ISSN 2278-3091

Volume 10, No.2, March - April 2021

International Journal of Advanced Trends in Computer Science and Engineering

Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse831022021.pdf

https://doi.org/10.30534/ijatcse/2021/831022021

Security Threat Detection and Cryptanalysis of Dynamic and Random S Box Based Two-Fish Algorithm

Sreeparna Chakrabarti[1], Dr. G N K Suresh Babu[2]

[1]ResearchScholar,Department of MCA, Visvesvaraya Technological University, Belgaum

[1]AssistantProfessor,Department of Computer Science, Kristu Jayanti College, Bengaluru

chakrabartisreeparna@gmail.com

[2]Professor,Department of CSE, Prince Dr. K. Vasudevan College of Engineering and Technology, Chennai

gnksureshbabu@gmail.com

ABSTRACT

In this modern era, computer vision techniques are widely being used for the diagnosis of various diseases in healthcare applications. Wireless techniques are popularly employed for the transfer of these medical data. Security issues are the major issues faced by these techniques during the transfer of medical data. Cryptanalysis techniques provide analytic examination of various defects in the cryptographic algorithms using which an attacker may break and detect the data. These techniques ensure the robustness and reliability of the cryptographic systems. In this work, we have performed cryptanalysis of Dynamic and Random S-Box (DRSB) Generation Algorithm. Analysis was carried out using various aspects like histogram, correlation, entropy, sensitivity and key space. This analysis is crucial as medical data contains sensitive information and hence ensuring the reliability of the cryptographic algorithm is mandatory. It was shown that the DRSB algorithm achieves very good performance in terms of all the analysis techniques. In addition, we also provide a threat detection system to protect the framework against the manipulation of data during its transmission. Any changes caused in medical data, can cause changes in the medical treatment and can lead to serious damage or even to death of the patient. Hence, identification of data manipulation is essential in health care applications. In this work, SHA-512 algorithm was utilized to generate a message digest using which the protection and authentication of data was ensured.

Key words: Correlation, Cryptanalysis, entropy, SHA-512, two-fish.

1.INTRODUCTION

Achievement of security during the real time transfer of health care data has become a trending research area. These healthcare applications involve huge amount of patient data. These data are often transmitted to various locations using wireless techniques to aid in remote treatment. This data transfer has resulted in tremendous security concerns since the information carried by this data is very important and confidential. Hence, design of effective encryption system to encrypt the health care data is vital. Many systems have been proposed in the literature to ensure the protection of healthcare data[1].

Chaotic systems are widely used in cryptographic frameworks since they have various advantages like ergodicity, randomness and deterministic nature [2][3]. The random sequence generated by these maps are used for the encryption of data[4][5]. S-box is a popularly used traditional block encryption system. This scheme has very good cryptographic features and is highly resistant to attacks. However, the only drawback of this system is its static nature. Recently, may researchers have combined the random nature of chaotic systems with the S-box structure to achieve robust encryption schemes.This system achieved high entropy value of 7.956. The time taken for encryption and decryption using this scheme was 1.67s and 1.30s respectively [6]. Cryptanalysis is an important step to ensure the reliability of encryption algorithms. A scheme for cryptanalysis of a combined chaos system has been proposed. The proposed encryption scheme involved the combination of SHA-512 algorithm and four-dimensional hyper chaotic system. This scheme was designed to solve the issues of image insensitivity. It was implemented using seven different system parameters. This scheme attained a maximum Lyapunov exponent value of 25.62. The performance analysis revealed that this framework achieved a key space of 2^{548}. Also, the pixel correlation was found to be 0.00032 [7].

2.LITERATURE SURVEY

Bashir et al. [8] has proposed a scheme for image encryption based on chaotic state variables. A four-dimensional dynamic scheme was employed that utilized a hyper-chaotic system. The main advantage of this method was its high speed. This high-speed feature was achieved since only few iterations were used by the dynamic system. Here, the plain image was initially subject to confusion. This image was then permuted using the key sequence generated by hyper-chaotic maps. Finally, the permuted image was subject to diffusion to obtain the cipher image. Liu et al. [9] has presented a system using dynamic S-box for the encryption of images. In this work, a new hyper-chaotic framework that has very high values of Lyapunov exponent was proposed. The sequences obtained from this chaotic system was used for performing permutation and substitution of the pixel values in the plain image. Affine transformation was used to create dynamic effect in the S-box structure. The Lyapunov exponent achieved by this system was about 2.256. Similarly, this scheme achieved a value of 0.500017 in the avalanche effect analysis.

