© 2017 IJSRSET | Volume 3 | Issue 5 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

A Text Encryption Algorithm Based on Self-Synchronizing Stream Cipher and Chaotic Maps

Dr. Ekhlas Abbas Albahrani, Tayseer Karam Alshekly
Department of Computer Science, Mustansiriyah University, Baghdad, Iraq

ABSTRACT

A new text encryption algorithm which is based upon a combination between Self-Synchronizing Stream Cipher and chaotic map has been proposed in this paper. The new algorithm encrypts and decrypts text files of different sizes. First of all, the corresponding ASCII values of the plain text are served as input to the permutation operation which diffuses the positions of these values by using hyper-chaotic map. Secondly, the result values are input to substitution operation via1D Bernoulli map. Finally, the resultant vales are XOR feedback with the key.The proposed algorithm has been analyzed using a number of tests and the results show that it has large key space, a uniform histogram, low correlation and it is very sensitive to any change in the plain text or key.

Keywords : Text encryption, Chaotic map, Self-Synchronizing Stream Cipher, hyper-chaotic, Bernoulli map, Henon map

I. INTRODUCTION

Chaos theory reliably assumes a dynamic part in current cryptography. The primary point of interest of the chaos-based method lies on the arbitrary behavior and its effect on the initial conditions along with control parameters. A self-synchronizing or asynchronous stream cipher is a stream cipher where the key stream is a key function and a fixed number of previously encoded text characters. [1] proposed a novel symmetric text encryption algorithm based on chaos. They used a 128-bit secret key, two logistics maps with optimal pseudorandom sequences, original text properties, and only one permutation diffusions round. They presented in [2] a new symmetric key stream image encryption method, by using three 2D chaotic maps, recently proposed by authors, rather than one chaotic map. These maps are derived from some plain curves equations; their trigonometric forms ensure a large key space. The proposed method is a bi-modular architecture, in which pixels are mixed by the random permutation generated by using a new efficient algorithm and a diffusion phase, in which pixel values are changed by using a new XOR scheme. According to [3], a new image-encryption method based on a new chaotic system consists of joining two chaotic maps: the logistics map and the cubic map. This chaotic system is used to encrypt the components of R, G, B from a color image at the same time and the three components affect each other. They proposed in [4], the method that utilizes two 1-D logistic maps with different keys and a Tinker bell 2-D map. The chaotic sequence generated a mixed sequence from A and B of the Tinker bell map, depending on the chaotic sequences of the two logistics maps. In [5], a novel fast and secure encryption technique which uses the chaotic map function to generate the different multiple keys was proposed and it showed that negligible difference in parameters of chaotic function generates completely different keys as well as cipher text. [6] proposed new algorithm for text encryption based on block cipher and chaotic maps. This proposed algorithm is encrypted and it decrypted a block size of (8×8) byte. The nonlinear substitution is S-box component that was previously designed, this algorithm used 2d Logistic map and 2d Cross chaotic map. First, each block is permuted by using Standard map and then substituted by the bytes in S-box. The resulting block is then Xored with the key. The proposed random key generator is based on Tent map to generate the key sequences that are used in the encryption and decryption process.

In this paper, a new chaotic and Self-Synchronizing Stream Cipher encryption / decryption system for text is suggested. The proposed algorithm consists of three operations which are implemented based on the chaotic system. These three operations are used to add the diffusion and confusion properties to stream cipher.

The remaining part of the paper is sorted out as follows: Section 1 presents the basic theory of the Self-Synchronizing Stream Cipher and chaotic functions; Section 2 explains the key generation method, Section 3 introduces the proposed algorithm and Section 4 presents the statistical and security analysis of the proposed algorithm.

II. METHODS AND MATERIAL

1. Basic theory

In this paper, Self-Synchronizing Stream Cipher and three chaotic maps have been used, and they are: hyper-chaotic, 1D Bernoulli map, and 2D Henon map.

