

CRYPTOGRAPHY AND DATA TRANSFER- EMPLOYABILITY OF RSA ALGORITHM AND RGB MATRIX IN ENHANCING ENCRYPTION FOR DATA TRANSFERABILITY

Sahil Kapoor

*Amity Int School
Sec-6, Vasundhara, Ghaziabad*

ABSTRACT

Data collected by each individual is increasing day by day and so is the rate of transfer of that data. Hence, there is a need to protect this data while the transfer is being done. One simple solution to this problem of data security is cryptography. Our paper proposes a method to share images after being encrypted by Logistic maps and Linear Feedback Shift Register (LSFR) followed by the RSA Algorithm. Thereby, we provide extra layers of security over the existing encryption technique making it difficult to decrypt the images after data transfer. The image can only be decrypted with the help of a key.

Keywords: Logistic maps · RSA Algorithm · Linear Feedback Shift Register (LSFR) · RGB Matrix · encryption

1 INTRODUCTION

For many years the backbone of human existence is information. As technology increases day by day, electronic devices have been advancing and most of the information exchange between devices is done with the help of digital signals. Due to this increasing demand of data transfer via digital signals with the help of electronic devices, there is an increasing demand of security of information which is being transferred as this information may be confidential and an increasing number of cases have come to light where data is being hacked in order to get access to this vital information. This leads to loss of integrity and authenticity of the information. This problem leads us to a field which was introduced in 1948 and was termed as cryptography. The study of methods to secure the data being transferred with the help of an external agent involved known as adversary in whose presence the other two parties communicate is known as cryptography. It involves rules of mathematics and protocols of computer science in order to encrypt the vital data which can then be decrypted on the other end with the help of some pre-set rules. Cryptography can be described by its two forms:

1.1 Symmetric

It is the form of cryptography in which there is only one key present which is responsible for both encryption as well as decryption operations at end of sender's and receiver's.

1.2 Asymmetric

It is the form of cryptography in which there are two types of keys, one is the public key which can be provided to anyone and the other is the private key which is to be stored securely by the user. Both these keys are used while encrypting and decrypting the data.

The use of electronic devices is increasing and so is the use of social media and messaging services and the rate of data transfer. With this large scale use of these services for data transfer, there is huge attraction of hackers. These hackers use the photos transferred between the users and then launch various attacks on the users to harm them socially. Images that are accessed by hackers can be easily modified which can lead to loss of integrity and authenticity and the resulting image could be used for the wrong purposes. Moreover, areas of military and defence where a high level of security is desired, if the images are accessed illegally, national security maybe at threat. Hence with increased use of images, there is an increasing need of cryptography in order to maintain the privacy of the users. Such highly encrypted processes are necessary in order to restrict the access of images with the sender and receiver only. In this paper along with RSA algorithm, we have used chaotic maps in order to provide an additional security layer and remove the discrepancies in encryption using RSA algorithm. Chaotic maps are based on the principle of chaos which simply means disorder. These chaotic states are extremely sensitive to their initial states. Even a slightest change in this initial state can lead to entire different data which is uncorrelated. There are many researches on encryption of data using chaotic maps. Initial states are very sensitive to logistic functions, which is one of the chaos functions. There are several advantages of using chaotic function like- easy implementation, fast computation power and difficulty in decryption.

2 LITERATURE SURVEY

Cryptography is an emerging research field and many electronic devices are using encryption before transferring data. Other than logistic maps [1], a lot of chaotic maps [2, 3, 4] have been used for encryption for example multi chaotic system [5]-[14], standard maps [8], baker maps [9], cat maps [10]. Use of systems based upon multi chaotic in order to encrypt coloured images is shown in [11]. There are cases where two of these chaotic maps are combined in order to perform encryption in two different stages [13]. In another research, encryption using logistic and pixel table is proposed [14]. Another author used encryption composed of baked map [15], logistic map, folded map. After achieving better efficiency even, the histogram is non-uniformly distributed for resultant encrypted images. Previously, the image uncertainty was improved with the help of table of pixel mapping. This is followed by row and column replacements and lastly random vector made by logistic maps is applied on the resultant.

