Al-Salam Journal for Engineering and Technology
Journal Homepage: http://journal.alsalam.edu.iq/index.php/ajest
e-ISSN: 2790-4822 p-ISSN: 2958-0862

Effective Design of Secure Cipher Application Based on Digital Alteration Technical

Saja Jumaa Hammad [1], Dr.Qusay Abboodi Ali [2], Dr. Mshari A.Alshmmri [1]*

[1]College of Computer Sciences and Mathematics, Tikrit University, Tikrit, IRAQ
[2]College of administration and economics, Tikrit University, Head of Technical, Tikrit, IRAQ
[1]College of Computer Science and Mathematics, Tikrit University, Tikrit, IRAQ.

*Corresponding Author: Dr. Mshari A.Alshmmri

DOI: https://doi.org/10.55145/ajest.2023.01.01.004
Received July 2022; Accepted October 2022; Available online October 2022

ABSTRACT: In today's era, communication and sharing of information is increasing rapidly. It is important to mention that Cryptography has been used for secure communication since it is regarded an important tool to protect the information in the modern world in computer systems.

Many techniques can be used to implement the encryption like substitution and permutation or sometimes by some mathematical readability. The cipher text can be generated according to the human comprehension and readability after applying any of the aforementioned techniques.

In this research, have studied and analyzed the current limitations and challenges of cipher and algorithms context from the perspective of security design. Then, we have identified the design dimensions and components of a secure cipher application based on digital alteration technical. Then, a secure cipher application based on digital change technical was constructed and developed. At last, we tested and evaluated the user interaction in cipher application prototype based on suggested technical. Through experience, it was confirmed that the digital alteration technical is useful and easy for users who work on text encryption.

Keywords: Secure Cipher**,** Permutation, Cryptography**,** Encryption, Decryption.

1. INTRODUCTION

Internet has made life easier ; however , it has added difficulty to the field of security. The advancement of technology and the internet in the last ten years has been enormous [1] . Previously, only textual data was utilised, but with the increasing emergence of computer networks, official files between organizations, such as formal text, photos, audio, and video, may now be readily sent via the internet. These benefits have a cost, in the form of a breach in the confidentiality of the information being transmitted .

Cryptography is defined as a technique which can be used to secure and guarantee the authenticity of data and it composed of two processes, which are encryption and decryption [2]. Thus, the textual encryption procedure necessitates 100% precise outcomes after decryption [3] .

In cryptography, the data of extreme secret can be encrypted in a way which even when the data is obtained by unauthorised parties, the genuine data cannot be discovered as it is encrypted. The original data to be conveyed is known as plaintext in cryptography, while the data that has been encrypted is known as ciphertext. The goal of cryptography is to keep the information included in the data private so that unauthorised individuals could not access it [2].

2. PROBLEM STATEMENT

Even now, cryptography is crucial in preserving information, keeping it private and resistant to attackers. Cryptography aids in the transmission of information from a transmitter to a recipient by guaranteeing secrecy and integrity. It is accomplished through two distinct methods : encryption and decryption [4] .

As a result, the encryption of communications is a significant in order to protect the transference of data in order not to be accessible during the performance of susceptible network. As technology advances, a new model of

*Corresponding author: *Saja.J.Hammad35532@st.tu.edu.iq* cryptographic algorithm is necessary to meet the new system demands. Several text encryption approaches, however, have been developed to increase text security [5] .

Actually, various permutation technological approaches are utilized to improve security in current digital ciphers . These techniques are meant to reorder or process the complete bit inputs using substitution boxes. However , the problem is that the majority of the current algorithms about the technical permutation has been developed to be used for only experts users of the text cipher rather than the normal users. In addition to the complexity and delay in the encryption and decryption [6] .

Furthermore, traditional ciphers are based on permutation and transposition ciphers , such as the Rail Fence cipher, the Caesar cipher, and the Playfair cipher [7]. The permutation component method is also necessary for reordering the acquired bits through the function of substitution. In light of what has been said, a good cipher should behave randomly. The byte permutation is more challenging because it affects the entire block .

