AN IMPROVED COLOR IMAGE ENCRYPTION ALGORITHM WITH PIXEL PERMUTATION AND BIT SUBSTITUTION

Lini Abraham[1], Neenu Daniel[2]

[1] M Tech Student, Computer Science and Engineering (CSE), Viswajyothi College of Engineering and Technology, Vazhakulam, Kerala, India, ***linirt33@gmail.com***

[2] Assistant Professor, Computer Science and Engineering (CSE), Viswajyothi College of Engineering and Technology, Vazhakulam, Kerala, India, ***neenudaniel@email.com***

Abstract

Today the transmission of multimedia data including image and video is growing in telecommunications. Security is one of the main issues in transferring such sensitive information. Powerful image encryption algorithm is the solution for this problem. This paper is an implementation of a color image encryption algorithm based on Rubik's cube technique. The Rubik's cube technique is used for pixel permutation and a bit substitution method based on DNA sequences are used to change the value of each pixel on the image. Then the time-stamp is appended with encrypted image, which can be used to identify the replay attack. For evaluating the performance of the algorithm a series of tests are performed. These tests include information entropy analysis, correlation analysis, analysis of NPCR and UACI values etc.

Index Terms: *Cryptography, encryption, decryption, timestamp, replay attack, plaintext, cipher-text, algorithm, chaos.*

--***--

1. INTRODUCTION

Information security plays a significant role in all fields, especially those related to confidential business or military affairs. Keeping data from being accessed by unauthorized users and from being corrupted is called data security. Encryption is a very important security mechanism. It works by scrambling the information into unreadable information and then uses a key to unscramble it for reading. Encryption on image or video objects has its own requirements due to the intrinsic characters of images such as bulk data capacity and high redundancy. Traditional symmetric encryption algorithms are generally not suitable for image encryption due to their slow speed in real-time processing and some other issues such as in handling various data formatting. A variety of chaos-based digital image encryption algorithms have been suggested. Usually chaos based encryption algorithms uses small key spaces. The theory of chaos has been widely used for image encryption because of its excellent cryptography characteristics and intrinsic features of image. Various algorithms provide different degrees of security and it is based on how hard they are to break. If the cost required to break an algorithm is greater than the value of the encrypted data then the algorithm probably considered to be safe. Modern high quality image encryption methods have several flaws and are subjected to extensive attacks by expert cryptanalyst. Thorough study and analysis between these techniques are needed to measure the performance and to choose the better one for the intended application. For certain applications speed of encryption may be the prime concern and for some other cases the security will be important.

There are three kinds of encryption techniques namely substitution, transposition or permutation and techniques that include both transposition and substitution. Substitution schemes change the pixel values while permutation schemes just shuffle the pixel values based on the algorithm. In some cases both the methods are combined to improve security. [3] Is an introduction about chaos based image encryption. Chaos theory has proved to be an excellent alternative to provide a fast, simple, and reliable image encryption scheme that has a high enough degree of security. The method in [8] is chaos based using bit level permutation. Permutation at the bit level not only changes the position of the pixel but also alters its value. In [9] a novel image encryption method based on total shuffling scheme is illustrated. In [10] combinations of two logistic maps are used for improving the security of encryption. Encryption in [11] uses multiple chaotic systems. But each of these methods has some security issues. The algorithm in [12] combines the diffusion and confusion operations and uses the spatial-temporal chaotic system for generating the key. But this is time consuming. As the key space increases the security of the algorithm also get improved. Here this proposed scheme is applied on a chaos based secure image encryption algorithm based on Rubik's cube principle in [1]. It is an image encryption algorithm based on Rubik's cube principle. From [2] it is evident that this algorithm performs well as compared to the technique in [12] in time period and other results are also comparable.

