal Processing for Digital Still Cameras. CRC press.

[45] Kalantari, N. K., Wang, T. C., & Ramamoorthi, R. (2016). Learning-based view synthesis for light field cameras. ACM Transactions on Graphics, 35(6), 1-10.

[46] Chang, Y., Jung, C., Ke, P., Song, H., & Hwang, J. (2018). Automatic contrast-limited adaptive histogram equalization with dual gamma correction. IEEE Access, 6, 11782-11792.

[47] Bhandari, A. K. (2020). A logarithmic law based histogram modification scheme for naturalness image contrast enhancement. Journal of Ambient Intelligence and Humanized Computing, 11(4), 1605-1627.

[48] Singh, K. B., Mahendra, T. V., Kurmvanshi, R. S., & Rao, C. V. R. (2017). Image enhancement with the application of local and global enhancement methods for dark images. International Conference on Innovations in Electronics, Signal Processing and Communication (IESC 2017), 199–202.

[49] Al-Ameen, Z., Saeed, H. N., & Saeed, D. K. (2020). Fast and Efficient Algorithm for Contrast Enhancement of Color Images. Review of Computer Engineering Studies, 7(3), 60-65.

[50] Patel, P., & Bhandari, A. (2019). A review on image contrast enhancement techniques. International Journal Online of Science, 5(5), 14-18.

[51] Dixit, A. K., & Yadav, R. K. (2019). A review on image contrast enhancement in colored images. Journal of Computer Sciences and Engineering, 7(4), 263-273.

[52] Maragatham, G., & Roomi, S. M. M. (2015). A review of image contrast enhancement methods and techniques. Research Journal of Applied Sciences, Engineering, and Technology, 9(5), 309-326.

[53] Bertalmío, M., Caselles, V., & Provenzi, E. (2009). Issues about retinex theory and contrast enhancement. International Journal of Computer Vision, 83(1), 101-119.

[54] Sheet, D., Garud, H., Suveer, A., Mahadevappa, M., & Chatterjee, J. (2010). Brightness preserving dynamic fuzzy histogram equalization. IEEE Transactions on Consumer Electronics, 56(4), 2475-2480.

[55] Celik, T., & Tjahjadi, T. (2011). Contextual and variational contrast enhancement. IEEE Transactions on Image Processing, 20(12), 3431-3441.

[56] Saleem, A., Beghdadi, A., & Boashash, B. (2012). Image fusion-based contrast enhancement. EURASIP Journal on Image and Video Processing, 2012(1), 1-17.

[57] Poddar, S., Tewary, S., Sharma, D., Karar, V., Ghosh, A., & Pal, S. K. (2013). Non-parametric modified histogram equalisation for contrast enhancement. IET Image Processing, 7(7), 641-652.

[58] Singh, K., & Kapoor, R. (2014). Image enhancement via Median-Mean Based Sub-Image-Clipped Histogram Equalization. Optik, 125(17), 4646-4651.

[59] Singh, K., Kapoor, R., & Sinha, S. K. (2015). Enhancement of low exposure images via recursive histogram equalization algorithms. Optik, 126(20), 2619-2625.

[60] Singh, K., Vishwakarma, D. K., Walia, G. S., & Kapoor, R. (2016). Contrast enhancement via texture region-based histogram equalization. Journal of Modern Optics, 63(15), 1444-1450.

[61] Yue, H., Yang, J., Sun, X., Wu, F., & Hou, C. (2017). Contrast enhancement based on intrinsic image decomposition. IEEE Transactions on Image Processing, 26(8), 3981-3994.

[62] Cao, G., Huang, L., Tian, H., Huang, X., Wang, Y., & Zhi, R. (2018). Contrast enhancement of brightness-distorted images by improved adaptive gamma correction. Computers & Electrical Engineering, 66, 569-582.

[63] Mahmood, A., Khan, S. A., Hussain, S., & Almaghayreh, E. M. (2019). An adaptive image contrast enhancement technique for low-contrast images. IEEE Access, 7, 161584-161593. [2] Patel, P., & Bhandari, A. (2019). A review on image contrast enhancement techniques. Int. J. Online Sci, 5(5), 14-18.

[64] Bhandari, A. K. (2020). A logarithmic law-based histogram modification scheme for naturalness image contrast enhancement. Journal of Ambient Intelligence and Humanized Computing, 11(4), 1605-1627.

[65] Wu, X., Sun, Y., Kawanishi, T., & Kashino, K. (2021). Contrast enhancement based on discriminative co-occurrence statistics. Multimedia Tools and Applications, 80(4), 6413-6442.

[66] Gandhamal, A., Talbar, S., Gajre, S., Hani, A. F. M., & Kumar, D. (2017). Local gray level S-curve transformation–a generalized contrast enhancement technique for medical images. Computers in Biology and Medicine, 83, 120-133.