3 IMPLEMENTATION

The encryption algorithm comprises of the following steps:

Step 1 Formation of RGB matrix

In order to present the mathematical part in cryptography with image depth, it is necessary to transform the image in a valid mathematical model. This can be achieved by representing all the pixels in the image as elements of a matrix having values originating at 0 and ending at 255[0-255].

- i. In order to encode images, the sender should have use of MATLAB i.e. a software for image processing.
- ii. The image should be converted to a three dimensional matrix by the sender. The command in MATLAB for this conversion is

```
X = imread ("image.jpg");
Display(X)
```

- iii. Once the correct RGB three dimensional matrix is formed by converting the image, sender has to convert X matrix into another row matrix Y in order to have mathematical operations available. Command in MATLAB to achieve this is Matrix $Y = X(:)$;

```
Y=Y';
```

- iv. The image is now available for performing encryption using various algorithms.

Step 2 Chaotic sequence of keys generated by logistic map sequence and progression of states of linear feedback shift

The function of logistic map is given by equation (1) which creates chaotic sequences { } where lies between 0 and 1.

$$x_{n+1} = (1 -) \quad (1)$$

Here x is bifurcation parameter that has a range of 0 to 4 and A_0 is initial value ranging from 0 to 1. This generates a sequence of elements according to equation (1). The value of x is when between 3.75 and 3.99, a very random sequence is generated.

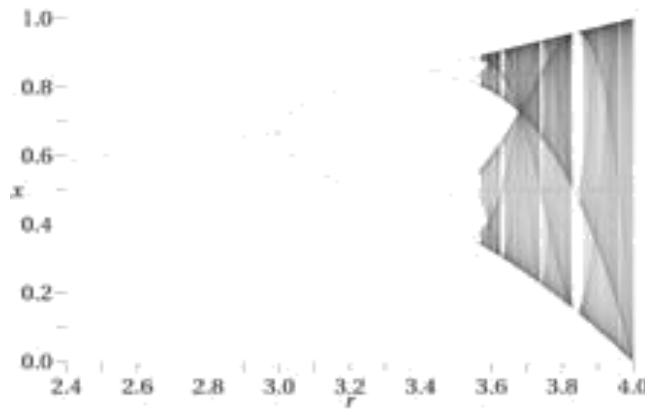


Fig. 1. Bifurcation diagram of Logistic Map

By selecting a value of x between 3.75 and 4 a random chaotic sequence is generated where x_0 is taken as initial value which can be any value between 0 and 1. The sequence is converted to unsigned integers with range 0 to 255 after multiplication with 255. The value of x is rounded off to the nearest value of decimal. This value received is used as the key sequence after being converted to an 8-bit sequence and called as $L_{1,i}$. Figure 1 shows Bifurcation diagram of Logistic Map.

$$L_{1,i} = (x_i * 255) \tag{2}$$

Simultaneously an m -stage Linear Feedback Shift Register is created by feedback polynomial of d (2), if the feedback polynomial used is primitive then the sequence of states generated is periodic and is of period (2^m-1) . Here $m=8$ is chosen with a polynomial $x^8 + x^6 + x^5 + x^4 + 1$. There are 255 possible initial states. Every initial state leaving zero forms sequence states with period $2^8 - 1 = 255$. Generated sequences are shifted versions of one another. In proposed scheme, LFSR of 8-bit are used to create the sequence which we call $L_{2,i}$. In fig 2 LFSR is shown in which $D_0, D_1, D_2 \dots D_7$ an initial input is provided which is known as seed and this further generates the sequence $L_{2,i}$.

