ARTICLE

JOURNAL OF UNIVERSITY OF BABYLON
For Pure and Applied Sciences (JUBPAS)

Vol.31; No.1.| 2023

Encrypting of Text Based on Chaotic Map

Hadeel Talib Mangi[1*], Suhad A. Ali[2], Majid Jabbar Jawad[3]

[1*]Computer Department, Science College for Women, , Babylon University, hadeel.mangi.gsci116@student.uobabylon.edu.iq ,Hilla, Iraq

[2]Computer Department, Science College for Women, Babylon University, suhad.ali2003@yahoo.com,Hilla,Iraq

[3]Computer Department, Science College for Women, Babylon University,Majid_al_sirafi@yahoo.com,Hilla,Iraq

***Corresponding author email:** hadeel.mangi.gsci116@student.uobabylon.edu.iq;mobil:07729013860

تشفير النص بالاعتماد على خريطة الفوضى

هديل طالب منجي*[1]، سهاد احمد علي[2]، ماجد جبار جواد[3]

* [1] كلية العلوم للبنات،جامعة بابل، hadeel.mangi.gsci116@student.uobabylon.edu.iq،الحلة،العراق

[2] كلية العلوم للبنات،جامعة بابل، suhad.ali2003@yahoo.com،الحلة،العراق

[3] كلية العلوم للبنات،جامعة بابل، Majid_al_sirafi@yahoo.com،الحلة،العراق

Received:	25 /1 /2023	Accepted:	29 /3/2023	Published:	31 /3 /2023

ABSTRACT

Background:

Due to the internet's recent rapid expansion, security has become a crucial issue when transmitting digital data via unsecure channels. This can be applied by employing dependable encryption methods. This research brought forward a text encryption system order to create safe databases.

Materials and Methods:

The research uses a chaotic map based on a logistic map Due to its widespread application in scientific research. Several processes are used to carry out the encryption activity. Firstly, the text is formatted in 2D matrix of numbers converted into vector. Secondly, to create a sequence for using it in the encryption process, the chaotic system is employed. Thirdly, sorting the generated vector in order to scramble the text values based on it. The final step involves encoding the scrambled text using a mathematical operation. Also, there are many steps used in the decryption process. In the first step, the same mathematical technique is used to decrypt the encrypted text after the identical chaotic sequence has been generated. In the second step, the scrambled values are descrambled to obtain the decrypted text.

Results:

The experimental results demonstrate that the suggested approach obtain an excellent value of entropy equal to (0.9955) and Correlation coefficient equal to (-0.0024) and Avalanche effect equal to (0.5120) as well as the proposed system examined under NIST tests and obtain a good results (>0.01) and examined for multiple other files and obtain a good results, in terms of execution time tests, the proposed system applied in a short amount of time.

Conclusion:

The proposed system matched the criteria for encryption techniques in terms of high sensitivity for initial values, high security, high randomizing Whatever text is to be encrypted. Also the proposed system can be applied for real time application due to its Short implementation time.

Key words:

Text encryption, chaotic maps, Chaos encryption, Text scrambling, Text diffusing.

مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية

info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com ISSN: 2312-8135 | Print ISSN: 1992-0652

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

الخلاصة

مقدمة:

نظرًا للتوسع السريع للإنترنت مؤخرًا، أصبح الأمان مشكلة حاسمة عند نقل البيانات الرقمية عبر قنوات غير آمنة. يمكن تطبيق ذلك من خلال استخدام طرق تشفير يمكن الاعتماد عليها. قدم هذا البحث نظامًا لتشفير النص لإنشاء قواعد بيانات آمنة.

طرق العمل:

يستخدم البحث خريطة فوضوية مبنية على خريطة لوجستية نظرا لتطبيقها الواسع في البحث العلمي، حيث يتم استخدام عدة عمليات لتنفيذ نشاط التشفير. أولاً، تم تنسيق النص في مصفوفة ثنائية الأبعاد من الأرقام المحولة إلى متجه. ثانيًا، لإنشاء تسلسل لاستخدامه في عملية التشفير، يتم استخدام النظام الفوضوي. ثالثًا، فرز المتجه الذي تم إنشاؤه من أجل خلط القيم النصية بناءً عليه. تتضمن الخطوة الأخيرة ترميز النص المخفوق باستخدام عملية حسابية. أيضًا، هناك العديد من الخطوات المستخدمة في عملية فك التشفير. في الخطوة الأولى، يتم استخدام نفس الأسلوب الرياضي لفك تشفير النص المشفر بعد إنشاء التسلسل الفوضوي المتطابق. في الخطوة الثانية، يتم تفكيك القيم الممزوجة للحصول على النص الذي تم فك تشفيره.