The production of "confusion and diffusion" in the text blocks generated by several rounds of Feistel- or SPN-based ciphers depends heavily on the substitution and permutation operations [8]. A subkey manufacturing mechanism and related rounds of substitution and permutation methods are used by several symmetric block ciphers to produce a different round key for every encryption round. There are predefined substitution and permutation boxes used by algorithms like DES. As opposed to other algorithms like the Blowfish block cipher [9], Khufu algorithm and Twofish [10] utilize dynamic substitution and permutation boxes. All these processes of algorithms cause a delay in the encryption and decryption of text [11].

Because standard cryptography algorithms are too heavy to execute, there is currently no reliable solution that ensures security for resources restricted devices [12] . International organisations, consulting businesses, think tanks, and universities, for their part, have emphasised the rising relevance of cyber threats [13].

3. LITERATURE REVIEW

In [14] created the encryption technique using a mix of the Self-Synchronizing Stream Cipher and a chaotic map. The algorithm for encryption and decryption involves four fundamental operations . Key generation operations, permutation operations, substitution operations, and XOR feedback operations are all examples of these operations. Although the proposed encryption scheme is considered secure because of its large key space (2^128) ,it is highly sensitive to the cipher keys and plaintext. However, the results of other investigations (2D Tent map, 2D CNT, 2D Chebyshev polynomial, 2D Henon map) are unquestionably superior. Given that the key space is greater than (2^128), all offered methods are clearly resistant to any brute-force attacks, as it is (2^256, 2^319 , 2^149 , 2^928)and has more than key sensitivity.

In [15] To improve the security of the Serpent block cipher algorithm, a dynamic technique based on chaotic maps for key generation, permutation, and replacement was presented. The outcome showed that the dynamic approach has better randomness than a conventional Serpent algorithm. As a result, it can cut down on both time and round usage. Additionally, for added protection, chaotic map-based key creation. The outcome indicated that the dynamic technique has good randomness, nonetheless. However, because the dynamic technique uses a chaotic map to generate key rounds, it is sensitive to any change in the key.

In [16] proposed a brand-new chaotic cryptosystem for text ciphering that is utilized to protect user privacy and the confidentiality of data in a variety of applications. By including a chaos-based permutation step utilizing Arnold's cat map, the cryptosystem is strengthened. This permutation technique may allow the investigation to mask a chaotic synchronization indexation. The cryptosystem produces great results: it generates a uniform histogram, has a large secret key size to withstand a brute force assault, is sensitive to the secret key, and can withstand an entropy attack. But there is a delay in the execution time, and the system cannot withstand all attacks.

In [17] used three secret keys in their proposed encryption and decryption techniques for speech signals . The permutation of the speech signal's segments serves as the foundation for the suggested algorithm. A circular shift (in row and column) based on the bits of the encryption keys is used in the permutation process. DCT or DST are also used by the encryption system to obliterate signal inteligibility. An experimental investigation of the algorithm revealed that it is more robust and secure. However, there was a correlation between the original speech and the encoded speech, and there were running-time delays.

From other side, [18] designed a 2D Baker's map-based safe and lightweight image encryption technique. As a result, the suggested technique permuted a plain image first used a randomly numbers of a pseudo sequence which can be generated by a map of 2D Baker's and then it is followed a procedure of diffusion relying on XORing. The technique employed secret keys with two pairs, where one of them is used for permutation and the other one for diffusion. It showed good outcomes after only one cycle of encryption. Since the proposed design was implemented using a single round and the permutation was performed to change the pixel positions without changing their values, the proposed work was not considered safe enough.

However, [19] outlined a method for image encryption based on pixel permutation and Josephus traversal in relation to plaintext. First, improved Josephus traversing was employed to scramble the image rather than ordinary Josephus traversing. Additionally, the Chen chaotic system was driven to conduct bit exclusive or cross operations on the block image using the hash value of the encrypted picture as its initial argument. The straightforward bit position altering technique was unable to alter the statistical distribution of the bits in order to mitigate the dangers brought on by the independence of the picture encryption algorithm and the plaintext. [20], and it was easy to track the bits, which led to cracking. Last, the confusion and diffusion characteristics of the algorithm were further enhanced by cipher feedback.