1.1 Self-Synchronizing Stream Cipher

Self-Synchronizing stream cipher was developed from SOBER which was suggested by Rose in1998. This cipher is designed to generate a secret key of up to 128 bits. It also provides message encryption, message integrity, or both [7]. In a Self-Synchronous Stream Cipher (SSSC), the key stream only relies on the key and on a limited number of the last cipher text symbols as shown in figure 1 [8].

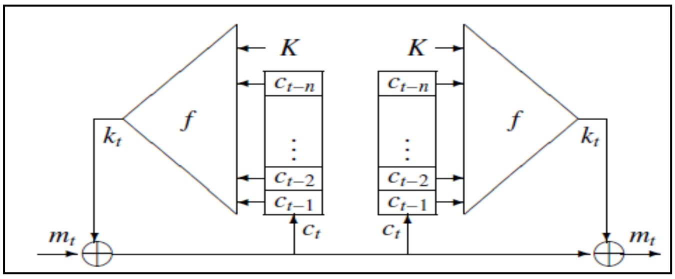


Figure 1: Self Synchronizing Stream Cipher model

where m_t represent the original message, k_t represent key stream, f represent the function of key stream generator and c_t represent the cipher text

1.2. Hyper-chaotic system

A hyper-chaotic system that is generated from Chen's chaotic system consists of 4D and was modeled by [9]:

$$\begin{cases} x_1 = a * (x_2 - x_1) \\ x_2 = -x_1 * x_3 + d * x_1 + c * x_2 - x_4 \\ x_3 = x_1 * x_2 - b * x_3 \\ x_4 = x_1 + k \end{cases} \qquad (1)$$

Where a, b, c, d and k are parameters, when a=36, b=3, c=28, d=-16, and -0.7 ≤ k ≤ 0.7 then the system is hyper-chaotic.

1.3.1D Bernoulli map

Bernoulli map is one dimensional and is described as follows [10]:

$$x_{n+1} = \begin{cases} r * \ x_n + 0.5 \,; \ x_n < 0 \\ r * x_n - 0.5 \,; \ x_n \ \geq 0 \end{cases} \qquad (2)$$

Where $-0.5 < x_n < 0.5$ and $1.2 < r < 2$.

In this paper, the Bernoulli map has been normalized in a directed manner by exchanging the x rang ($-0.5 < x < 0.5$) in equation (2) into new rang ($0 < x \leq 255$) and the map becomes:

$$x_{n+1} = \begin{cases} r * \ x_n + 128 \,; \ x_n < 128 \\ r * x_n - 128 \,; \ x_n \ \geq 128 \end{cases} \qquad (3)$$

1.4. 2D Henon map:

Henon Map was first discovered in 1978, which is described in following equation [11]:

$$\begin{cases} y_{n+1} = 1 - a * \ y_n^2 + z_n \\ \quad z_{n+1} = b * z_n \end{cases} \quad (5)$$

The system has two control parameters a and b, and the system will show chaotic behavior when (a=1.4, b=0.3).

2.key generation:

The key stream for the proposed algorithm is generated by using the Chaotic Key Stream Generator (CKSG) that has been previously designed in [12]. CKSG is designed based on 3D Henoun map and 3D Cat map. In the proposed algorithm, the key generation algorithm consists of the following steps:-

1- Inputting the initial parameters (x_0, y_0, z_0, v_0) for CKSG, which are floating point numbers where the precision is 10^{-16}.

2- The CKSG generates the key stream that will be used for encryption and decryption algorithm.

3- The initial parameters(x_0, y_0, z_0, v_0) are changed by using simple Xor operation as shown in the following equations:

$$\begin{cases} Newx_0 = x_0\ Xor\ v_0 \\ Newy_0 = y_0\ Xor\ v_0 \\ Newz_0 = z_0\ Xor\ v_0 \end{cases} \qquad (6)$$

The resulting values are used as new initial parameters for CKSG in order to generate the necessary parameters for the permutation and substitution operations in the proposed encryption algorithm.

