Evaluation of Cipher Application Based on Digital Permutation Technical

Saja Jumaa Hammad [a], Dr. Qusay Abboodi Ali [b] , Dr. Mshari A. Alshmmri [c]
[a] Master student , Saja.J.Hammad35532@st.tu.edu.iq
[b] College of administration and economics , Tikrit University , Head of technical , Dr.qusay.a.ali@tu.edu.iq
[c] College of Computer Science and Mathmatics , Tikrit University.

Abstract: Security is one of the most prominent and important terms at the present time in order to protect our information and data that we want to preserve from any interference or intrusion. Security and the protection of our data can be achieved in several ways, the most important of which is cryptography.

Due to the importance of documents and information that institutions need to deal with or transfer via the Internet, and therefore unauthorized persons or through hackers can view and manipulate them. Therefore, these documents must be encrypted using cipher methods and techniques .

In this study, it was proposed new cipher application based on digital permutation technical . The application encrypts text files and it is characterized by high randomness . This system works on permutation of the letters and symbols many times until to get the ciphertext.

After the application, testing and evaluation of the system by the intended users, it was found that the system achieves the objectives of this study and meets the needs and requirements of the users in an easy and uncomplicated manner.

Keywords: Cryptography , Cipher , Digital Permutation Technical , Encryption Text , Decryption Text .

1. Introduction

To make communications inaccessible when transferring the information over any susceptible network encryption is a method that may be used. Enacryption is classified into two sorts of keys: symmetric and asymmetric key algorithms**(Bandyopadhyay, 2017)**. Traditional ciphers are based on substitution ciphers and transposition ciphers. Secure symmetric key encryption, on the other hand, is connected to the current block cipher. A block cipher is sometimes referred to as a deterministic algorithm with constant groupings of bits known as blocks and unchanging transformation. A key in a contemporary block cipher only permits a selective mapping of potential inputs to potential outputs. As a result, a contemporary block cipher is composed of a substitution function and a permutation function.

To reorder the bits acquired via the substitution function, the permutation function method is necessary. Circular shift and swap are two typical permutation functions used during block ciphers. According to **(Mohamed, Ali, & Ariffin, 2020)**, the byte permutation is more difficult because it spans the full block. As a result, a secure permutation is critical in making it impossible for an attacker to discover the structure of any other parts. Permutations should preferably be unrecognizable from a permutation chosen randomly from the collection of all permutations in the communication space**. (Sailaja, Srinivasa, & Ramesh, 2019)**

Because this ideal security primary aim is difficult to achieve, a more practical "security notion" has been founded, namely that a cryptographic primitive is assumed to be secure if no significant weaknesses have been discovered over a sufficiently extended time frame (e.g., a

few years) **(Beierle et al., 2019)**. On the other hand, another research **(Naito & Sugawara, 2020)** verified that quite efficient and adaptable block ciphers of that sort can surely be regarded to be the best understood architecture today and no serious vulnerabilities have been identified since its publication. Its simplicity and attractive structure, as well as its adaptability for a wide range of applications, make it today's cutting-edge cipher.

The architecture of a substitution permutation network was first described in a matrix, where the linear layer A was specified as a permutation of bits, i.e., the A to Z related matrix is a permutation matrix over. Currently, many permutation ciphers are key-alternating ciphers, and unkeyed round processes may be divided into (invertible) nonlinear layers and (invertible) linear **layers (Beierle, Canteaut, & Leander, 2018).**

2.Significance Of The Study

The importance of the study lies in achieving security objectives, For the highest degree of security and integrity of transmitted data. By blocking hackers who are proficient in hacking security and protecting Information from illegal use and unauthorized access. By designing a secure encryption system based on permutation technical , at the same time, it is easy, uncomplicated for the normal user and applicable.

Also , the search is limited to encrypting texts, numbers and symbols, and then ensuring that they are transmitted securely by using digital permutation technical. The designed system can be used by normal users.