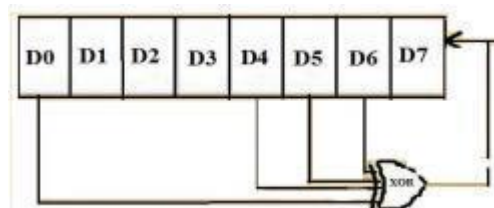


Fig.2. 8-Bit linear feedback register

The final sequence is generated by XORing s_1 and s_2 , which is called and this sequence is further used in next step. Figure 3 shows block diagram of

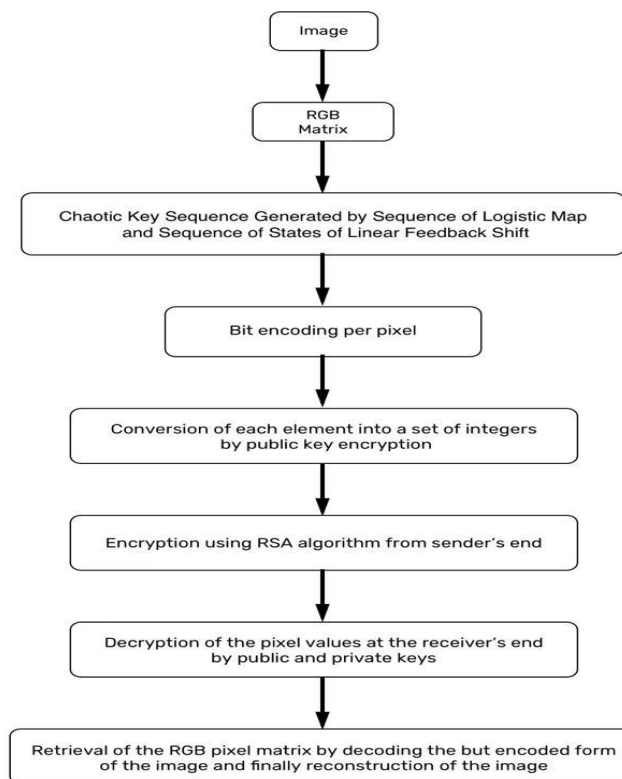


Fig. 3. Block diagram of the proposed scheme

Step 3 Non-standard number system is received from pixels

Let pixel 210 be taken as a sample. (They range from 0 - 255)

- i. First, the binary number of 8 bits is calculated from pixel:

$$(210)_{10} = (1101\ 0010)_2$$

- ii. The octal number is calculated by taking 4 bits from the eight-bit binary number:

$$(1101)_2 = (15)_8$$

$$(0010)_2 = (02)_8$$

Hence,

$$(1101\ 0010)_2 = (1502)$$

iii. To increase the security layer, nine's compliment is taken:

$$(1502) = (8497)$$

iv. The result comprises of all the digits present in a decimal system i.e. 0 to 9.

v. The resultant is converted into two parts and every part is used to obtain its octal number, which is then combined to get a number of 6 digits.

$$(84)_{10} = (124)_8$$

$$(97)_{10} = (141)_8$$

Hence resultant is

$$(8497)_{10} = (124141)$$

Step 4 Encryption using RSA algorithm at receiver's end

Once we have the matrix form of the image, RSA algorithm is applied on all the pixels. The receiver has a matrix comprising of private and public keys with one to one mapping for decryption.

It contains the following steps:

i. Two prime numbers are taken by the receiver, such as $a = 17$ and $b = 29$.

$$C = a \times b = 17 \times 29 = 493$$

ii. Another number has to be generated by receiver (e) are given

$$\text{below: } - (a-1) = 16$$

$$(b-1) = 28 \quad (a-1) \times (b-$$

$$1) = 448$$

The character e is any figure which does not have 2 or 7 as its factors. We take $e = 5$, there are many possibilities.

iii. Now the receiver sends $C = 493$ and $e = 5$ to the sender. It should be difficult to know a and b from C .

iv. Sender can now encrypt the converted bit pixel with C and e . The number is raised to the power of e :

$$(124141)^5 = 2.946645 \times 10^{25}$$

v. Partial encryption of the message is done. Now C is used for further encryption. The calculated number with power of e is divided by C .