الاستنتاجات:

أظهرت النتائج التجريبية أن الطريقة المقترحة تحصل على قيمة ممتازة للإنتروبي تساوي (0.9955) ومعامل الارتباط يساوي (−0.0024) وتأثير الانهيار الجليدي يساوي (0.5120) وكذلك النظام المقترح الذي تم فحصه تحت اختبارات *NIST* حصل على نتائج جيده (< 0.01) وتم فحصها لعدة ملفات أخرى والحصول على نتائج جيدة، من حيث اختبارات وقت التنفيذ، تم تطبيق النظام المقترح في فترة زمنية قصيرة.

الكلمات المفتاحية:

تشفير النص، الخرائط الفوضوية، تشفير الفوضى، تشويش النص، نشر النص.

1. INTRODUCTION

The act of transmitting information via the Internet has become incredibly simple, quick, and beneficial as a result of the enormous advancements in technological communications and the growth of the internet's popularity. Attackers might attempt to access the sent data. These data may be faced to many illicit activities, such as copying, modification, sabotage, or theft, by employing clever software. As a result, the creation of a practical method for maintaining the security of this information—such as availability, confidentiality, and authenticity—became vital. The highest level of security is required, and that criterion is confidential. Encryption is one of the key methods used to safeguard information.

Encryption is the operation of reshaping data to a form that is difficult for unauthorized parties to decipher or understand Before data is transmitted across an insecure channel, the process of returning the data to a readable format is known as decryption and is the opposite of encryption [1]. There are many different kinds of encryption, including symmetric and asymmetric. In the asymmetric type, a private key is used, whereas, in the asymmetric type, a public key is used. Text

encryption is required in a number of applications, including communications, business, the military, banks, healthcare, and personal data. The most significant of these are DNA coding, elliptic coding, quantitative coding, chaotic coding, and coding systems based on mathematical equations, collectively referred to as mathematical coding [2]. As more encryption algorithms are developed, the idea of chaos is among the most important discoveries of the 20th century. At the moment, chaos and its applications play a significant role in many scientific domains, and many businesses have begun employing chaotic encryption as an alternative to the established technique Chaos can be used to achieve beneficial results or it can have undesirable effects, such as oscillations in chemical reactors. Most research projects concentrate on enhancing encryption quality, reducing execution, and increasing security robustness against assaults. Techniques based on chaos have outperformed more well-known ones for encryption. while additionally demonstrating their ability to meet greater security and privacy requirements through the use of changeable keys [3].

Cryptography based on chaotic dynamical systems is one of a large number of chaos applications. Dynamic systems with extremely complex behavior are used in chaotic cryptography. On the one side, the results of such systems appear random., while their acquisition is entirely deterministic. These factors have led to the usage of chaotic mappings in various fields, including data encryption. The technique employs scrambling and diffusion operations to defend against a chosen or known plain text assault. The process of scrambling involves altering the locations of image pixels according to the key. Diffusion is a process that modifies the image's pixel values. The outcome of the two procedures is a new, distinctively encoded text from the source text [4]. The goal of this paper is introduction effective and secure text encryption based on the chaotic system. The remainder of the paper is handled in the following manner: Related studies are included in Section 2. Section 3 provides preliminary information. In Section 4, the suggested encryption method is described. In Section 5, experimental findings and analysis are presented. Section 6 presents the conclusions.

2. RELATED WORKS

Early efforts on chaotic cryptography focused on text encryption, among other multimedia assets. More articles utilizing chaotic mappings to encrypt textual data have surfaced over time, including. However, chaotic mapping-based text encryption algorithms have lost their appeal to researchers in recent years.

In 2009, D. Yang and his research team presented a work that based on The iterating map with output-feedback-based encryption method. A 2D chaotic function that exhibits high degrees of chaotic activity and consistent bifurcation over many parameters to produce a random sequence that is utilized to encrypt the data coming in. The suggested solution makes use of a genetic algorithm to increase the security of any text data by optimizing the map's parameters [5].

In 2013, Ch. K. Volos and his research team suggested an approach using the Chaotic Pseudo-Random Bit Generator (CPRBG) based on a Logistic map. Textual content encryption was created by Volos and colleagues. The latter is built on two logistic maps running side by side, each

info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com ISSN: 2312-8135 | Print ISSN: 1992-0652

with distinct initial conditions and system parameters. The key benefit of this method in is how easily it can be implemented using the bit sequences' X-OR function [6].

In 2014, M. A. Murillo-Escobar his research team proposed symmetric text cipher algorithm based on chaos in a set of rules. They employed enhanced logistic maps with pseudo-random sequences and a 128-bit mystery key., plain text properties, and optimal permutation diffusion spherical in their approach. The technique showed quick encryption speed, although it only has a tiny parameter space [7].