Differential and cryptographic attacks are major concerns in data transmission. Even thorough some of the chaos based image encryption techniques resist these types of attacks to some extent; more protecting solutions are needed for security outbreaks. It can be defined as a network attack in which a genuine data transmission is maliciously repeated or delayed. It can be done by the originator or by an advisory. The common measures for this type of attacks are session tokens, one time passwords, combination of nonce and MAC and timestamps. The content in [4] describes the replay attack. [5] and [6] proposes some methods to prevent such attacks. In [7], Denning proposed a method for preventing replay attack with the help of timestamps. These methods are usually used for preventing replay attack in normal data transmission. The proposed system is all about to prevent the replay attack on digital image transmission with the help of timestamps. The technique based on grey scale images is proposed in [14]. In [14] only permutation mechanism is used for encrypting the grey scale image. But the proposed system improves the security of that algorithm by adding a bit substitution technique in [15] for encrypting color images.

further improvement. Replay attack is one of the major

The remaining of this paper is organized as follows. Section 2 describes the proposed system. The overview of the algorithm is presented and detailed explanation of DNA bit substitution technique is also given. In section 3 the new image encryption technique is compared with the Rubik's cube technique and the result for the same is also presented. The results of images with distinct and various sizes are evaluated and discussed. The last section describes the conclusions and further discussions.

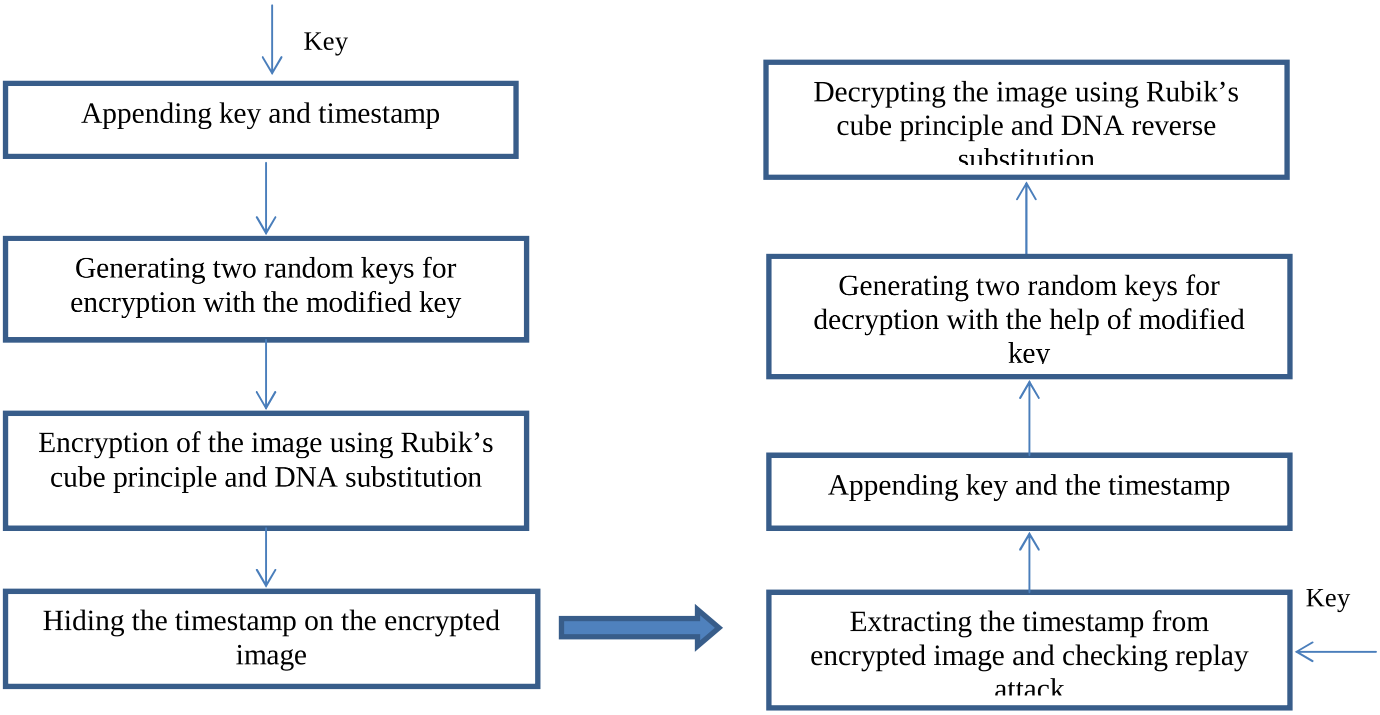

Key
Appending key and timestamp
Generating two random keys for encryption with the modified key
Encryption of the image using Rubik's cube principle and DNA substitution
Hiding the timestamp on the encrypted image
Decrypting the image using Rubik's cube principle and DNA reverse substitution
Generating two random keys for decryption with the help of modified key
Appending key and the timestamp
Extracting the timestamp from encrypted image and checking replay attack
Key