Banik et al.[10] has designed a technique for the encryption of multiple medical images using elliptic curve cryptosystem. This encryption was performed using pseudo random number generator using Mersenne Twister system. The cartesian space coordinates were employed for scrambling the data. This system achieved high execution speed since the number of calculations was minimized. This system was used for encrypting multiple images like CT, MRI, X-Ray, etc., simultaneously. Kumar et al. [11] used discrete cosine transform (DCT) for the medical image encryption. This framework was employed using two levels. In the first level, the fractional DCT was applied over the medical images. In the second level, the coefficients of fractional DCT were subject to chaotic maps. This scheme produces robust results compared to the fractional Fourier transform. The analysis based on key sensitivity and key space showed that this scheme produced good encryption for the medical images.

Priya et al. [12] introduced a scheme that produced encryption along with watermarking of medical images. Encryption algorithms are used for encrypting the watermarked images. A new visual encryption technique was proposed in this paper, in which, integer wavelet transform (IWT) was utilized. Initially, the images are watermarked. These watermarked images are then split into low and high frequency sub-bands. The reference image was subject to IWT. The low frequency coefficients were combined using inverse IWT and the finger print of the doctor was combined with the high frequency coefficients of the reference image. Lima et al. [13] presented a model for the encryption of 3-dimensional medical images. A cosine number transform (CNT)based model was proposed in this paper. Here, the input images were first divided into cubic blocks. Each block was encrypted using a secret key to obtain the intermediate image. Arnold map was used for further encryption of the intermediate image. Finally, inverse transform was used to obtain the encrypted image.

3.CRYPTANALYSIS OF DYNAMIC AND RANDOM S BOX BASED TWO-FISH ALGORITHM

a. Proposed Dynamic and Random S-box model

We have proposed a novel algorithm for the generation of Dynamic and Random S-box (DRSB). In this algorithm, the contents of the S-box tables are shuffled based on the 32-bit sub-keys. Thus, we create sub-key-dependent DRSB structure. Here, using the S_0sub-key bits for each S-box $S_0 = [b_1^{\,0}, b_2^{\,0}, \ldots, b_{32}^{\,0}]$, the initial key value is computed using,

$$Z_0^{\,0} = \left(\sum_{j=1}^{32}(b_j^{\,0} \times 2^{j-1})\right)/2^{32} \qquad (1)$$

Similarly, using the S_1 sub-key bits for each S-box $S_1 = [b_1^{\,1}, b_2^{\,1}, \ldots, b_{32}^{\,1}]$, the initial key value is computed using,

$$Z_0^{\,1} = \left(\sum_{j=1}^{32}(b_j^{\,1} \times 2^{j-1})\right)/2^{32} \qquad (2)$$

Note that the subkey S_0 is used to shuffle the table contents of q_0 and subkey S_1 is used for shuffling the table contents of q_1.Using the computed value, chaotic sequences are generated with logistic map [14] using the following formulas.

$$Z_{n+1}^{\,0} = 3.9955 Z_n (1 - Z_n^{\,0}) \qquad (3)$$

$$Z_{n+1}^{\,1} = 3.9955 Z_n (1 - Z_n^{\,1}) \qquad (4)$$

b. Cryptanalysis

The cryptanalysis is performed to evaluate the strength of the proposed encryption algorithm. This analysis is done using five different tests which are discussed below.

c.Histogram Analysis

Histogram analysis is done to evaluate the distribution of pixels in an image. The quality of the encryption is indicated by the uniformity in the distribution of the histogram. Encrypted images having uniform distribution have better security than those that have non-uniform distribution. Figure 1(a) shows the Brain image and Figure 1(b) shows the encrypted Brain image using the proposed encryption algorithm, Figure 1(c) depicts the histogram of Brain image and Figure 1(d) illustrates the histogram of the encrypted Brain image. Figure 1(d) clearly shows that the histogram has a uniform distribution. Thus, the proposed algorithm has very good security features and is highly resistant against statistical attacks.