[67] El Malali, H., Assir, A., Bhateja, V., Mouhsen, A., & Harmouchi, M. (2020). A contrast enhancement model for x-ray mammograms using modified local s-curve transformation based on multi-objective optimization. IEEE Sensors Journal, 21(10), 11543-11554.

[68] Nnolim, U. A. (2018). An adaptive RGB colour enhancement formulation for logarithmic image processing-based algorithms. Optik, 154, 192-215.

[69] Bhateja, V., Nigam, M., Bhadauria, A. S., & Arya, A. (2020). Two-stage multi-modal MR images fusion method based on parametric logarithmic image processing (PLIP) model. Pattern Recognition Letters, 136, 25-30.

[70] Vertan, C., Florea, C., & Florea, L. (2021). A parametric logarithmic image processing framework based on fuzzy graylevel accumulation by the hamacher t-conorm. Sensors, 21(14), 4857.

[71] Khan, M. S., King, R., & Hudson, I. L. (2016). Transmuted kumaraswamy distribution. Statistics in Transition New Series, 17(2), 183-210.

[72] Murat, U., & Kadılar, G. (2020). Exponentiated Weibull-logistic distribution. Bilge International Journal of Science and Technology Research, 4(2), 55-62.

[73] Florea, C., & Florea, L. (2013). Logarithmic type image processing framework for enhancing photographs acquired in extreme lighting. Advances in Electrical and Computer Engineering, 13(2), 97-105.

[74] He, C., Xing, J., Li, J., Yang, Q., & Wang, R. (2015). A new wavelet thresholding function based on hyperbolic tangent function. Mathematical Problems in Engineering, 2015, 1-11.

[75] Łoza, A., Bull, D. R., Hill, P. R., & Achim, A. M. (2013). Automatic contrast enhancement of low-light images based on local statistics of wavelet coefficients. Digital Signal Processing, 23(6), 1856-1866.

[76] Nizami, Imran Fareed, et al. "Natural scene statistics model independent no-reference image quality assessment using patch based discrete cosine transform." Multimedia Tools and Applications 79.35 (2020): 26285-6304.

[77] Fang, Y., Ma, K., Wang, Z., Lin, W., Fang, Z., & Zhai, G. (2014). No-reference quality assessment of contrast-distorted images based on natural scene statistics. IEEE Signal Processing Letters, 22(7), 838-842.

[78] Min, X., Gu, K., Zhai, G., Liu, J., Yang, X., & Chen, C. W. (2017). Blind quality assessment based on pseudo-reference image. IEEE Transactions on Multimedia, 20(8), 2049-2062.

اداء طرق التشفير الكتلي وتحليل المخاطر

امنة خالد خليل الرجبو
المديرية العامة للتربية في محافظة نينوى
الموصل، العراق
amina.20csp64@student.uomosul.edu.iq

ياسين حكمت اسماعل
كلية علوم الحاسوب والرياضيات،
جامعة الموصل، الموصل، العراق
Yaseen-hikmat@uomosul.edu.iq

تاريخ الاستلام:30/6/2022 **تاريخ القبول:13/11/2022**

الملخص

يعد أمن خوارزميات التشفير الكتلي مسألة مهمة للغاية في مجال أمن المعلومات، إذ يسمح هيكلها البسيط والتشفير القائم على البرمجيات بتنفيذها في العديد من التطبيقات مثل أمان البيانات والحوسبة السحابية. في هذه الورقة، قدمنا مراجعة ثمان خوارزميات تشفير الكتلة، التي قدمت في السنوات الخمس الأخيرة واستخدامها في تطبيقات مختلفة. وهي DES و DES٣ و Blowfish و Two fish و PRISENT و KLEIN و IDEA و AES. جميع هذه الخوارزميات عبارة عن نظم تشفير كتلة متماثلة المفاتيح بتصاميم مختلفة. أظهرت نتائج المقارنة أن طرق تشفير الكتلة ما زالت تستخدم بشكل واسع في تطبيقات ومجالات مختلفة. كما أظهرت أن العديد من التعديلات المقدمة من قبل الباحثين اعتمدت على الدوال الفوضوية في توليد المفاتيح لتعزيز متانة طرق تشفير الكتلة وعشوائيتها. وأظهرت أيضًا أن AES هو أحد طرق تشفير الكتلة التي لا تزال خوارزمية غير مكسورة، ولا تزال تعديلاتها مستمرة لتناسب التطبيقات الجديدة الأخرى. بينما طرق التشفير الأقل قوة تحسنت بالتعديل المقدمة، لتكون أقوى ضد بعض الهجمات المحتملة. ويعد طول المفتاح وتعقيده وهيكل النظم التشفير من الاتجاهات الأساسية لتحسين طرق التشفير الكتلي.

الكلمات المفتاحية: تشفير البيانات، التشفير، التشفير الكتلي، تحليل الأداء.