3.The proposed algorithm:

The proposed stream text encryption algorithm consists of two major algorithms: encryption algorithm and decryption algorithm. Each algorithm has four main operations, these are:-

1- Key generation operations.
2- Permutation operations.
3- Substitutions operations.
4- XOR Feedback operation.

Each step will be described in details in the next section.

3.1 Encryption algorithm:

The main steps of the proposed stream text encryption algorithm are: -

Step 1: Plain text file is imputed where ASCII values of the plain text characters are stored in a one dimensional array called N.

Step 2: Initial parameters (x_0, y_0, z_0, v_0) are imputed for CKSG to generate the key stream for permutation operations, substitutions operations and XOR Feedback operation. These parameters numbers are floating point numbers with precision of 10^{-16} and they are considered as the keys of the algorithm.

Step 3: The following three operations are performed on the array N:

1- Permutation operation:

- ✓ Hyper-chaotic map equation (1) is iterated 50 times and the results are ignored in order to eliminate the transient effect of chaotic map.
- ✓ Hyper-chaotic map is iterated for number of times equals to the size of N. In each iteration, the four floating point outputs are converted to the four integer numbers in the range [1…N]. These numbers represent the new positions that will be used to permute the original array N.
- ✓ The original array N is permuted by using the resulting new positions.

2- Substitutions operation: Each byte in the permuted array is substituted by a new byte in the following way:

- ✓ Each byte of permuted array is imputed to the 1D Bernoulli map equation (2).
- ✓ The output from 1D Bernoulli map is XORed with position number of the current byte.
- ✓ These two steps are repeated on all permuted array.

3- XOR Feedback operation: is performed on the substituted array in the following way:

- ✓ The first byte in the resulted substituted array is XORed directly with the first byte of key.
- ✓ The remaining bytes in the substituted array are XORed with key bytes in the following way:
  - o 2DHenon map is iterated four times. The four resulting floating point numbers are converted into four integer number in the range [0…7], which represent the positions of different four-bits in byte.
  - o A new key byte is generated by XORing the four bit in previous cipher text byte and four bits in current key byte where their positions are determined in the previous step
  - o The new key byte is Xored with the byte in the substituted array. The result is a cipher text byte.

3.2. Decryption algorithm:

The text decryption algorithm is a reverse of text encryption algorithm where each operation can easily be reversible.

- ✓ Reverse XOR Feedback operation is the same operation in encryption algorithm where it is performed by XORing the encrypted array to the same key.
- ✓ Reverse Substitutions operation is performed in the same way as in the encryption algorithm, but the inverse of 1D Bernoulli map is used.

In reverse permutation operation, Hyper-chaotic map is iterated in the same way as in encryption algorithm, where each position defined by Hyper-chaotic map will be used as index to return byte in encrypted array to its original position.

III. RESULTS AND DISCUSSION

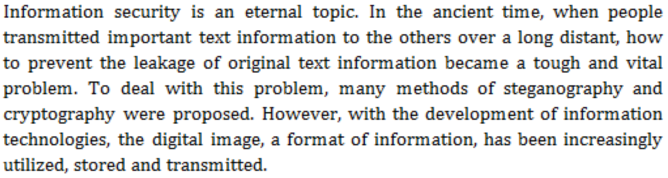
Experiment result:

The proposed algorithm is implemented using visual basic. Net programming language and the tests are performed on a Laptop with an Intel (R) Core(TM)2 Duo CPU T8100 @2.10 GH and 2 GB RAM .

The Security Analysis:

Key space analysis: -An ideal text encryption algorithm should have large key spaces. A key space size smaller than 2^{128} is not secured enough [13]. The proposed algorithm has a secret key with key space of 2^{213} that is sufficient and adequate to resist brute-force attack according to the computing power of the current PCs. Here, key space is constructed form the parameters required for generating keys (initial valuesx_0, y_0, z_0, v_0), these parameters are floating point numbers, where each one belongs to [-1.18, 1.5]. If the precision of each parameter is 10^{-16}, the total space of keys is 2^{213} $((10^{16})^4)$. The key space is adequate enough, far reaching to contradict an extensive variety of brute-force attacks.