Fig -1 Overview of the proposed system

2. PROPOSED SYSTEM

The proposed system is an enhancement to the Rubik's cube based technique in color image. The overview of the system is given in Fig -1. First the timestamp is taken and added with the shared key value. Then two random keys are generated for permuting the pixel values of the image using Rubik's cube principle in [1]. Then a substitution technique based on DNA sequences are employed which is described in [15]. Then KBRP (Key Based Random Permutation) [13] is used to hide the time-stamp in the encrypted image. That will form the cipher image.

During decryption, first the time-stamp is extracted from the encrypted image by using the shared secret key. The difference between the extracted time and the current time is taken. If that difference is within the threshold then the decryption is performed otherwise it is rejected. For performing the decryption, the time-stamp is appended with the key and the two random numbers are generated. The decryption is then performed to get the original image. Before performing these operations the system time should be synchronized.

Every module except the DNA substitution is already explained in [14]. In that proposal only permutation of pixels in the image was used. But if we are adding a substitution along with that image the security will get improved. In this paper a bit substitution method based on DNA sequences is proposed based on [15]. The detailed explanation about DNA sequence substitution is given below.

2.1 Chaotic DNA Substitution

The proposed substitution method is a chaotic DNA transformation. Here two rules or steps are involved. They are: -

- Binary coding rule
- Complementary rule

The binary coding rule transforms letters A, C, G and T into binary codes and vice versa. In this particular method the following binary encoding is adopted. A=00, C=01, G=10, T=11. That means A is coded as "00", C as "01" etc. Then each pixel value in the encryption is transformed to binary using the DNA encoding.

In complementary rule, each letter x is assigned to a complement denoted C(x). Here the C(x) represents the complement of x. For getting a clear picture, consider an example, for the following complementary transformation: (AT)(TC)(CG)(GA), the conclusion is that C(A) = T, C(T) = C, C(C) = G and C(G) = A. There are six allowable complementary transformations, they are: -

(AT)(TC)(CG)(GA)

(AT)(TG)(GC)(CA)

(AC)(CT)(TG)(GA)

(AC)(CG)(GT)(TA)

(AG)(GT)(TC)(CA)

(AG)(GC)(CT)(TA).

The perturbed chaotic value used to control the substitution process is transformed to binary format (8 bits). Each pixel is represented by 8 bits (4 pairs). For example consider the pixel value "222" which is represented as 11 01 11 10. A random value is generated for each pixel on the image using PWLCM (Piecewise Linear Chaotic Map). The equation for PWLCM is given by: -

$$X(n) = F[x(n-1)]$$

$$= \begin{cases} x(n-1) * \dfrac{1}{p} & if\ 0 \le x(n-1) < p \\ [x(n-1) - p] * \dfrac{1}{0.5 - p} & if\ p \le x(n-1) < 0.5 \\ F[1 - x(n-1)] & if\ 0.5 \le x(n-1) < 1 \end{cases}$$

Where *p* is the positive control parameter and the chaotic values *x(i)*,*i* = 1,2,...,n, are real values and belong to the intervals (0, 0.5) and (0, 1) respectively. The initial values *p* and *x(0)* are calculated from the modified key value. The output from the chaotic map is represented in 8 bits. For each pixel in the plain image a random value in 8 bits is generated and the pixel value is represented in 4 pairs as explained above.