3.Review Of Related Studies

In **(Mohamed, Ali, & Ariffin, 2020)** The researchers created a permutation function to increase the security of current block ciphers. The user submits the input data, known as plaintext, for the encryption method. Plaintext is then XORed with the cipher key. As a result, each element in a State was substituted byte by byte in the S-box known as SubByte. This paper is based on the S-box. After all components have been replaced, the elements are permuted using the Spiral Fibonacci function (the Fibonacci process is executed anticlockwise). It begins with a 4x4 square matrix of A2,1, A2,2, A1,2, A1,1 coordinate, which becomes A'0,0,A'1,0, A'2,0, A'3,0. The following items will be made accessible: A[r][c], where 'r' ranges from 0 to 3. (A[ ][ ] is the array). The above operations will be repeated until the matrix is filled with 'n*n' values). The components are then turned into a MixColumn operation, which is comparable to the AES idea. The components of the MixColumn are then XORed with the AddRoundKey to generate the ciphertext, . As a result, the suggested block cipher enhanced the diffusion characteristic between plaintext and ciphertext.

In **(Murillo-Escobar, Abundiz-Pérez, Cruz-Hernández, & López-Gutiérrez, 2014)** present a novel symmetric text encryption algorithm based on chaos. The approach uses two logistic maps and one permutation & diffusion round (which involves changing the symbol value and position) to defend against a chosen or known plain text attack. Additionally, a secret key with 32 hexadecimal digits (128 bits) is used. This technical does not have a high level of security due to the use of only one permutation and diffusions round. In addition, the logistic map has some disadvantages when it is used in cryptography such as chaotic ranges discontinues, distribution not uniform, small space key and periodicity in chaotic ranges.

From other side **(Karimnia, Khaleel, & Turaev, 2018)** proposed encryption and decryption methodologies based on permutation matrices. The algorithms rely on a random selection of elements from the permutation matrix, also called the key matrix - entries . A permutation matrix is an $\boldsymbol{n}\times\boldsymbol{n}$ matrix which is obtained by permuting its rows and columns

according to some permutations of the numbers **0** to $\boldsymbol{n}$. In the permutation matrix proposed both sender and receiver sides use the same keys which are the introduced permuted matrices being vulnerable to attack.

Researchers such as **(Yin & Wang, 2018**) proposed a new chaotic image encryption scheme using breadth-first search and dynamic diffusion . The permutation-diffusion architecture is employed in this scheme . The breadth-first search is firstly used to transform an image into a sequence, and then the sequence is divided into 4 × 4 matrices to be traversed using breadth-first search. Thus the correlation between adjacent pixels of an image in all directions can be broken. Meanwhile, the diffusion key stream is rearranged using breadth-first search in the control of the scrambled key stream . The suggested dynamic diffusion method increases the sensitivity of the cryptosystem and can guarantee that each pixel being encrypted is connected to every other pixel.

In the same issue **(Ping, Xu, Mao, & Wang, 2018)** propose an efficient permutation - substitution image encryption network with Henon map. In order to improve the encryption efficiency, present a new two-point diffusion strategy which is able to process two pixels simultaneously. Hence, if there are multiple processing units, the diffusion process would be further expedited. Besides, permutation and diffusion are no longer two independent parts . When a new pixel position is determined, the pixel value is changed rather than determining the following pixel position. The permutation and diffusion stages are merged so that the image pixel matrix is required to be scanned just one time in each round. The enhanced permutation-substitution architecture is hence more effective.

In **(Ping, Fan, Mao, Xu, & Gao, 2018)**The researchers suggested image -cryptosystem uses the traditional "permutation-diffusion" framework. In the permutation step, a new digit-level permutation algorithm is suggested. This type of digit-level permutation can remove excessive correlation between neighbouring pixels while also changing the pattern of pixels in the plain-image. The suggested image encryption technique additionally uses the "Image Feature" to update the 2D-starting LASM's values. As a result, key-stream creation is reliant on a plain-image that can efficiently withstand a chosen-plaintext assault.

4. Methods

The study population included all the professors and employees of the College of Pharmacy, Tikrit University, which numbered (45) individuals. The sample was determined to include the community as a whole as a comprehensive intentional sample, as an electronic questionnaire form was distributed to the sample members (45 individuals). The number of retrieved and valid forms for analysis reached (36) forms, with a recovery rate of (80%), after excluding the forms that refused to answer, or that included a lack of information.

4.1.Statistical Techniques Used in the Present Study

In light of the technical and digital progress that witnessed a wide-scale exchange of official and unofficial information electronically and via the Internet, whether at the level of individuals or institutions. This led to the limited ability to control information security and its disclosure with the presence of a large number of professional people to penetrate technical systems and steal their information, so the interest has become more focused on building digital walls that help reduce this intrusion and using all means to help achieve this. Perhaps among those means are data encryption processes, which help in achieving a kind of security and protection for that data. Therefore, in this study, an attempt was made to propose an effective design of new cipher application based on digital permutation technical. To test the extent to which it can be applied in the Iraqi environment, and to evaluate the extent of the achieved benefit and the success of its use. The evaluation was done using a questionnaire

form prepared for this purpose that included testing the proposed design according to four characteristics (Usability, Ease of use, Flexibility, and Security).