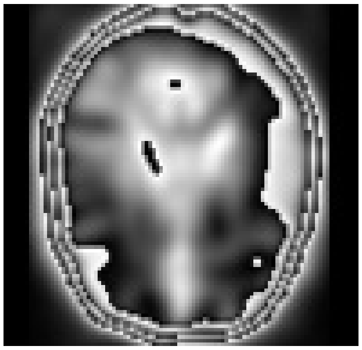

Fig 1. (a) Brain Image

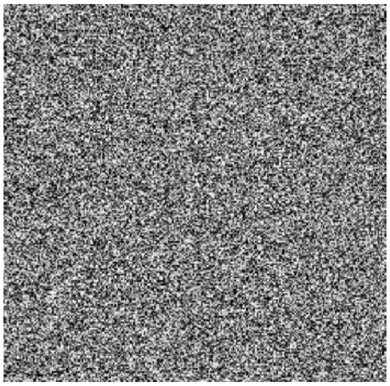

Fig.1 (b) Encrypted Image

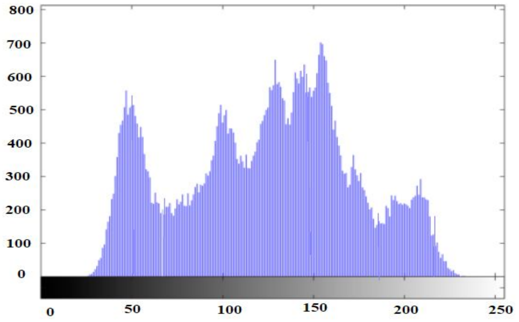

Fig 1. (c) Histogram of Brain image

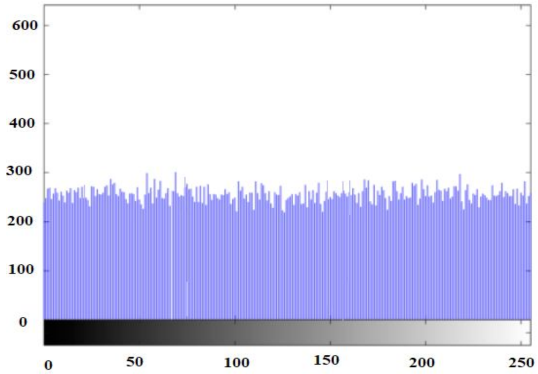

Fig.1 (d) Histogram of encrypted Brain image

d. Pixel Correlation Analysis

This analysis is done to estimate the correlation between adjacent pixels of an image. A Plain image usually has very high correlation between its adjacent pixels. However, this value reduces in an encrypted image. The encrypted image that has least value of pixel correlation is said to be the one with greater security. This value is computed as in [15]. The values of correlation coefficient obtained using the proposed DRSB algorithmis shown in Table 1. From Table 1, we see that the value of correlation of plain image is too high and is close to 1. The proposed DRSB system achieves very less value of 0.000198 which is the least among various other chaos-based encryption algorithms proposed in the literature.

Table 1. Comparison of pixel correlation

Plain image	**Pixel correlation**			
	Hyper Chaos [7]	**Chaotic state variable** [8]	**Chaotic S-Box** [6]	**Proposed DRSB encryption**
0.9354	0.00032	0.0054	0.5310	0.000198

Entropy Analysis

The randomness of an image can be quantitatively expressed using entropy analysis. High values of entropy indicate that the randomness is high and thus the image is highly secure. It is computed as

$$H(I) = -\sum_{j=0}^{2^m-1} P(I_j)\log_2[P(I_j)] \qquad (5)$$

Here, $P(I_j)$ denotes the probability of occurrence of I_j .Since grey-scale images have 256 different values, the total number of levels are 2^8, hence the maximum ideal value is 8. Values close to 8 indicates better quality of encryption. The values of entropy obtained using the proposed DRSB algorithm is shown in Table 2. The proposed DRSB system achieves very high value of 7.9991 which is the highest among various other chaos-based encryption algorithms proposed in the literature.