From the random value generated for a pixel, the most significant 3 bits are used to select one of the six transformations given above. And that transformation rule is used for that particular pixel value. The transformation number can be calculated by the following equation: -

$$tr = mod\left(\frac{c}{2^5}, 6\right)$$

Remaining 5 bits are used to compute the number of iterations the complementary transformation is to be applied on each pair of bits. Here the complementary rule is applied only on 3 pairs, the right most pair is not used because of the chances of changes during the time-stamp hiding. In other words the fourth and fifth bits of the random number are used to generate how many times *it(1)*, the complementary transformation is applied to the first two bits of the pixel value in process. The fifth and sixth random bits are used to determine number of the complementary rounds of *it(2)* for the second pair of bits. The sixth and seventh bits are used for the third pair of the value in process. The extraction of this number of iterations on 1st, 2nd and 3rd pair of pixel values are given by: -

$$it(1) = mod\left(\frac{c}{2^3}, 4\right)$$

$$it(2) = mod\left(\frac{c}{2^2}, 4\right)$$

$$it(3) = mod\left(\frac{c}{2}, 4\right)$$

For example, consider the previous example "222" as the pixel value. It can be represented as 11 01 11 10. Now take the first pair of bits "11". The binary coding rule is given as A=00, C=01, G=10, T=11. From the generated chaotic value the most significant 3 bits can be used to find out the sequence number. Suppose that the sequence number for that particular pixel is 5. So the 5th complementary rule is (AG)(GT)(TC)(CA).

If *it(1)* = 2, then the number of iterations for the first pair is 2. Here the first pair "11" means T from the binary coding rule. In first iteration C(T) = C(from fifth sequence). The value of C is "01" as per the binary coding rule. First T ("11") is replaced with C ("01"). In the second iteration C(C) = A. So "01" is replaced by "00". This is performed for the remaining two pairs and again they are combined together to get the cipher value. For each pixel this is repeated. So for each one the sequence selected and the number of iterations is different.

3. RESULTS AND DISCUSSIONS

The Fig -2 shows an example for the encryption and decryption using the proposed method. The test image selected is AIR plane. The experiments are done on

256×256 images with 128 bit key. We can see that the original and the decrypted images are same and the rate), UACI (Unified average changing intensity), entropy, correlation coefficient and PSNR (Pixel to noise ratio) are encrypted image is random. For performing the analysis the parameters like NPCR (Number of pixel change evaluated. The definitions and detailed explanations of these parameters are given in [16].

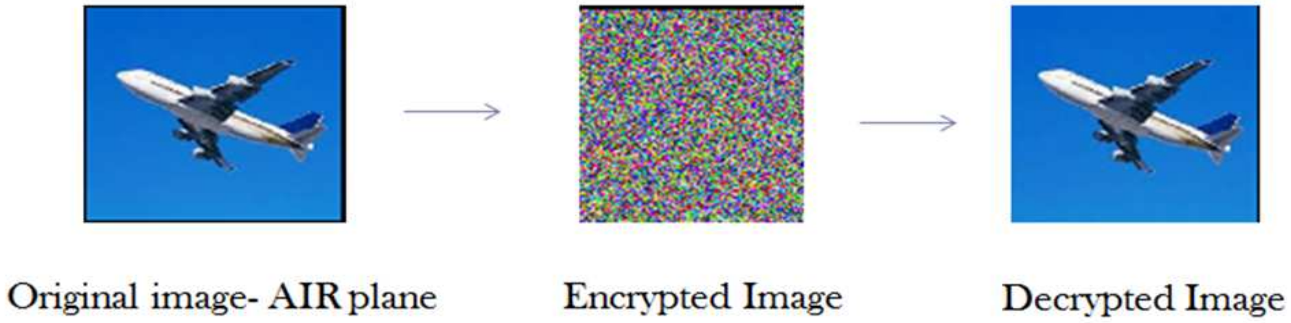


Fig -2 Example using improved scheme

Some of the evaluation results for the improved scheme are given in Table -1. The NPCR is 99.6246 and the UACI is 34.7988 for a *256×256* AIR plane color image. The NPCR should be high as possible for an enhanced technique. The UACI should be around 33%. We can see that the correlation coefficients are also low. The time for encryption and decryption will vary from system to system. The time required for overall process is below one minute. The PSNR value between original and decrypted image is infinity. This means that the pixel values in original and the encrypted images are distinct.