4.2.Data Analysis and Interpretation

Regard to the distribution of sample items according to demographic variables, Table 1. shows the distribution of the study sample.

Variables	Category	Frequency	Percentage %
Gender	Male	27	%75.0
	Female	9	%25.0
Age	20-29	4	%11.1
	30-39	18	%50.0
	40-49	7	%19.4
	50-59	6	%16.7
	60- or more	1	%2.8
Educational	Diploma	1	%2.8
	B.Sc	6	%16.7
	Master's	18	%50.0
	PhD	11	%30.6
Experience	1-4 year	7	%19.4
	5 year or more	29	%80.6

Table 1 : Distribution of sample vocabulary according to demographic variables

It is clear from Table 1. that:

First. In terms of gender: It is noted that (75%) of the sample surveyed are males, compared to (25%) females, which means that the majority of the respondents are males, as shown in Figure (1).

Secondly. In terms of age: it is noted that a large percentage of the sample are (29) years and older approximately (89%). Because the study sample included university employees and professors, and students were not included, as shown in Figure (2).

Third. In terms of education: The number of the respondents who hold a higher master's and doctorate degrees reached (29) individuals, a percentage of (80.6%). Which is the largest percentage among the sample members, while (2.8%) are holders of diplomas and (16.7%) are holders of a bachelor's degree. Which means that the majority of the sample are university professors, as shown in Figure (3).

Fourthly. In terms of experience: The number of the respondents whose years of experience were (5) years and more was (29) individuals, with a percentage of (80.6%) of the total sample size of (N=36) individuals, which enhances the aspect of experience among the sample members and the accumulation of technical knowledge, as shown in Figure (4).