4. Materials and Methods

The study proposes “**Secure Cipher Application (SCA) Based on Digital Alteration Technical”** for text files encryption. In this study, the general Research Design Methodology is method which is developed by Vaishnavi and Kuechler (2019) . It composed of five phases, which are: Awareness of a problem, Suggestion, Design, Testing, Evaluation and Conclusion

Actually, there are many encryption algorithms (techniques) today to improve the security of the text, there is still a need to redesign the encryption technical to meet the user needs and modren system requirements. Therefore, there are many methods used permutation technical for improving security in modern digital, but the problems belongs to that the technique of permutation encryption algorithms is designed only for experts users of the text cipher regardless the normal users. As well, complexity and delay in the encryption and decryption.

Therefore, after identifying and understanding the needs of users from the first phase of the design research method, This study proposes an “Effective Design of Secure Cipher Application Based on Digital Alteration Technique” to text cipher . So that this technical should meet the needs of the normal user .

The design phase includes the main tools and components used to design suggested technical including “Hardware Tools” represented by (Laptop , Processor , Memory and Hard Disk) and “Software Tools “ as this work suggests a high level security for the proposed encryption technical designed and it was implemented in Java language and its components . Java was used because it is a high-level programming language. It works on all the most important Operating Systems, such as Windows, Linux, and Mac. That it is considered one of the most popular and powerful programming languages at all. It has an integrated platform, It is also an objective oriented language and has a long and rich language history and provides many built-in libraries in different fields.

After the project is successfully implemented, the testing phase comes to ensure that the research is working as per the specifications and its objectives are achieved.

When the technical was designed, practically applied and it was tested, it will be presented and used by one of the official institutions in the Iraq. Because this phase will consist of soliciting feedback from others as well as a self-evaluation of the project, by conducting a questionnaire for the purpose of evaluating the designed technical to see the extent to which the proposed encryption technical is achieved User Requirements.

5. System Components

After the program is run, Fig1: shows the system interface designed to encrypt and decrypt text files, in addition to the screen of encryption and decryption processes based on using digital alteration technical. The original text is initially entered, encrypted and then decrypted to be restored it to its original form. This system includes four main parts as shown in the screen below.