Key Sensitivity Analysis :- Adecent cryptosystem should be delicate to the secret keys; this suggests that 2 cipher texts is generated with small different secret keys needed to be altogether completely different. The plaintext of size 490 characters is as follows:-



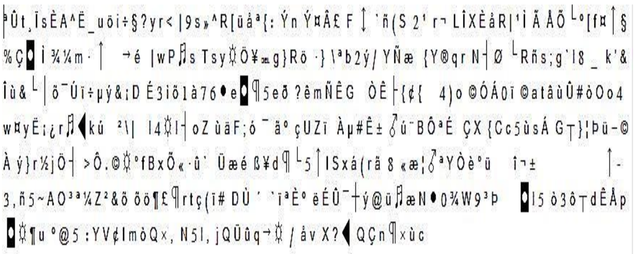
Information security is an eternal topic. In the ancient time, when people transmitted important text information to the others over a long distant, how to prevent the leakage of original text information became a tough and vital problem. To deal with this problem, many methods of steganography and cryptography were proposed. However, with the development of information technologies, the digital image, a format of information, has been increasingly utilized, stored and transmitted.

This plain text is encrypted by using two keys with very small difference as shown:

Key 1:

X_0=1.5389241520346711
Y_0=-0.9275413174568903
Z_0=0.3489512706410170
V_0=1.8234567891011124

The resulting cipher text is as follows:

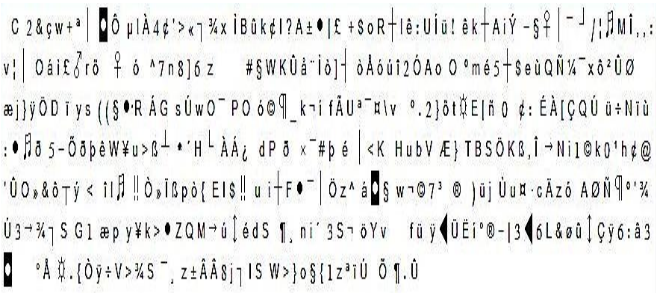


```
|ªÛt¸ÏsÈA^Ë_uöi÷§?yr<|9s»^R[üåª{: Ýn Ý¤Â£ F ↕ `ñ(S 2¹ r¬ LÎXÈåR|¹Ì Ã ÅÕ └°[f¤↑§
%Ç◘ Ì ¾¼m· ↑   →é |wP♫s Tsy☼Ö¥▬g}Rö ·} \ªb2ý/ YÑæ {Y®qr N┤ Ø └Rñs;g`I8 _ k'&
Îù& └| õ¯Úï÷µý&¡D É3iõ1à76•e◘¶5eð ?êmÑÊG  ÒÊ├{¢{  4)o ©ÓÁ0ï ©atâùÛ#òOo4
w¤yË¡¿r♫◄kú  ²\|  I4☼I┤oZ ùäF;ó ¯ ä° çUZï Àµ#Ê± ♂ú¨BÔªÉ ÇX {Cc5ùsÁ G┬}¦þü-©
À ý}r½jÖ┤ >Ô.©☼°fBxÕ«·û` Üæé ß¥d¶ └5↑ISxá(rã 8 «æ¦♂ªYÒè°ü   î¬±          ↑-
3,ñ5~AO³ª¼Z²&õ öö¶£¶rtç(ï# DÙ ´ `ïªÈ° ëÉÛ¯┼ý@ü♫æN•0¾W9³Þ   ◘I5 ò3ô┬dÊÅp
◘☼¶u °@5 :YV¢ImòQ×, N5I, jQÜûq→☼ / åv X?◄ QÇn¶×ùc
```

Key 2:

X_0=1.538924152034671**2**
Y_0=-0.927541317456890**4**
Z_0=0.348951270641017**1**
V_0=1.823456789101112**5**

The resulting cipher text is as follows:



```
C 2&çw+ª| ◘Ô µIÀ4¢'>«┐¾x İBûk¢I?A±•|£ +$oR┼lê:UÍü! êk┼AiÝ -§♀|¯┘/¡♫MÎ,,:
v¦| OáI£♂rõ  ♀ ó ^7n8]6z    #§WKÛå¨Ìò]┤ òÅóúî2ÓAo O °mé5┼$eùQÑ¼¯xô²ÛØ
æj}ÿÖD ï ys ((§•·R ÁG sÚwO¯ PO ó©¶_k¬i fÃUª¯¤\v °.2}öt☼E|ñ 0 ¢: ÉÀ[ÇQÚ ü÷Nïù
:•♫ð 5-ÕðþêW¥u>ß┴ •´H └ ÀÁ¿ dP ð ×¯#þ é |<K HubV Æ} TBSÖKß,Î→Ni1©k0¹h¢@
'ÛO»&ô┬ý < î1♫ ‼Ò»Ïßpò{ EI$‼ u i┼F•¯|Öz^ á◘§ w¬©7³ ® )üj Ùu¤·cÄzó AØÑ¶°'¾
Ú3→¾┐S G1 æp y¥k>•ZQM→ú↕édS ¶¸ ni´ 3S¬ öYv   fü ÿ◄ÜËí°®-|3◄6L&øû↕Çÿ6:â3
◘   °Å ☼.{Òÿ÷V>¾S ¯¸ z±ÂÂ8j┐IS W>}o§{1zªïÚ Õ ¶.Û
```

The cipher text with inaccurate key does not demonstrate any data related with plaintext, hence the proposed algorithm is sensitive to secret key, the correlation of the two cipher text is equal to (-0.0215), this means the two cipher text are different.

Statistical Attack Analysis:

The statistical analysis of the encrypted image and plaintext can be considered by:

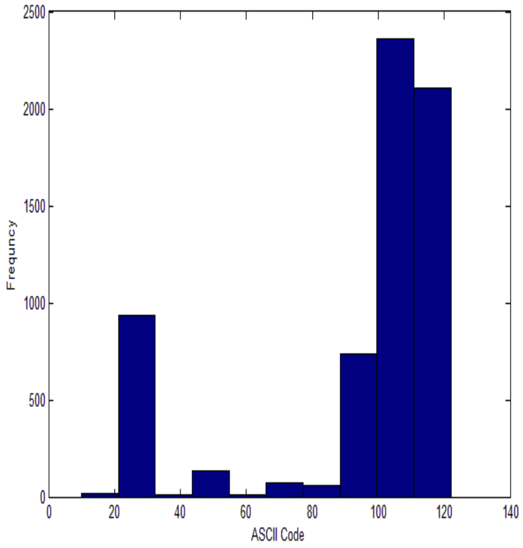
- ✓ Histogram analysis: - this indicates how constantly a conception shows up in the content. The histogram can tackle information on the plaintext, the closeness to one chest key or both. On the instance that the histogram of the all images in figure content is reasonably equally circulated over the scale, no data about the plaintext can be accumulated through histogram examination. The histogram of the plaintext of size 6439 characters and its cipher text are shown in Figure (2). The cipher text histogram is uniform and does not indicate any information about the original plaintext, so the proposed scheme is powerful against histogram attacks in addition to frequency attacks.

✓ Correlation coefficient analysis: - Correlation assessment checks the relationship between plaintext and cipher text. The correlation distribution of two horizontally adjacent bytes in the plaintext of size 6439 characters and its cipher text are shown in Figure (3). This Figure shows that the correlation distribution of cipher text is uniform as compared with the plain text. Table (1) shows the results of correlation coefficient of 10 plaintext and its cipher text files with different sizes. These results indicate that the correlations between the plaintext and its cipher text are very small.