In 2016, Ekhlas et al. and his research team suggested a block cipher and chaotic map-based method for text content encryption. Their approach principally relied on permuting and substituting the byte in the S-box to encrypt and decrypt an 8*8 bytes block. Their solution has low entropy and low security despite employing a lot of key space [8].

In 2017, S. J. Sheela and her research team suggested one of the chaos-based text encryption techniques by using a modified Henon map and Sine map, be taken into consideration. The steps of the encryption process are: converting the message to ASCII codes, Shuffling the ASCII codes, scanning the ASCII codes and XORing process. For various text data, the algorithm's encryption characteristics are confirmed [9].

In 2020, Ibrahim Y. and his reasech team suggested using perpetuation-based data encryption for both diffusion and confusion rounds. Media encryption is performed in a hybrid a chaos structure by mixing various maps. To create the control parameters for the permutation (shuffle) and diffusion (substitution) structures, blended chaotic maps are used. its advantages, which include necessary sensitivity and little lingering clarity[3].

In 2020, U. Menon and his reasech team used an algorithm to encrypt text that makes use of the chaotic map's inherent properties by employing the MS map as a keystream generator. The Bruce-force attack and known-plaintext assault have a very difficult time breaking the cipher text discovered by the purposed technique. The procedure for decryption has been a test was conducted utilizing three distinct secret keys (which are quite comparable to the secret key used in the encrypted process [10].

3. Preliminaries

3.1 Chaotic Map

Many different forms of mathematical models have been developed and explored in the past, when chaos theories were mostly studied. A control system for creating chaotic maps might be easy or complicated. A chaotic system's behavior can be seen in chaotic maps. The logistic map, the tent map, the quadratic map, and other well-known maps are examples of well-known maps. Any chaotic map has the mathematical definition given in equation (1) [11]:

$$x_{n+1} = f(x_n) \ , n = 1,2, \quad \text{...n} \quad \text{.... (1)}$$

info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com ISSN: 2312-8135 | Print ISSN: 1992-0652

ISSN: 2312-8135 | Print ISSN: 1992-0652
www.journalofbabylon.com | jub@itnet.uobabylon.edu.iq | info@journalofbabylon.com

Where x_n represents the iteration n state, the function f is the mapping of The state xn-1 to the state xn that follows

In this research We employed and concentrates on a logistic Map. logistic map equation is determining by the (2) [12]:

$$x_{n+1} = r - (x_n)2 \quad \text{.... (2)}$$

Where n denotes the number of iterations, this is the chaotic parameter, and x_n is a number between zero and one.

4. The Proposed System

The suggested system comprises of two key steps., called, encryption and decryption. The following is a list of their specifics:

4.1 Encryption Stage

There are various steps in this level. The general steps of the encryption process are shown in Figure 1.

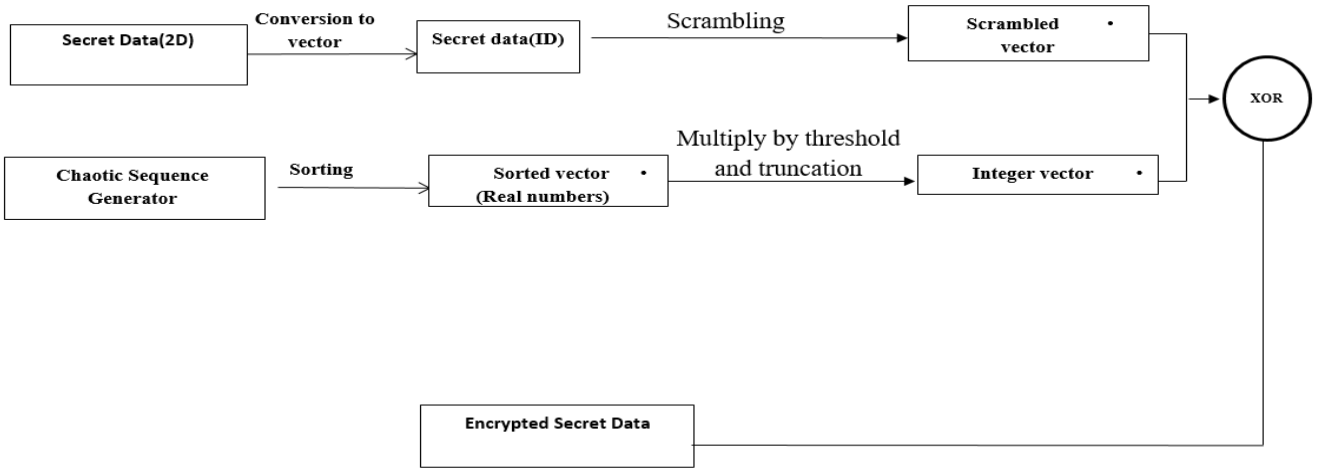

Figure (1): Secret Data encryption

The main steps of the encryption procedure are:

4.1.1 Chaotic Sequence Generator

In this step, the input secret data is transformed into a 1D vector (v- Data), and then the logistic chaotic system equation (2) is used to produce a chaotic sequence (Seq) of length equal to

info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com ISSN: 2312-8135 | Print ISSN: 1992-0652

(v-Data). The chaotic series contains real values in the range [0, 1], the steps of obtaining the random vector that used for encrypting the secret text as follows:

Step 1: Create a random sequence using the logistic map equation (2) to get the Chaotic _Seq vector.

Step 2: The secret data is transformed into a 1D vector (vec Data), and it is subsequently jumbled by shifting bits.It is crucial to carry out this operation by first sorting the newly produced Chaotic Seq in ascending (or descending) order, after which the bit location must be changed to match the matching indices of the New Sequence.

Figure (2) describe the steps of chaotic generators.

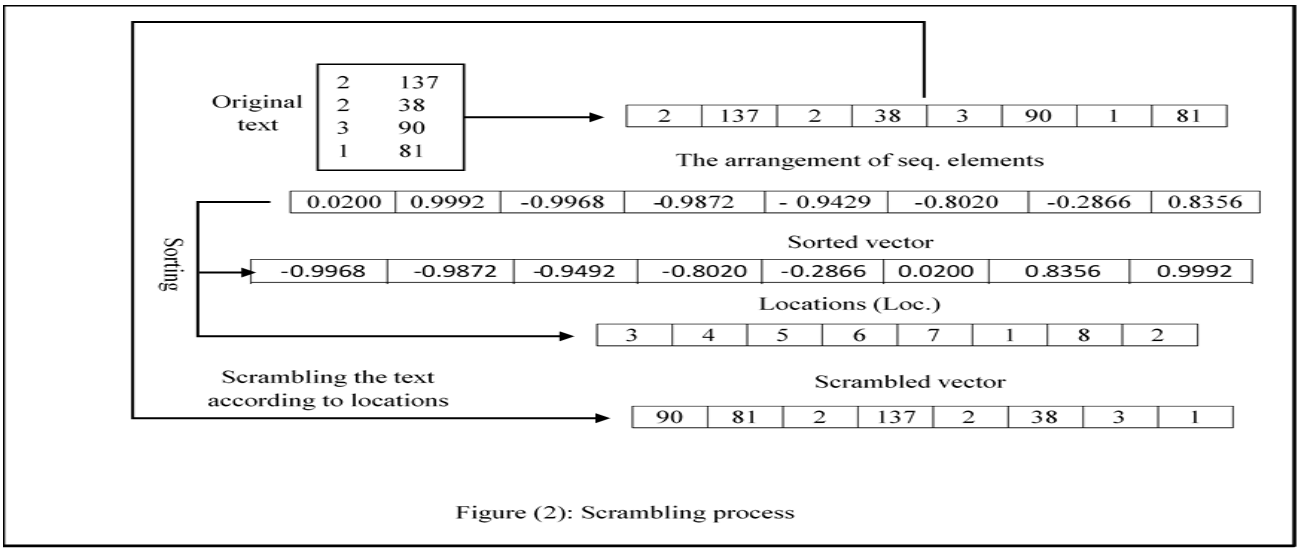

Figure (2): Scrambling process

4.1.2 Encryption

The chaotic sequence that was formed is employed to create the mask. that will afterwards have utilized in the encryption method. The first step is to construct the mask sequence element (Mask_ Seq) for each secret data piece utilizing the following equation:

$$Mask_{Seq(i)} = \|[\text{Chaotic\_Seq (i)}]\| \times n$$

$$\text{for i=1…length (text)} \quad \ldots, (3)$$

where n is a specific threshold, here we give n=1024

For encrypting the secret text, a mathematical operation is performed, we use the XOR operator between the Scrambled vector and Mask for getting encrypted secret data (ESD).

info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com ISSN: 2312-8135 | Print ISSN: 1992-0652

4.2 Decryption Stage

The reverse process of the encryption procedure is the decryption procedure. The suggested decryption method is displayed in Figure 3.