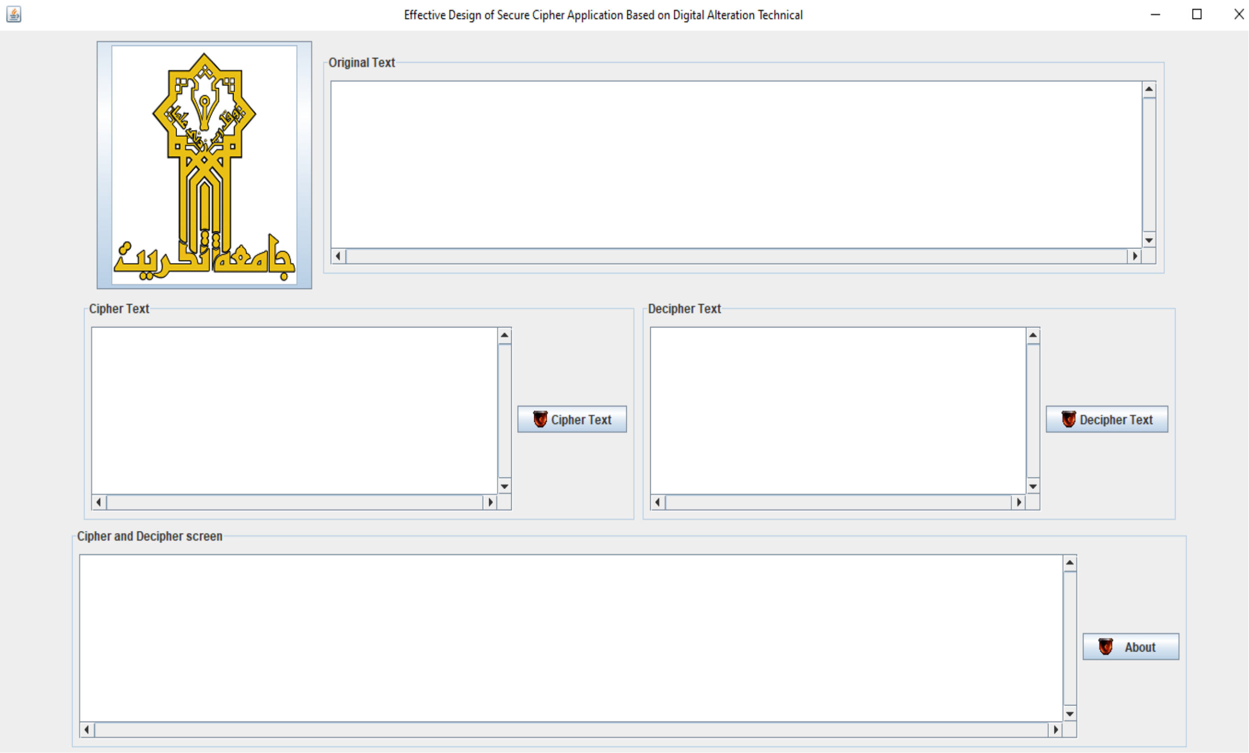
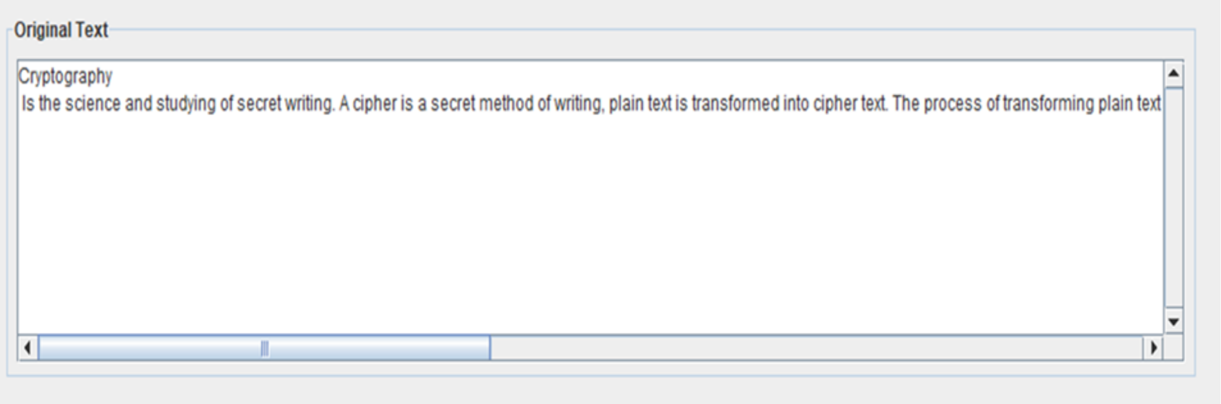

Effective Design of Secure Cipher Application Based on Digital Alteration Technical
Original Text
Cipher Text
Decipher Text
Cipher Text
Decipher Text
Cipher and Decipher screen
About