Table 2. Comparison of entropy

Entropy			
Chaotic S-Box [6]	**Hyper chaotic & Dynamic S-box** [9]	**Combined chaos**[16]	**Proposed DRSB Encryption**
7.9566	**7.9934**	**7.9964**	**7.9991**

Sensitivity Analysis

Since the proposed encryption scheme is based on chaos theory, it is highly sensitive to key parameters which are the initial condition and the control parameter. Thus, to test the secret key sensitivity we change the initial key value by a very small Δ=10^{-14} value. The decryption is then performed using new set of keys $Z_0{}^i + \Delta$ and $i = 1, 2$. Figure 2 shows the original data, encrypted data and the result obtained after decryption using the new set of keys. From the Figure 2, it is evident that the data cannot be retrieved back even if there is a small change in the key parameter values. Thus, our proposed framework possesses very high secret key sensitivity. The sensitivity level is in the order of 10^{-14} which a is very low value.

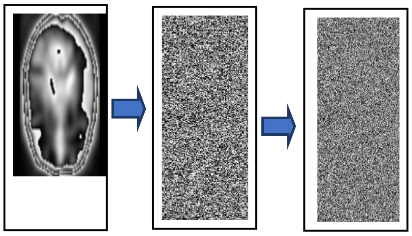

Figure 2Results obtained using secret key sensitivity analysis of Brain image

Key Space Analysis

The key space of any encryption scheme should be very large so that the key cannot be predicted using brute force attack. Else, in a particular span of time, using an exhaustive search technique the key can be predicted and the data can be decrypted. The initial key value for chaotic sequence generationin this framework is $Z_0{}^i$ and $i = 1, 2$. We know that in the proposed encryption scheme, $0.0000... \le Z_0{}^i \le 1.0000...$.We also know that the precision value of a 64-bit double data is 10^{-15}. Thus, the range is 10^{15}. In this algorithm, we find that there are 6 q_0 and 6 q_1. Therefore, the key space of the proposed scheme is $(10^{15})^{2\times6}$= $(10)^{180}$≈ $(2)^{598}$. The key space of AES algorithm is $(2)^{256}$. Thus, it is clear that the encryption capability of the proposed scheme is better than that of AES algorithm.

Computational Complexity Analysis

The proposed system was simulated using MATLAB R2015b running on windows intel i5 core processor with 4GB RAM. The time taken by the proposed framework for encryption is 2.193s. The time complexity taken by the encryption scheme as in Reference [6] is 2.465s. Thus, it is obvious that, this scheme has minimal computational complexity.

4. THREAT DETECTION USING SHA-512 ALGORITHM

To identify if the data has been manipulated during transmission, in this work we have employed the hash SHA-512 algorithm. The hash algorithms are used for representing the input message in the form of a digest with a fixed length. The main advantage of using hash algorithms are for assuring authentication and protection of the data. Any kind of data manipulation can be identified using these algorithms. SHA-512 algorithm generated the largest hash value with a length of 512 bits. This algorithm offers the highest attack complexity of 2^{256}.Threat detection using the SHA-512 algorithm is done using the following steps.

Transmitter side:

Step1: Convert the input medical image of size $M \times N$ to a one-dimensional sequence of length L (where $L = M * N$).

Step 2: Append zeros to the sequence such that L is a multiple of 1024.

Step 3: Divide the sequence into sub-blocks each of length 1024.

Step 4: Each sub-block is processed iteratively using an initial 512-bit hash value to finally obtain a final 512-bit hash value H^t.

$$H^t = \{H_1, H_2, ..., H_{64}\}$$

where each H_i refers to the i^{th} byte and $H_i = \{h_{i1}, ..., h_{i8}\}$.

Step 5: Append the encrypted image EI with the hash H^t and transmit it.

Receiver side:

Step 1: Using decryption algorithm decrypt the encrypted image EI to get the decrypted image DI

Step 2: Obtain the 512-bit received hash value H^r using the decrypted image DI.

Step 3: Compare the two hash values H^t and H^r.

Step 4: If $H^t \neq H^r$, then threat is detected.