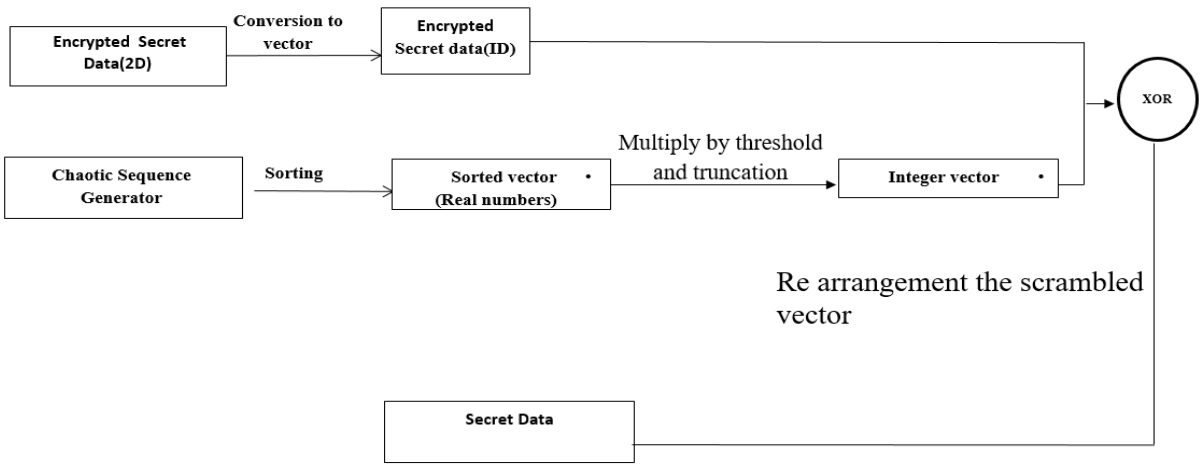

Figure (3): Secret Data Decryption

The receiver follows the same procedures as the sender did to recover the original text: sorting the random vector produced by the Chaotic Sequence Generator, performing the XOR operation as explained in section 4.1.1, and then applying Re arrangement to the scrambled vector that was produced.

5. Results and Discussion

The suggested effectiveness is evaluated text file of size 5,137 bytes containing numbers values ordered as 2D Matrix in terms of encryption and decryption processes and the level of security of it by using security measurements for testing the randomization of the algorithm.

5.1 Testing the encryption and decryption procedure

For understanding the suggested approach, suppose that we have a sample of the text (as shown in Figure 4.

2,137
2,29
2,138
1,67
2,31
1,160
1,68
6,112
.
.

Figure 4: sample of the plain text

On the sender side, the encryption process is carried out as follows:

1. Covert the plain text from 2D Matrix into vector (text (as shown in Figure 5)

2 137 2 29 2 138 1 67 2 31 1 160 1 68 6 112 . .

Figure 5: vector of plain text

2. Generate a random sequence by chaotic sequence generator of length equal of the plain text (as shown in Figure 6).

0.1000 0.3258 0.7951 0.5897 0.8759 0.8759 0.3935 0.8639 0.4256 0.8849 0.3686 0.8425 0.4804 0.9036 0.3153 0.7815 ……

Figure 6: generated random sequence

3. Sorting the generated random sequence as ascending order resulting the new sorted vector and the location vector that contains the old location of each value.

4. Scrambling the plain text according to the locations vector.

5. Creating a mask by applying each value of the sorted vector by 255 and truncation it for getting the integer values.

6. Encrypting the plain text by XORing the scrambled vector with the mask. The result of the encryption process is shown in Figure 9.

53 79 77 79 140 205 36 78 11 78 75 78 78 75 76 82 …..

info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com ISSN: 2312-8135 | Print ISSN: 1992-0652

Figure 7: Encryption process

7. Convert the result to 2D Matrix.
8. Send the cipher text to the receiver.

On the receiver side, the following activities are done

1. Receive the encrypted text and convert it into a vector.
2. Generate a random sequence and sort it.
3. Creating a mask by applying each value of the sorted vector by 255 and truncation it for getting the integer values.
4. Apply the XOR process to the encrypted text and the mask.
5. Apply the Re arrangement process for getting the decrypted vector.
6. Convert the vector to 2D Matrix for getting the original text.

The result of the decryption process is shown in Figure 10.

2,137
2,29
2,138
1,67
2,31
1,160
1,68
6,112
.
.

Figure 8: Decrypted text

5.2. Key Sensitivity Analysis

It is thought to be one of the most important measures for assessing encryption algorithms. It is employed to gauge an encryption system's sensitivity to even the slightest alteration to the secret key that is utilized for both encryption and decryption. The suggested approach encrypts the secret message displayed in figure 4 using the secret key value (x0=0.6). By modifying the secret key to (x0=0.6000001) and applied to the secret's decryption as shown in figure (9. d) which differs greatly from the original message (x0=0.6). That suggests that the proposed method is extremely sensitive to even the slightest alteration in the secret key.

info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com ISSN: 2312-8135 | Print ISSN: 1992-0652

2 137 2 29 2 138 1 67 2 31 1 160 1 68 6 112 . .