FIGURE 1. **Integrated system interface**

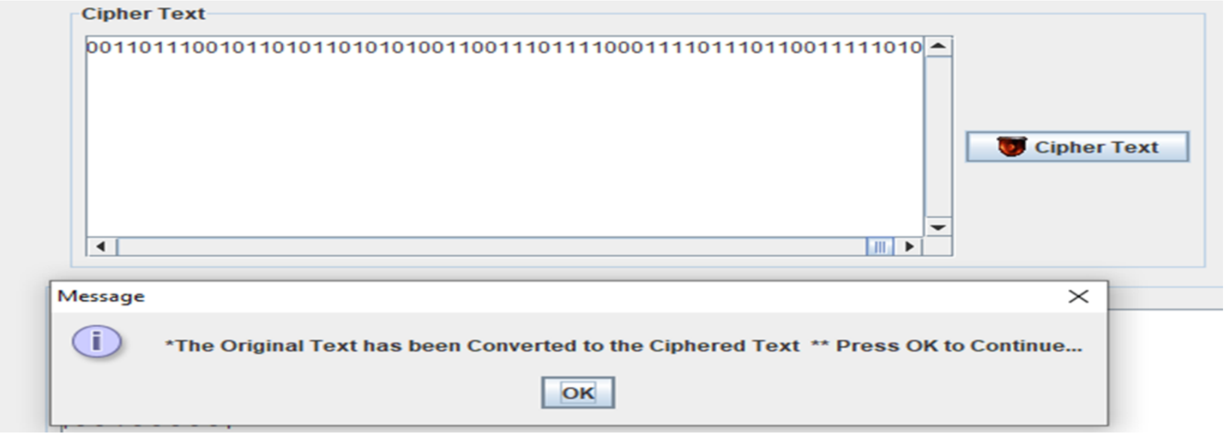
Fig 2: that shows the (Original Text Component) This component includes the original text (short, or long text) , that allows the user to types text to be ciphered.



Cryptography
Is the science and studying of secret writing. A cipher is a secret method of writing, plain text is transformed into cipher text. The process of transforming plain text

FIGURE 2. **The interface of entering the original text**

Fig3: that shows the (Cipher Component) the cipher component works based on a four phases. The first phase is to enter the original text (letters) to the two dimensional array. Second phase convert the original text (letters) into digits (0,1) by using multi array. Third phase is to change between (0,1). Finally after pressing the cipher button, the text will be encrypted, and this field shows a series of zeros and ones (0,1) . Also, a message appears indicating the end of the encryption process .



Cipher Text

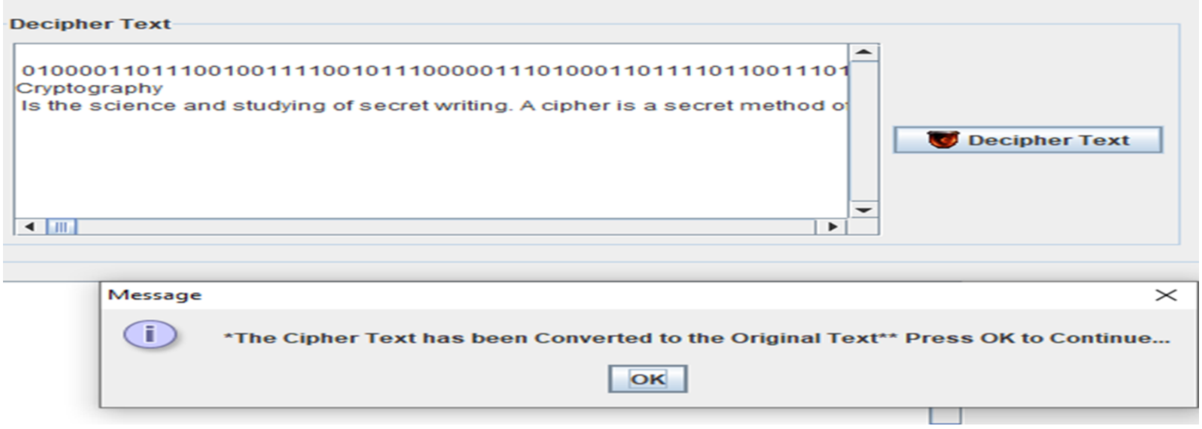
001101110010110101101010100110011101111000111101110110011111010

Message

*The Original Text has been Converted to the Ciphered Text ** Press OK to Continue...

FIGURE 3. Cipher text with message

Fig4: that shows the (Decipher Component) third part of the system component. The ciphertext that appears in the second interface of system is decrypted. When the user presses on the decipher button, all processes in previous part (Cipher component) will be repeated to convert cipher text (0,1) into the original text . Also , a message appears indicating to the end of decryption process .