Table -1 Results of simulation on color image

Parameter	Improved technique
NPCR	99.6246
UACI	34.7988
Entropy	7.9970
Horizontal correlation	-0.0347
Vertical correlation	0.0015
Diagonal correlation	-0.0022
PSNR	Infinity

Now the results by the application of the new scheme in different *256×256* color images are given in Table -2. Here the test images are Lena, Baboon and Pepper. As it includes the effect of the time-stamp which varies by time, a little variation in the results is possible. It is because of the reason that on each times the timestamp varies. From the table we can see optimal results.

Table -2 Results for different images having same size

Parameter	AIR plane	Lena	Baboon	Pepper
NPCR	99.6038	99.6048	99.6099	99.6068
UACI	34.7276	31.0178	29.1335	31.9751
Entropy	7.9973	7.9975	7.9973	7.9971
Horizontal correlation	-0.0057	-0.1290	0.0013	-0.0030
Vertical correlation	0.0037	-0.0026	0.3152	0.7563
Diagonal correlation	0.1035	0.0041	-0.0016	0.2527
PSNR	Infinity	Infinity	Infinity	Infinity

Next the Rubik's cube technique and the improved scheme is applied on variable sized test images. The results of this comparison are plotted as graphs in Fig -3 and Fig -4.

In Fig -3 the NPCR values are compared. Higher NPCR values are desired for ideal encryption schemes. This will indicate the percentage of different pixels between two images. The red line shows the improved scheme and the blue line is the Rubik's cube based technique.

The Fig -4 shows the comparison of entropy values. It is an important concept for analyzing an encryption scheme. Entropy gives an idea about self-information. From the results it is evident that the improved method is comparable with the Rubik's cube technique and provides more security.

Fig -3 Comparison of NPCR values

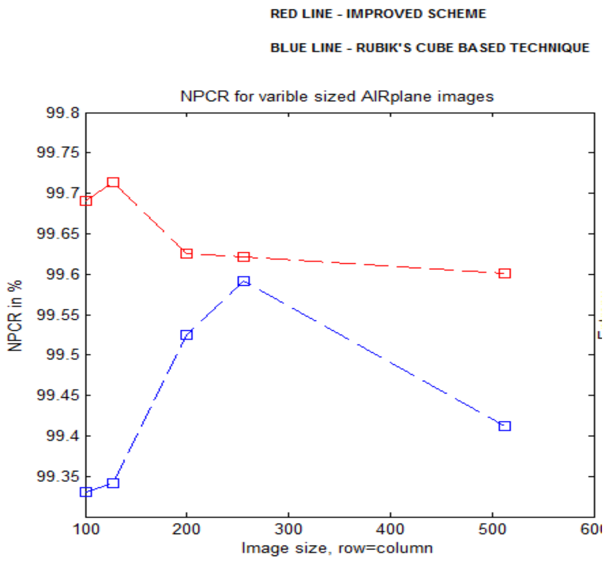
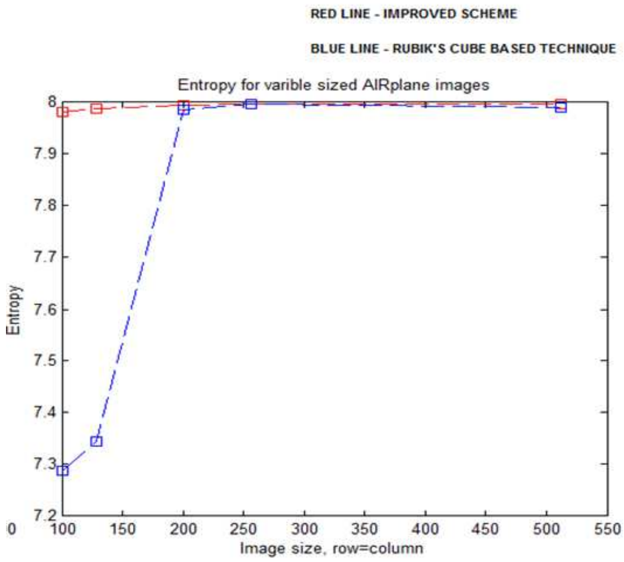