A. Original Message

53 79 77 79 140 205 36 78 11 78 75 78 78 75 76 82 …..

B. Encrypted Message with(x=0.6)

2 137 2 29 2 138 1 67 2 31 1 160 1 68 6 112 . .

C. Decrypted Message with(x=0.6)

96 237 158 45 246 247 236 241 418 127 921 161 298 386 2….

D. Decrypted Message with(x=0.6000001

Figure 9: key influencing on encryption and decryption process

5.3 Testing the security of the system

A few numerical values of the encrypted text are displayed to help determine whether the encryption algorithm complies with specific security standards. Measures associated with the suggested strategy including entropy, correlation coefficient, and avalanche effect should be used in text cryptanalysis. In addition to using National Institute of Standards and Technology (NIST) tests In order to gain assurance that recently created pseudo-random bit generators are cryptographically secure, These metrics are described in the subsections that follow, together with their explanations for the studied example.

All values of measurements are described in the Table (1) and Table (2)

5.3.1 Entropy

The information entropy measures the randomness of a system. With rising entropy, a system's level of unpredictability rises. Equation (4) can be used to define the information entropy H of a discrete random variable X with possible values of "x1, x2,..., xn," where p(.) is the probability mass function of X [13].

$$H(S) = -\sum_{i=0}^{N-1} p(s_i)\ \log_2 p(s_i) \ldots (4)$$

Where si represents the binary value and p(.) is the probability mass function of X and n is the number of binary values. the ideal value for entropy for the encrypted binary secret data should be (1) or a value close to (1).

5.3.2 Correlation coefficient (CC)

An essential statistical metric is the correlation coefficient (CC). Its value illustrates how the plain and encrypted texts differ from one another. When the correlation coefficient value is

info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com ISSN: 2312-8135 | Print ISSN: 1992-0652

close to 1, it indicates that there is a strong correlation between the two photos. As a result, the encryption system will be subject to attacks. The CC is assessed using equation (6)[13].

$$r = \frac{\sum_m \sum_n (A_{mn} - A^-)(B_{mn} - B^-)}{\sqrt{(\sum_m \sum_n (A_{mn} - A^-)^2 (\sum_m \sum_n (B_{mn} - B^-)^2}} \quad \dots (6)$$

Where A' and B' is the average of original text and encryption text respectively,

5.3.3 Avalanche effect (AE)

The Avalanche Effect explains how changes to the plaintext affect the cipher text for a strong cipher. The method produces a completely different output when the input is merely slightly changed. The effectiveness of diffusion is evaluated using this metric. A strong encryption algorithm should be capable of causing the output bits to change significantly following a modest change in the key or the plaintext should cause the cipher text to change significantly (approximately half of the output bits must fluctuate) [65]. determining the value of the (AE) is done According to equation (7)[14].

$$\mathrm{AE} = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} [(C(i,j) * C'(i,j)^2]}{M * N} \quad \dots (7)$$

Table (1): Security measurements values

Metric name	Value
Entropy	0.9955
Correlation coefficient	-0.0024
Avalanche effect	0.5120

As shown in table (1), the proposed text encryption is effective and provides a higher level of security.

5.3.4 The NIST tests

NIST Test is the collection of statistical tests was developed to assess the randomness of (arbitrarily long) binary sequences produced by hardware- or software-based cryptographic random or pseudorandom number generators. Eight tests of NIST are used for evaluating the proposed system including the Frequency test, Non-Overlapping Template Matching Test, Overlapping Template Matching Test, Linear Complexity Test, Cumulative Sums (Forward) Test, Cumulative Sums (Reverse) Test, Random Excursions Test and Random Excursions Variant. The significance value (P) indicated that the default value of the NIST tests indicated that the fraction of the sequence is random or not random based on the default value (0.01). The sequence is regarded as random if the P-value is greater than 0.01. Otherwise, if the P- value is less than 0.01, the sequence is considered as not random [15].

info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com ISSN: 2312-8135 | Print ISSN: 1992-0652

1. **Frequency Test (Mono bit):** Check to see if a sequence has roughly the same amount of ones and zeros as would be anticipated for a really random sequence.

2. **Non-Overlapping Template Matching Test:** Determine how frequently a specific non-periodic (aperiodic) pattern appears by counting the occurrences of predetermined target strings. The 68-bit aperiodic pattern 0 1 1 1 1 1 is an example.

3. **Overlapping Template Matching Test:** This test, like the last one, checks for instances of pre-defined target strings. This test shifts the test window by one byte when a match is made, whereas the prior test moved the test window to the end of the matching sequence.