Decipher Text

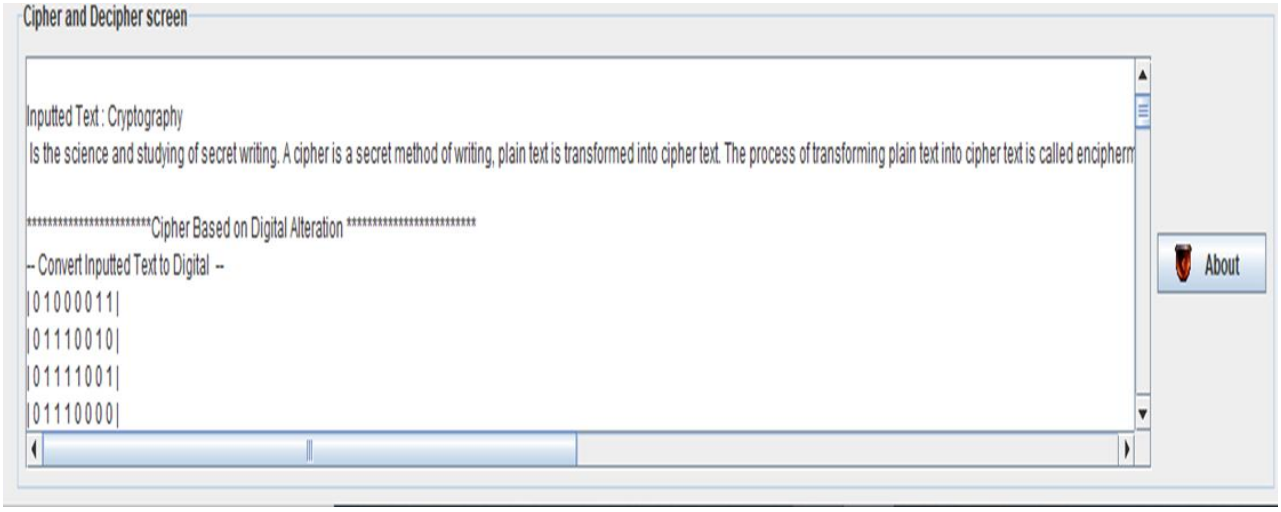
0100001101110010011110010111000001110100011011110110011101
Cryptography
Is the science and studying of secret writing. A cipher is a secret method of

Message

*The Cipher Text has been Converted to the Original Text** Press OK to Continue...

FIGURE 4. Decipher text with message

Cipher and decipher screen component as shown in Fig5: is the fourth and final component of the system interface, showing all the processes and phases that include the original text phases to be converted into the ciphertext and then decipher text and to restore the text to its original form. In detail, first, the original text is entered into two dimensional array that contains zeros and ones . Then, this array is divided into two arrays (side A and side B) based on the change between array columns and rows. The process of permutation is started with changing between digits (0,1) . Then , the process of permutation happens between the two arrays, cell with cell, then column with column, then row with row, and finally mixed side A with side B in one array that includes the ciphertext. This permutation process is repeated ten times to get the ciphertext. Then, the decoding process is done with the same steps but in the opposite order to obtain the original text. Furthermore, at the bottom of the screen, the time required for the encryption and decryption processes is displayed in milliseconds.



```
Inputted Text : Cryptography
Is the science and studying of secret writing. A cipher is a secret method of writing, plain text is transformed into cipher text. The process of transforming plain text into cipher text is called encipherm

************************Cipher Based on Digital Alteration ************************
-- Convert Inputted Text to Digital --
|01000011|
|01110010|
|01111001|
|01110000|
```

FIGURE 5. Cipher and Decipher screen

6. Results

In this study, a prepared questionnaire is adopted to evaluate the effectiveness of the used design for secure cipher based on digital alteration technique. The model included four dimensions that represent the distinctive characteristics of this design (Usability, Ease of use, Flexibility, and Security), with 30 items distributed to the previous four dimensions, as well as for four demographic information (Gender, Age, Educational level and Experience). Table1: displays the questionnaire's dimensions and items.