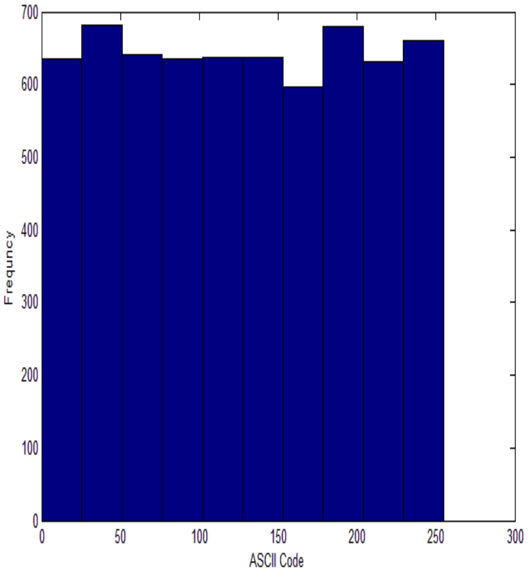
Differential attack analysis:

To implement plaintext sensitivity examination, a rival may attempt to build up a relationship between the plain text and its cipher text by watching the impact of a slight change on the overall encryption output. With the assistance of different examination strategies, the secret key might be acquired. This type of cryptanalysis turns out to be practically infeasible if such a slight change can be adequately diffused to the entire ciphered text. There are two measurements to decide this robustness [14].

✓ NPCR (Net Pixel Change Rate): - it measures the quantity of characters that are different between two cipher texts C1 and C2 from two analogous plaintext; the value of NPCR is represented in percentage, where 100% means that both cipher texts are totally different. The NPCR is calculated with:



(a)



(b)

Figure (2): Histograms of: a) plaintext and b) cipher text

Table 1: the result of correlation between text file

File name	Correlation	Size of file in byte
Plaintext1 & ciphertext1	0.0067	5116
Plaintext2 & ciphertext2	0.0034	5479
Plaintext3 & ciphertext3	0.0058	7278
Plaintext4 & ciphertext4	0.0167	3595
Plaintext5 & ciphertext5	0.0046	4001
Plaintext6 & ciphertext6	-0.0136	12109
Plaintext7 & ciphertext7	-0.0335	2786
Plaintext8 & ciphertext8	-0.0008	6439
Plaintext9 & ciphertext9	0.0092	11260
Plaintext10 & ciphertext10	0.000001	8279

$$\mathrm{NPCR} = \sum_{i=1}^{N} \frac{w(i)}{N} * 100\% \qquad (7)$$

Where N is the text length and

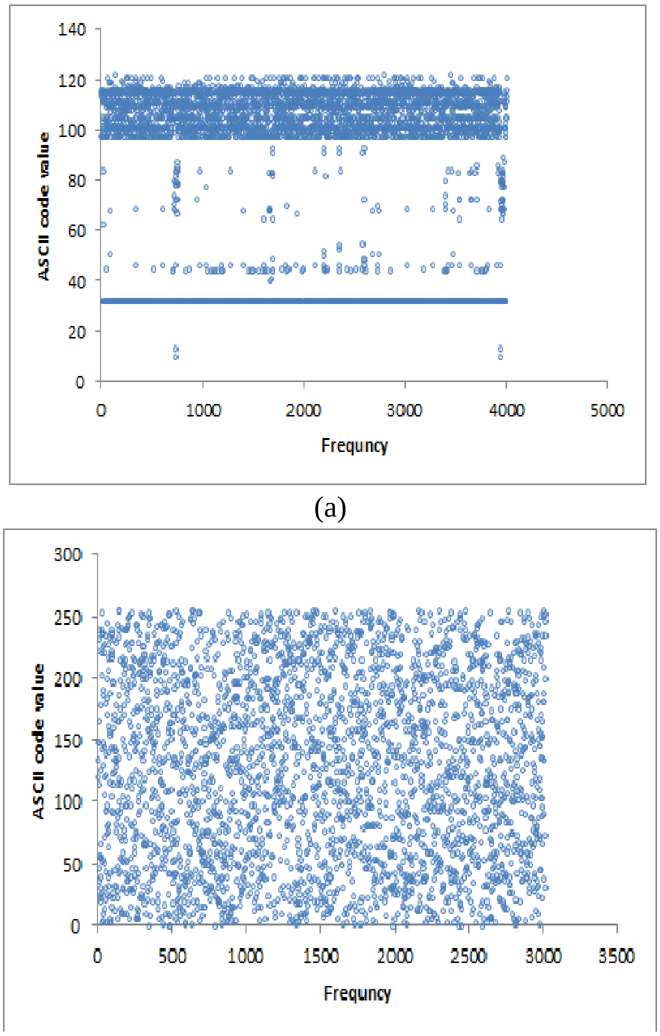
$$w(i) = \begin{cases} 0, \text{if } C1(i) = C2(i) \\ 1, \text{if } C1(i) \neq C2(i) \end{cases} \qquad (8)$$