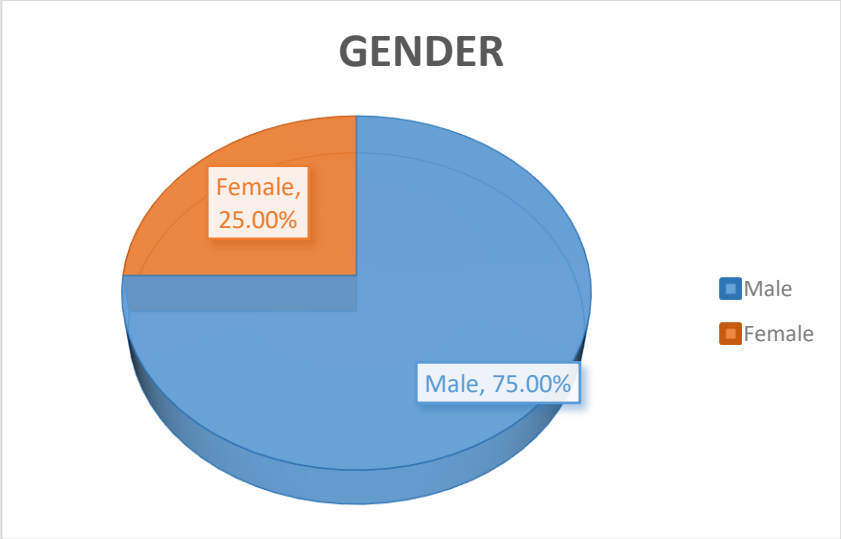

Figure 1. Distribution of the study sample according to the Gender

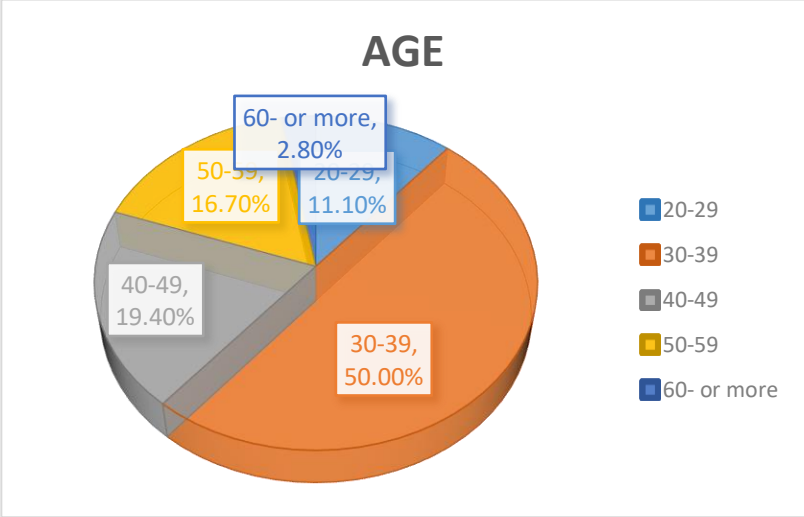

Figure 2. Distribution of the study sample according to the Age

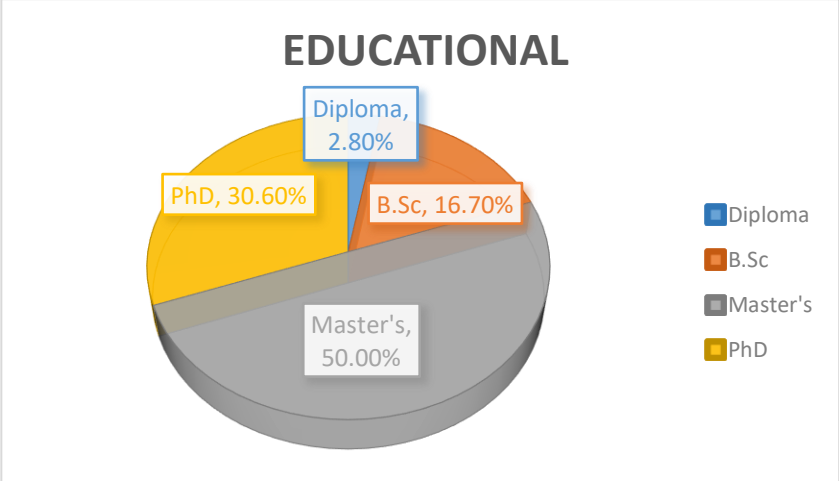

Figure 3. Distribution of the study sample according to Educational

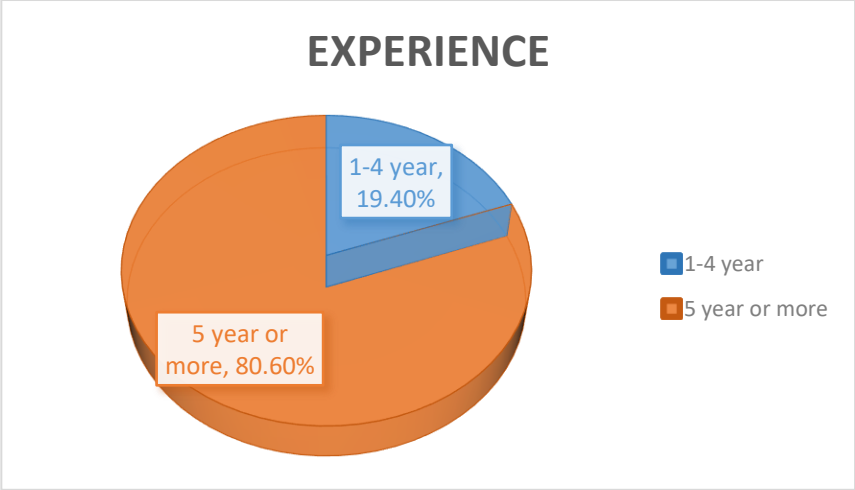

Figure 4. Distribution of the study sample according to Experience

Figure (5) shows the mean of the four dimensions as well as their combined values.