Fig -4 Comparison of UACI values



CONCLUSIONS

Chaos based encryption algorithms are employed nowadays because of their better security and performance aspects. Each of the image encryption techniques has its own advantages. Identification of the suitable algorithm for a particular application depends on the prerequisites of that application. The technique using Rubik's cube principle has a large key space and its implementation is quite simple. Later the security of the Rubik's cube technique has improved by adding time-stamp and chaotic DNA substitution. The time-stamp is appended with the original key. So the time-stamp is specially added to produce different cipher texts by applying same key on same plain text. Also it can be used to check the replay attack. But it is under the assumption that the system time is synchronized. In basic Rubik's cube based approach bit substitution is not used. So a chaotic bit substitution method based on DNA sequences is added for improving the security. The comparison results and assessments have done and presented. From that the efficiency of the improved approach is evident. The experimental result shows that the improved scheme performs well in color images. New techniques and modifications can be added on to the proposed system for making excellent multimedia applications.

REFERENCES

[1] Khaled Loukhaoukha, Jean-Yves Chouinard, and Abdellah Berdai, "A Secure Image Encryption Algorithm Based on Rubik's Cube Principle", Department of Electrical and Computer Engineering, 2011.

[2] Lini Abraham, Neenu Daniel, "Secure image encryption algorithms: A review", IJSTR, 2013.

[3] Yaobin Mao and Guanrong Chen, "Chaos-Based Image Encryption", in Hand- book of geometric computing, Springer,2005.

[4] Li Gong and Paul Syverson, "Fail-stop protocols: An approach to designing secure protocols", In 5th International Working Conference on De- pendable Computing for Critical Applicaitons, pages 44–55, September 1995.

[5] Sreekanth Malladi, Jim Alves-Foss, Robert B. Heckendorn, "On Preventing Replay Attacks on Security Protocols".

[6] T. Aura "Strategies against replay attacks", In Proceedings of the 10th IEEE Computer Society Foundations Workshop, pages 59 – 68, Rockport, MA, June 1997. IEEE Computer Society Press.

[7] D. Denning and G. Sacco, "Timestamps in key distribution protocols". Communications of the ACM, 24(8):553–536, August 1981.

[8] Zhi-liang Zhu, Wei Zhang, Kwok-wo Wong, Hai Yu, "A chaos-based symmetric image encryption scheme using a bit-level permutation", Information Sciences 181 1171–1186 Elsevier, 2010.

[9] G. Zhang and Q. Liu, "A novel image encryption method based on total shuffling scheme", Optics Communications, vol. 284, no. 12, pp. 2775–2780, 2011.

[10] Ismail1, Mohammed Amin, Hossam Diab, " A Digital Image Encryption Algorithm Based A

Composition Of Two Chaotic Logistic Maps", Proc. 27th IEEE Int'l Conf. Signal Processing., pp. 733-739,2011.

[11] H.Alsafasfeh, and, A.A.Arfoa, Image encryption based on the general approach for multiple chaotic system, Journal of Signal and Information Processing 2, 238- 244, 2011.

[12] Yong Wanga, Kwok-Wo Wong, XiaofengLiaoc, Guanrong Chen, "A new chaos- based fast image encryption algorithm", in Applied Soft Computing, Elsevier, 2011.

[13] Shakir M. Hussain1 and Naim M. Ajlouni, "Key Based Random Permutation", Journal of Computer Science 2 (5): 419-421, 2006.

[14] Lini Abraham, Neenu Daniel, "Enhancing the Security of Image Encryption Algorithms by Adding Timestamp", IJARET, Vol. 1, Issue VIII, Sep. 2013.

[15] Abir Awad and Ali Miri, "A New Image Encryption Algorithm Based on a Chaotic DNA Substitution Method" in , Communications (ICC) on IEEE, p. 1011-1015, June 2012.

[16] Jawad Ahmad and Fawad Ahmed, "Efficiency Analysis and Security Evalu- ation of Image Encryption Schemes", in International Journal of Video and Image Processing and Network Security, IJVIPNS-IJENS, Vol:12 No.04, 2010.