Where C1 (i) and C2 (i) are the symbol values of the cipher text C1 and C2.

- UACI (Unified Average Changing Intensity): - it is the intensity difference average between two cipher texts C1 and C2.The UACI is calculated as follows:

$$\mathrm{UACI} = \frac{100}{\mathrm{N}} * 95 \sum_{\mathrm{i}=1}^{\mathrm{N}} |\mathrm{C1} - \mathrm{C2}| \qquad (9)$$

Table 2 demonstrates the result of NPCR and UACI. These results are very close to ideal values of NPCR and UACI which means that the proposed algorithm is robust against differential attacks. In addition, these results show that a small change in the original image will result in a great change in the encrypted image; this implies that the proposed algorithm has an excellent capability to resist the differential attack.



(a)

(b)

Figure 3 : Correlation analyses: a) plaintext correlation b)cipher text correlation.

Table 2: The results of UACI and NPCR

File name	NPCR	UACI
Ciphertext1	98.87643	32.658
Ciphertext2	98.67433	33.067
Ciphertext3	99.55001	33.143
Ciphertext4	99.05432	33.674
Ciphertext5	98.76534	32.775
Ciphertext6	98.60068	32.754
Ciphertext7	99.26086	33.077
Ciphertext8	99.64341	33.214
Ciphertext9	99.17743	33.430
Ciphertext10	99.45088	33.601

Information Entropy Analysis:

The encryption process must generate an unpredictable message, similar to noise, and with high disturbance. These characteristics are checked with the information entropy examination: the higher entropy, higher disturbance in the encoded text. In contrast, if the encryption process is not sufficiently random, low entropy and the cryptographic algorithm can be responsible for the entropy attack, because there is a certain level of predictability of the encryption technique.The entropy H (m) of a message m can be calculated as follows [15]:-

$$H(m) = \sum_{i=1}^{2^{n-1}} p(m_i) \log 2 \frac{1}{p(m_i)} (10)$$

Where N is the number of bits of the message m, 2^N means all possible symbols, $p(m_i)$ represents the probability of m_i and the entropy is expressed in bits. If a message is encrypted with 2^N possible symbols, the entropy should be H(m) = N ideally. Table (3) demonstrates the result of entropy analysis of 10 text files. These results are very close to ideal values of entropy, which means that the proposed algorithm is robust against entropy attacks.