5.CONCLUSION

The cryptanalysis of Dynamic and Random S-Box (DRSB) Generation Algorithm was presented in this paper. Analysis was carried out using various aspects like histogram, correlation, entropy, sensitivity and key space. It was shown quantitatively that the DRSB algorithm achieved very good performance in terms of all the analysis techniques. In particular, this system produced a histogram that has a uniform distribution. The pixel correlation analysis revealed that this scheme produces very less correlation of about 0.000198 between the adjacent pixels. Also, entropy analysis showed that the DRSB algorithm attains very high entropy of about 7.9991. The sensitivity analysis proved that the sensitivity of this algorithm was as low as 10^{-14}. The key space analysis revealed that the key space of DRSB algorithm was $(2)^{598}$. In addition, a threat detection system to protect the framework against the manipulation of data during its transmission was also presented in this research. In this work, SHA-512 algorithm was used for ensuring the protection of medical data.

REFERENCES

[1] Q. A. Kester, L. Nana, A. C. Pascu, S. Gire, J. M. Eghan, and N. N. Quaynor, “A Cryptographic Technique for Security of Medical Images in Health Information Systems,” in *Procedia Computer Science*, 2015, vol. 58, pp. 538–543.

[2] K. T. Alligood, T. D. Sauer, J. A. Yorke, and J. D. Crawford, “ Chaos: An Introduction to Dynamical Systems ,” *Phys. Today*, vol. 50, no. 11, pp. 67–68, 1997.

[3] A. N. Pisarchik and M. Zanin, “Chaotic map cryptography and security,” *Encryption Methods, Softw. Secur.*, pp. 1–28, 2010.

[4] F. Pareschi, G. Setti, and R. Rovatti, “Implementation and testing of high-speed CMOS true random number generators based on chaotic systems,” *IEEE Trans. Circuits Syst. I Regul. Pap.*, vol. 57, no. 12, pp. 3124–3137, 2010.

[5] F. Özkaynak, “Cryptographically secure random number generator with chaotic additional input,” *Nonlinear Dyn.*, vol. 78, no. 3, pp. 2015–2020, 2014.

[6] Ü. Çavuşoğlu, S. Kaçar, I. Pehlivan, and A. Zengin, “Secure image encryption algorithm design using a novel chaos based S-Box,” *Chaos, Solitons and Fractals*, vol. 95, pp. 92–101, 2017.

[7] M. Ahmad, E. Al Solami, X. Y. Wang, M. N.

Doja, M. M. Sufyan Beg, and A. A. Alzaidi, “Cryptanalysis of an image encryption algorithm based on combined chaos for a BAN system, and improved scheme using SHA-512 and hyperchaos,” *Symmetry (Basel).*, vol. 10, no. 7, pp. 1–18, 2018.

[8] Z. Bashir, J. Watróbski, T. Rashid, S. Zafar, and W. Salabun, “Chaotic dynamical state variables selection procedure based image encryption scheme,” *Symmetry (Basel).*, vol. 9, no. 12, 2017.

[9] Y. Liu, X. Tong, and J. Ma, “Image encryption algorithm based on hyper-chaotic system and dynamic S-box,” *Multimed. Tools Appl.*, vol. 75, no. 13, pp. 7739–7759, 2016.

[10] A. Banik, Z. Shamsi, and D. S. Laiphrakpam, “An encryption scheme for securing multiple medical images,” *J. Inf. Secur. Appl.*, vol. 49, 2019.

[11] S. Kumar, B. Panna, and R. K. Jha, “Medical image encryption using fractional discrete cosine transform with chaotic function,” *Med. Biol. Eng. Comput.*, vol. 57, no. 11, pp. 2517–2533, 2019.

[12] S. Priya and B. Santhi, “A Novel Visual Medical Image Encryption for Secure Transmission of Authenticated Watermarked Medical Images,” *Mob. Networks Appl.*, 2019.

[13] V. S. Lima, F. Madeiro, and J. B. Lima, “Encryption of 3D medical images based on a novel multiparameter cosine number transform,” *Comput. Biol. Med.*, vol. 121, no. February, p. 103772, 2020.

[14] R. M. May, “Simple mathematical models with very complicated dynamics,” *Nature*, vol. 261, no. 5560, pp. 459–467, 1976.

[15] C. Zhu, G. Wang, and K. Sun, “Cryptanalysis and improvement on an image encryption algorithm design using a novel chaos based s-box,” *Symmetry (Basel).*, vol. 10, no. 9, 2018.

[16] W. Wang *et al.*, “An encryption algorithm based on combined chaos in body area networks,” *Comput. Electr. Eng.*, vol. 65, pp. 282–291, 2018.