Table 1. Dimensions and phrases the model of the secure cipher application based on digital alteration technical

Items	Dimensions	Number	Sequence
The first axis is composed of demographic information	Gender		
	Age		
	“Educational Level”		
	Experience		
The second axis: model of the secure cipher application based on digital alteration technical	Usability	6	1-6
	Ease of use	6	7-12
	Flexibility	7	13-19
	Security	11	20-30
Total		30	1-33

The five-point Likert scale was chosen to represent the sample's patterns. The scale went from (5 = “strongly agree”, to 1 = “strongly disagree”). The process utilized to quantitatively describe the qualitative data from the questionnaire is shown in Table 2.

Table 2. The five-point Likert scale's opinion direction

Scale	Degree	Mean	Direction of view
“Strongly Disagree	1	1 - 1.79	Very weak
Disagree	2	1.80 - 2.59	Weak
Neutral	3	2.60 - 3.39	Average
Agree	4	3.40 - 4.19	High
Strongly Agree	5	4.20 to 5	Very high”

In order to determine the values of the arithmetic averages, standard deviations, highest and lowest values that illustrate the characteristics of the study variables according to the respondents' opinions, the research carried out a descriptive analysis of the data using the statistical program (SPSS Ver.22). Table3 displays the findings.

Table 3. The outcomes of the descriptive analysis of the respondents' opinions

Dimensions	Mean	Std. Deviation	Minimum	Maximum	Relative importance%	Variation coefficient	Severity of approval
Usability	3.713	0.833	2.170	5	74.3%	22.4%	High
Ease of use	3.857	0.697	2.670	5	77.1%	18.1%	High
Flexibility	3.726	0.537	2.710	5	74.5%	14.4%	High
Security	3.826	0.493	3.000	5	76.5%	12.9%	High
Total (Secure Cipher)	3.786	0.393	3.070	5	75.7%	10.4%	High

According to the relative importance ratio of (74.5%–77.1%) and the value of the mean that was higher than the standard mean of (3) for all dimensions, it is clear from Table 3 that the respondents' awareness of the dimensions of the effective design of secure cipher application based on digital alteration technical was high. More people agreed on the secure cipher application's flexibility of use, security, and convenience of use based on digital alteration technology. Usability came in last. Additionally, it should be emphasized that there was no variance in the sample members' assessments of the efficacy of the secure cipher application based on technical digital alteration, as measured by the standard deviation and coefficient of variation, which recorded a proportion for all dimensions less than (50%), confirming the presence of consistency in opinions about the effectiveness of the model.

7. Discussion/Conclusion

In this study, the effectiveness of the design for secure cipher application is proposed according to digital alteration technique. The college of Pharmacy at Tikrit University is selected as a suitable Iraqi environment according to its needs and requirements. A questionnaire form is designed in order to evaluate and measures the achieved benefits and its success in its usage. It is noted that this system proves its effect in encryption according to the analysis of the obtained results.

However, this study has concluded the following findings about the Digital Alteration Technical:

1. It is noted that this technique is very easy, simple with a way of complex-free which reflects that the cipher text is strong and secure that no one can be easily permeated by the attacker.
2. The text size after applying the digital alteration technical and the encryption procedure is the same as the length of the original text, meaning that there is no increase in the text size after encryption.
3. The time it takes to encrypt the text depends on the length of the text (that is, it is directly proportional with the text size).
4. The accuracy of the results in the decrypting process has been confirmed by (100%) .
5. Digital alteration technical is very fast in relation to the encryption time.
6. Through the practical application of the technical, was found that it is understand and can be used easily.

REFERENCES

[1] S. P. Indrakanti and P. Avadhani, "Permutation based image encryption technique," *International Journal of Computer Applications*, vol. 28, pp. 45-47, 2011.