Table 3: Results of entropy analysis of the proposed algorithm

The ciphertext	Entropy
Ciphertext1	7.9630
Ciphertext2	7.9699
Ciphertext3	7.9761
Ciphertext4	7.9485
Ciphertext5	7.9579
Ciphertext6	7.9877
Ciphertext7	7.9227
Ciphertext8	7.9703
Ciphertext9	7.9809
Ciphertext10	7.9785

IV. CONCLUSION

A self-synchronizing or asynchronous stream cipher is a stream cipher where the key stream is a key function and a fixed number of previously encoded text characters, but it has little diffusion and confusion. The proposed text encryption algorithm increased this property by the combination of a Self-Synchronizing Stream Cipher and chaotic map .The main idea is to encrypt and decrypt a text file of any size based on permutation, substitution and XOR feedback operation. Security analyses indicate that the proposed algorithm has desirable properties such as the key space analysis, statistical attack analysis and differential attack analysis that are performed numerically and visually. All the experimental results showed that the proposed encryption scheme is secure because of its large key space; it is highly sensitivity to the cipher keys and plaintext. All these agreeable properties make the proposed algorithm a potential possibility for encryption of multimedia data such as images, audios and even videos.

V. REFERENCES

[1]. M. A. Murillo-Escobar, F. Abundiz-Perez, C. Cruz-Hernández, R. M. López-Gutiérrez “A novel symmetric text encryption algorithm based on logistic map", Proceedings of the 2014 International Conference on Communications, Signal Processing and Computers,215

[2]. R. E. BORIGA, A. C.DĂSCĂLESCU, and A. V. DIACONU" A New Fast Image Encryption Scheme Based on 2D Chaotic Maps", IAENG International Journal of Computer, 30 November 2014

[3]. N.F.Elabady , H.M.Abdalkader, M. I. Moussa ,S. F. Sabbeh" Image Encryption Based on New One-Dimensional Chaotic Map ", IEEE,2014

[4]. G.Hanchinamani, L.Kulakarni" A Novel Approach for Image Encryption based on Parametric Mixing Chaotic System", International Journal of Computer Applications, Volume 96, June 2014

[5]. A.A. Khare, P. B. Shukla and S. C. Silakari" Secure and Fast Chaos based Encryption Systemusing Digital Logic Circuit", Computer Network and Information Security,vol 6,2014

[6]. E. A. Albhrany, Dr. L.F. Jalil, Prof. Dr. H. H. Saleh" New Text Encryption Algorithm Based on Block Cipher and Chaotic Maps", IJSRSET, Vol 2, 2016

[7]. TAYSEER S. ATIA," DEVELOPMENT OF A NEW ALGORITHM FOR KEY AND S-BOX GENERATION IN BLOWFISH ALGORITHM", Journal of Engineering Science and Technology, Vol. 9, No. 4 (2014).

[8]. P.Guillot and S.Mesnager," Non-Linearity and Security of Self Synchronizing Stream Ciphers", International Symposium on Nonlinear Theory and its Applications, 2005

[9]. T.Gao , Z. Chen ,"A new image encryption algorithm based on hyper-chaos",Elsevier,2008

[10]. Sheela S.and S. V. Sathyanarayana “Application of chaos theory in data security-a survey",ACCENTS Transactions on Information Security,Vol 2(5), 2017.

[11]. K.Singh, K. Kaur" Image Encryption using Chaotic Maps and DNA Addition Operation and Noise Effects on it", International Journal of Computer Applications, Volume 23, June 2011

[12]. Dr. E.A. Albhrany, T.K. Alshekly"A New Key Stream Generator Based on 3D Henon map and 3D Cat map",International Journal of Scientific & Engineering Research,Volume 8, Issue 1, January-2017

[13]. W. Liu , K. Sun, C.Zhu “A fast image encryption algorithm based on chaoticmap",ElsevierLtd,2016

[14]. C.Fu , J.B. Huang , N.N. Wang , Q.B. Hou and W.M.Lei “A Symmetric Chaos-Based Image Cipher with an Improved Bit-Level Permutation Strategy",entropy,2014, 16

[15]. M.A. Murillo-Escobar , C. Cruz-Hernández, F. Abundiz-Pérez , R.M. López-Gutiérrez “Implementation of an improved chaotic encryption algorithm for real-time emb e dde d systems by using a 32-bit microcontroller",Elsevier,2016