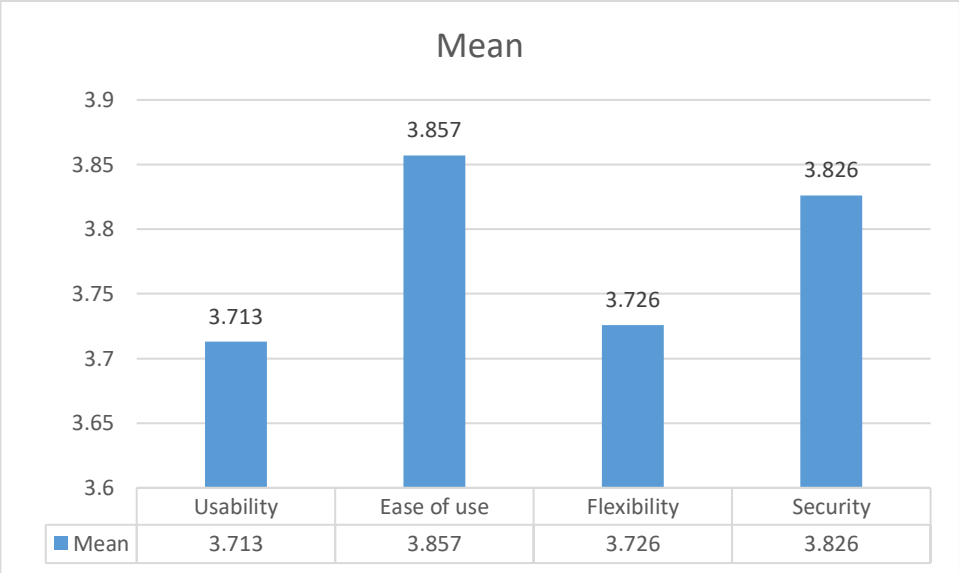

Figure 5. The Mean for the dimensions of application

5.Recommendations

- To improve the system, the following recommended:
- Find other approaches to increase the level of security and reduce Complexity.
- Design an encryption application with simple and easy user interface.
- Technical rounds can be increased to increase the randomness of the encryption.
- Design encryption methods and techniques that take into account the requirements of the normal user .

6.Conclusion

Security plays a main role in transmitting our data and dealing with it, because this data can be accessed by a third party or an outsider. Cryptography plays an important role in the safe transmission of data. Data is encrypted and decrypted by many techniques. but the crisis is that most of the available encryption algorithms of permutation technical are designed for only professional user to text cipher without care to the normal user

Therefore , has been proposed an effective design of new cipher application based on digital permutation technical. To test the extent to which it can be applied in the Iraqi environment . College of Pharmacy at Tikrit University has been selected according to their request and need , and to evaluate the extent of the achieved benefit and the success of its use. The evaluation was done using a questionnaire form prepared for this purpose that included testing the proposed design . After analyzing the responses and based on the results this system proved its effectiveness in encryption .

In conclusion, in an easy, simple and complex-free way the technical which makes the ciphertext stronger and secure that could not be easily determined by an attacker .

References

1. Bandyopadhyay, M. G. P. S. K. (2017). A Proposed Method for Cryptography using Random Key and Rotation of Text. *International Journal, 6*(2).
2. Beierle, C., Biryukov, A., dos Santos, L. C., Großschädl, J., Perrin, L., Udovenko, A., . . . Biryukov, A. (2019). Schwaemm and Esch: lightweight authenticated encryption and hashing using the Sparkle permutation family. *NIST round, 2*.
3. Beierle, C., Canteaut, A., & Leander, G. (2018). Nonlinear approximations in cryptanalysis revisited. *IACR Transactions on Symmetric Cryptology, 2018*(4), 80-101.
4. Karimnia, R., Khaleel, G., & Turaev, S. (2018). New Cryptosystem Based-on Permutation Matrix. *International Journal on Perceptive and Cognitive Computing, 4*(1).
5. Mohamed, K., Ali, F. H. H. M., & Ariffin, S. (2020). A New Design of Permutation Function Using Spiral Fibonacci in Block Cipher. *International Journal, 9*(1.3).
6. Murillo-Escobar, M., Abundiz-Pérez, F., Cruz-Hernández, C., & López-Gutiérrez, R. (2014). *A novel symmetric text encryption algorithm based on logistic map.* Paper presented at the Proceedings of the international conference on communications, signal processing and computers.
7. Ping, P., Fan, J., Mao, Y., Xu, F., & Gao, J. (2018). A chaos based image encryption scheme using digit-level permutation and block diffusion. *IEEE Access, 6*, 67581-67593.
8. Ping, P., Xu, F., Mao, Y., & Wang, Z. (2018). Designing permutation–substitution image encryption networks with Henon map. *Neurocomputing, 283*, 53-63.
9. Sailaja, K., Srinivasa, R., & Ramesh, P. (2019). A New Circle based Symmetric key Encryption Technique for Text Data. *International Journal of Advanced Trends in Computer Science and Engineering, 8*(5), 2573-2576.
10. Yin, Q., & Wang, C. (2018). A new chaotic image encryption scheme using breadth-first search and dynamic diffusion. *International Journal of Bifurcation and Chaos, 28*(04), 1850047.