The resultant is 6.02×10^{15} . This number is sent to the receiver.

vi. The number that the receiver has i.e. 448 is used for decryption. Receiver needs a multiple of 5 which is more than 448's multiple by 1.

Multiples of 5 are: -

5, 10, 15, 20, 25, 30, 35, 40

While those of 448 are: -

448, 886, 1344, 1792, 2240, 2688

The desired number is 1345 which is greater than 1344 by 1.

$$1345 = 5.269 d$$

$$= 269$$

vii. Once we have all the public and private keys, the values are sent to the receiver.

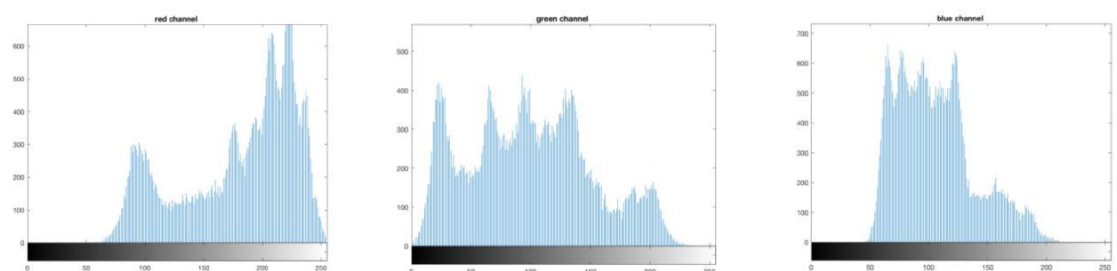


Fig. 4. Histograms Before Encryption



Fig. 5. RGB Components of Image

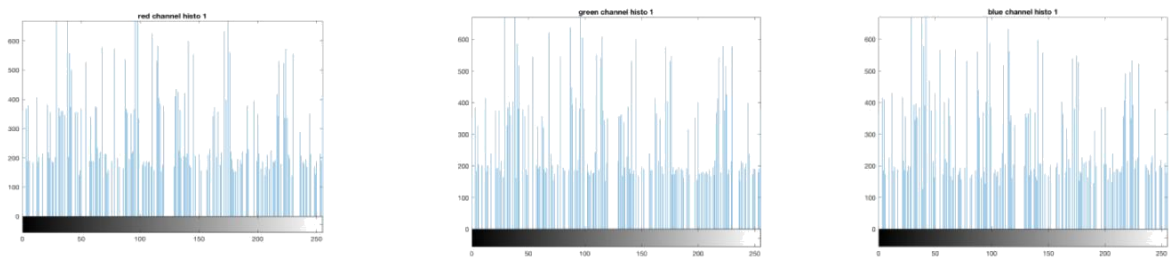


Figure 5.2: Green Histogram

Fig. 6. Histograms After Encryption

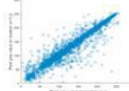
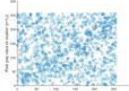
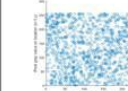
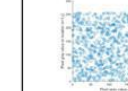
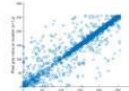

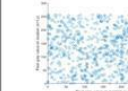
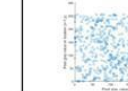
RESULTS

In order to calculate encryption quality, correlation coefficient among adjacent pixels is calculated and histograms are formed as shown in Figure 4 and Figure 6. Table 1 shows the calculated correlation coefficients that show how much correlated they are with each. Use of three thousand pixels is done in order to calculate the correlation coefficient. Figure 5 shows RGB components of image.