[2] J. Jamaludin and R. Romindo, "Implementation of Combination Vigenere Cipher and RSA in Hybrid Cryptosystem for Text Security," *IJISTECH (International Journal of Information System & Technology)*, vol. 4, pp. 471-481, 2020.

[3] S. Mutnuru, S. K. Sah, and S. P. Kumar, "Selective encryption of image by number maze technique," *Int. J. Cryptogr. Inf. Secur*, vol. 10, pp. 1-10, 2020.

[4] K. Minematsu, "Fast decryption: a new feature of misuse-resistant AE," *IACR Transactions on Symmetric Cryptology*, pp. 87-118, 2020.

[5] K. Mohamed, F. H. H. M. Ali, and S. Ariffin, "A New Design of Permutation Function Using Spiral Fibonacci in Block Cipher," *International Journal*, vol. 9, 2020.

[6] T. Hiscock, O. Savry, and L. Goubin, "Lightweight instruction-level encryption for embedded processors using stream ciphers," *Microprocessors and Microsystems*, vol. 64, pp. 43-52, 2019.

[7] Z. Bao, J. Guo, T. Iwata, and K. Minematsu, "ZOCB and ZOTR: tweakable blockcipher modes for authenticated encryption with full absorption," *IACR Transactions on Symmetric Cryptology,* pp. 1-54, 2019.

[8] K. Sailaja, R. Srinivasa, and P. Ramesh, "A New Circle based Symmetric key Encryption Technique for Text Data," *International Journal of Advanced Trends in Computer Science and Engineering,* vol. 8, pp. 2573-2576, 2019.

[9] Y. Naito and T. Sugawara, "Lightweight authenticated encryption mode of operation for tweakable block ciphers," *IACR Transactions on Cryptographic Hardware and Embedded Systems,* pp. 66-94, 2020.

[10] J. Cao, X. Zhang, H. Wang, and L. Jiang, "Research on Automatic Analysis Technology of Cryptographic Algorithm," in *2020 2nd International Conference on Information Technology and Computer Application (ITCA),* 2020, pp. 182-185.

[11] N. Zakaria, "A block cipher based on genetic algorithm," *Universiti Putra Malaysia,* 2016.

[12] S. Thapliyal, H. Gupta, and S. K. Khatri, "An Innovative Model for the Enhancement of IoT Device Using Lightweight Cryptography," in *2019 Amity International Conference on Artificial Intelligence (AICAI)*, 2019, pp. 887-892.

[13] T. Simon and B. Venard, "Technical codes’ potentialities in cybersecurity. A contextual approach on the ethics of small digital organizations in France," in *2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*, 2020, pp. 1-8.

[14] E. A. Albahrani and T. K. Alshekly, "A Text Encryption Algorithm Based on Self-Synchronizing Stream Cipher and Chaotic Maps," *vol,* vol. 3, pp. 579-585, 2017.

[15] I. A. Yousif, "Proposed A permutation and substitution methods of serpent block cipher," *Ibn AL-Haitham Journal For Pure and Applied Sciences,* vol. 32, pp. 131-144, 2019.

[16] M. Azzaz and M. Krimil, "A new chaos-based text encryption to secure gps data," in *2018 International Conference on Smart Communications in Network Technologies (SaCoNeT),* 2018, pp. 294-299.

[17] D. Slimani and F. Merazka, "Encryption of speech signal with multiple secret keys," *Procedia computer science,* vol. 128, pp. 79-88, 2018.

[18] B. Mondal, P. Kumar, and S. Singh, "A chaotic permutation and diffusion based image encryption algorithm for secure communications," *Multimedia Tools and Applications,* vol. 77, pp. 31177-31198, 2018.

[19] Y. Niu and X. Zhang, "A novel plaintext-related image encryption scheme based on chaotic system and pixel permutation," *IEEE Access,* vol. 8, pp. 22082-22093, 2020.

[20] Z. Guan, J. Li, L. Huang, X. Xiong, Y. Liu, and S. Cai, "A Novel and Fast Encryption System Based on Improved Josephus Scrambling and Chaotic Mapping," *Entropy,* vol. 24, p. 384, 2022.