4. **Linear Complexity Test:** This measures the linear feedback shift register's length (LFSR). A sequence's linear complexity is determined by how long the smallest linear feedback shift register (LFSR) produces the sequence. Longer LFSR's are a characteristic of random sequences. A too-short LFSR suggests non-randomness.

5. **Cumulative Sums (Forward and Reverse) Tests:** This test focuses on the random walk's maximum excursion (from zero), which is determined by the cumulative sum of the sequence's adjusted (1, +1) digits. The random walk's excursions for a random sequence must be close to zero.

6. **Random Excursions Test:** Test the number of cycles in a cumulative sum random walk that contains exactly K visits. The goal of this test is to ascertain whether the amount of trips to a specific state during a cycle differs from what would be predicted by a random sequence.

7. **Random Excursions Variant:** determine how many times a specific state is visited overall in a cumulative sum random walk. This test looks for variations from the predicted frequency of visits to different states in a random walk.

Table (2): NIST tests values

Test Name	p-value	Status
Frequency Test	0.23766913514378418	Random
Non-Overlapping Template Matching Test	0.015071913555110667	Random
Overlapping Template Matching Test	0.5300681304070924	Random
Linear Complexity Test	0.2769527106967955	Random
Cumulative Sums (Forward) Test	0.1088781721542848	Random
Cumulative Sums (Reverse) Test	0.6948466492938212	Random
Random Excursions Test(state='+1')	0.6948466492938212	Random
Random Excursions Variant(state='-1.0')	0.4652088184521418	Random

info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com ISSN: 2312-8135 | Print ISSN: 1992-0652

As shown in table (2), the results indicate that the generated algorithms have successfully completed the NIST-recommended tests, showing that their P-values are higher than the default P-value. As a result, there is a significant amount of randomness in the binary sequence produced by the developed algorithm.

5.3.5 Testing the Effectiveness of Chaotic Keys

To ensure the effectiveness of selecting the keys for the proposed encryption system in this work, several text files were taken and examined them in terms of security measurements. These are shown in figure 10. The results of experiments shown in table (4.14).

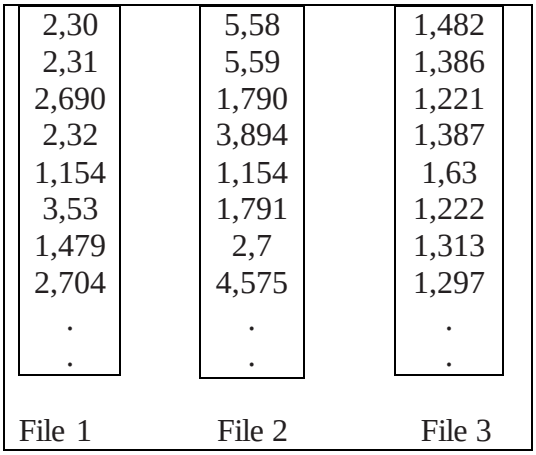

Figure 10: Tested files

Table (2): Security analysis for tested files

Test Name	File 1	File 2	File 3
Entropy	0.9992	0.9990	0.9988
Correlation coefficient	-0.0275	-0.0168	-0.0113
Avalanche effect	0.5204	0.5161	0.5143
Frequency Test	0.0012542153797004468	0.16957076893854925	0.0026908791992790956
Non-Overlapping Template Matching Test	0.7336197496183545	0.3117177898297621	0.29136936084421955
Overlapping Template Matching Test	0.07718381974119057	0.21902402109999833	0.11266235959071592
Linear Complexity Test	0.1843088471021681	0.35368829889182485	0.6797694863885718

info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com ISSN: 2312-8135 | Print ISSN: 1992-0652

Cumulative Sums (Forward) Test	0.8325158009071099	0.3089225013384137	0.0532051758089975
Cumulative Sums (Reverse) Test	0.8491450360846096	0.6999858358786277	0.6999858358786277
Random Excursions Test(state='+1')	0.7728299926844475	0.6170750774519739	0.22067136191984693

As shown in Table 3 the proposed encryption algorithm achieves a high level of security and randomize Whatever the type of text

5.4 Execution Time Analysis

One of the important factors for any encryption algorithm is the time Elapsed in encryption and decryption algorithm. By testing the execution time in seconds of the two processes for the message shown in figure 4 we obtaining the results shown in Table 4.

Table 4: Execution time analysis

Elapsed time in Encryption process	Elapsed time in Decryption process
0.007185	0.005907

As shown in Table 4 the execution time for both encryption and decryption processes is very little and approximate for real time applications.