The equation of correlation is given by equation 3. ‘r’ is the correlation coefficient.

$$r = \frac{(\sum x_i y_i) - (\sum x_i)(\sum y_i)}{\sqrt{[\sum x_i^2 - (\sum x_i)^2][\sum y_i^2 - (\sum y_i)^2]}} \quad (3)$$

TABLE 1. Correlation Coefficient between adjacent pixels

	Original image	Cipher Image		
		P=113,q=71, e=6469,d=589	P=47,q=59, e=31,d=1291	P=17,q=23, e=109,d=2661
Lenna				
Corr.	0.9230	0.0064	0.0039	0.0169
Tower				
Corr.	0.9549	0.0030	0.0255	0.0048

CONCLUSION

This paper presents a unique way in encrypting images with help of logistic maps, LSFR and RSA algorithm. These lead to the addition of various extra layers of security and preservation to the existing administrative structure of systems. The problem we are facing while using the technique at hand is of space and time complexity, and we have to look at the problem because we have the limit of both. In order to create a system that is hard to penetrate and cannot be hacked easily, a compromise has to be reached for this trade-off. The encryption technique can be used in highly secure projects which are of high value and importance, like it contains tremendous military applications and security for the data of the people which is held in government servers to maintain privacy.

REFERENCES

1. Rivest, R.L., Shamir, A., Adleman, L., "A Method for Obtaining Digital signatures and public-key cyptosystems", Communications of the ACM, Vol 21, No.2, February 1978.
2. Jonathan Kaltz, Yehuda Lindell, "Introduction to Modern Cryptography: Principles and Protocols", ISBN: 978-1-58488-551-1, 2008.
3. Ahmad Abusukhon and Mohammad Talib, "A Novel Network Security Algorithm based on Private Key Encryption", IEEE 2012.
4. Yan-Bin, Zheng, Ding Qun. "A new digital chaotic sequence generator based on Logistic Map", Proceedings of Second International Conference on Innovations in Bio-inspired Computing and Applications (IBICA), 2011, pp.175-178
5. Zouhozr Ben Jemaa, Safya Belghzth "Correlation properties of binary sequences generated by the logistic map-application to DSCDMA." Proceedings of IEEE

International Conference on Systems, Man and Cybernetics, Hammamet, Tunisia. 2002, pp. 447-451.

6. Zhang D., Gu Q. , Pan Y. and Zhang X. “Discrete Chaotic Encryption and Decryption of Digital Images”, Proceedings of International Conference on Computer Science and Software Engineering, 2008, pp. 849-852.
7. Xiang Di, L. X. , Wang P., “Analysis and improvement of a chaos image encryption algorithm” Chaos, Solution and Fractals, Volume 40, Issue 5, 15 June 2009, pp. 2191– 2199.
8. Jin-mei Liu, Qiang Qu, “Cryptanalysis of a substitution–diffusion based image cipher using chaotic standard and logistic map” Proceedings of Third International Symposium on Information Processing, 2010, pp. 67-69.
9. M. Salleh, S. Ibrahim, I. F. Isnin, “Enhanced chaotic image encryption algorithm based on Baker's map.” Proceedings of IEEE Conference on Circuits and Systems, 2003, vol.2, pp. 508-511.
10. K. Wang, W. Pei, L. Zou, A. Song, Z. He, “On the security of 3D Cat map based symmetric image encryption scheme,” Physics Letters A, 2005, vol. 343, pp. 432-439.
11. Hong, Lianxi, and Chuanmu Li. "A novel color image encryption approach based on multi-chaotic system." Proceedings of 2nd IEEE International Conference on Anti-counterfeiting, Security and Identification, 2008, pp. 223-226.
12. Honglei, Yu, Wu Guang-shou, "The compounded chaotic sequence research in image encryption algorithm". Proceedings of WRI Global Congress on Intelligent Systems, 19-21 May 2009. Vol. 3. pp. 252 -256.
13. Weihua Z. Ying S. “Encryption Algorithms Using Chaos and CAT Methodology”, Proceedings of International Conference on Anti- Counterfeiting Security and Identification in Communication (ASID), 2010 ,pp. 20 – 23
14. Al-Najjar, Hazem Mohammad, Asem Mohammad AL-Najjar, K. S. A. Arar "Image Encryption Algorithm Based on Logistic Map and Pixel Mapping Table", Proceedings of International Arab Conference on Information Technology, 2011 (ACIT 2011).
15. “The RSA Algorithm” – Adrian Dudek, PhD, Australian National University.