6. CONCLUSION

In this work, we presented a powerful text-based encryption strategy to add another layer of security, that is based on chaos theory. There are a number of benefits to chaos theory, including the fact that it is one of the main issues in contemporary cryptosystems and that beginning conditions have a significant impact on it. Several processes of encryption are done for the encryption of the text, and the inverse operation from encryption is used for decryption. Based on the experimental results, the proposed chaos-based method prove that is very sensitive for changing the initial value, the proposed algorithm can be utilized send text data with excellent security that met the criteria for text security, achieve a high value of entropy very close to perfect value(1),very low value of Correlation Coefficient of negative value, good value for Avalanche effect as well as the proposed algorithm was tested by NIST tests of randomize and prove that the system has a sufficient amount of randomize and security for any type of text that examine for multiple texts, And the proposed method also examined under the execution time for it and prove that is has a very little time. Although the proposed method achieved excellent results in terms of security, it is limited that it lacks the sufficient complexity. Therefore, in future work, we shall propose another algorithm to be combined with the proposed method to increase the complexity.

info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com ISSN: 2312-8135 | Print ISSN: 1992-0652

info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com ISSN: 2312-8135 | Print ISSN: 1992-0652

Conflict of interests.

There are non-conflicts of interest.

References

[1] F. Maqsood, and M. M. Ali, "Cryptography: A Comparative Analysis for Modern Techniques", International Journal of Advanced Computer Science and Applications, vol.8,no.6,pp. 673-678, 2017.

[2] M. Popli, Gagandeep, "DNA Cryptography: A Novel Approach for Data Security Using Flower Pollination Algorithm", International Conference on Sustainable Computing in Science, Technology & Management, vol., no., pp.1-10,24 ,2019.

[3] I. Yasser, M. A. Mohamed, A. S. Samra, "A Chaotic-Based Encryption / Decryption Framework for Secure Multimedia Communications," pp. 1–23, 2020, doi: 10.3390/e22111253.

[4] N. Dwivedi , R. K. Gupta and S. Agarwal ,"Image Encryption using Curved Scrambling and Diffusion", International Journal of Engineering and Technology, December 2016, Vol 8 ,No 6,PP. 2990-2991 December 2016, DOI: 10.21817/ijet/2016/v8i6/160806262.

[5] D. Yang, X. Liao, and Y. Wang, "A novel chaotic block cryptosystem based on iterating map with output-feedback," vol. 41, pp. 505–510, 2009, doi: 10.1016/j.chaos.2008.02.017.

[6]] Ch. K. Volos, I. M. Kyprianidis, and I. N. Stouboulos, "Text Encryption Scheme Realized with a Chaotic Pseudo-Random Bit Generator",vol. 6, no. 4, pp. 9 – 14,2013.

[7] M. A. Murillo-Escobar , F. Abundiz-Pérez, C. Cruz-Hernández and R. M. López-Gutiérrez, "A novel symmetric text encryption algorithm based on logistic map," vol. 2, no. 1, pp. 0–4, 2014.

[8] E. A. Albhrany, L. F. Jalil, P. Hilal, and H. Saleh, "New Text Encryption Algorithm Based on Block Cipher and Chaotic Maps," vol. 2, no. 2, pp. 67–73, 2016.

[9] S. J. Sheela,K. V. Suresh,Deepaknath Tandur, "Secured text communication using chaotic maps",vol. 32, pp. 41–47,2017,DOI:10.1109/ICAMMAET.2017.8186653

[10] U. Menon, A. R. Menon,and A. Hudlikar "A Novel Chaotic System for Text Encryption Optimized with Genetic Algorithm," no. November, 2020, doi: 10.14569/IJACSA.2020.0111005.

[11] N. Ramadan, H. E. H. Ahmed, S. E. Elkhamy, and F. E. A. El-Samie, "Chaos-based image encryption using an improved quadratic chaotic map," *American Journal of Signal Processing*, vol. 6, pp. 1-13, 2016.

[12] M. Sharafi, F. Fotouhi-Ghazvini, M. Shirali, and M. Ghassemian, "A low power cryptography solution based on chaos theory in wireless sensor nodes," *IEEE Access*, vol. 7, pp. 8737-8753, 2019.

[13] H. Luo, B. Ge. " Image encryption based on Henon chaotic system with nonlinear term," *Multimed Tools Appl*, PP: 34323–34352 (2019). https://doi.org/10.1007/s11042-019-08072-4 .

[14] G. Patidar, N. Agrawal, and S. Tarmakar , " A block Based Encryption Model to improve Avalanche Effect for Data Security, " , *International Journal of Scientific and Research Publications* , Vol.(3) , No. 1 , January 2013.

[15] L. Hao and L. Min, "Statistical tests and chaotic synchronization based pseudorandom number generator for string bit sequences with application to image encryption," 2014, doi: 10.1140/epjst/e2014-02182-2.