A Novel Color Image Encryption using Chaotic Maps

Dr P.Shanthi

Assistant Professor

Department of Information Technology

VHNSN College(Autonomous)

Virudhunagar

Abstract:

Sensitive information requires safe and secure transmission. To hide such information, cryptographic models are used which require a set of keys in their working. Maintaining such keys itself is costly and securing them adds to the task of security. Also, such models are specific to a particular type of information that can be hidden i.e. not dynamicin working. In this paper, a color image cryptographic algorithm combining with multiple chaotic maps is proposed. Confusion is carried out through employing 2 encryption keys. The first key is generated from the 2D Arnold map while the second key is generated from the logistic map and the. For better results and analysis we incorporated our focus on the type of chaotic maps and on parameters such as Peak Signal to Noise Ratio (PSNR). The proposed method shows greater flexibility in operation and low maintenance in regard to other crypto methods. The suggested technique would be suitable to incorporate in scenarios requiring least suspicion duringan exchange of information and hence less prone to attackers. It would be easy to utilize on public modes of communication as sensitive information would be hidden in any media file which will appear just like some other normal media file.

Keywords: Chaotic Maps and Discrete Wavelet Transform

I.INTRODUCTION

An impressive technological revolution materialized in recent decades reshaping human lives. This is easily seen in the advancements in computing, wireless smart devices, the Internet as well as their interconnectivity through heterogeneous 5G networks. Such advancements came hand in hand with expansive developments in multimedia, where huge numbers of files are being exchanged every second around the globe. This has posed security challenges to scientists, mathematicians and engineers, who are now constantly developing new algorithms to secure the transmission of data between any two communication entities. For some time, a number of algorithms were mostly utilized to provide this much needed security. Those included the Data Encryption Standard (DES) and its variant, triple DES (3DES), as well as the Advanced Encryption Standard (AES). While they did provide security for a while, they are no longer suitable for the purposes of image encryption. This is because they have either been proven susceptible to cryptanalysis or are simply not efficient algorithms for image encryption. Unlike textual data, images possess a number of properties that require different encryption algorithms. For example high-definition (HD) images have very high data payloads. Moreover, adjacent pixels in an image exhibit a very high redundancy and correlation [1][2]. A review of the literature on image encryption confirms Shannon’s theory, where a high level of image security can only be attained through the application of two mutually independent encryption stages, namely, confusion and diffusion [3]. A confusion stage forces every bit in an encrypted image to depend on many parts of the key, thus hiding the connection between the two [4]. While a diffusion stage introduces an avalanche effect, such that a change of a single bit in the plain image would result in a change of roughly half of all the bits in the encrypted image. The purpose of diffusion is to eliminate any statistical relationship from being exhibited between a plain image and its corresponding encrypted one [6]. It is in the design of those two stages of encryption where chaotic functions come into play. Chaotic functions exhibit a number of inherent characteristics that make their use advantageous in relation to communication security. Those characteristics include sensitivity to initial conditions, ergodicity, pseudo-randomness, control parameters and periodicity, to name a few [5]. In general, chaotic functions are classified either into one-dimensional (1D) or multi-dimensional (MD). The choice of adopting 1D over MD chaotic functions for their utilization in image encryption algorithms is always a matter of trade-off between complexity and security. One-dimensional chaotic functions provide simple software and hardware implementations at the price of acceptable security. This makes them ideal for image encryption applications requiring real-time efficiencies. On the other hand, MD chaotic functions provide excellent security but do achieve at the price of more complex designs and implementations [7]. The utilization of multi-dimensional chaotic maps for the purposes of image encryption is very well documented in the literature. For example, the Lorenz system of differential equations is employed .The authors of [3] [8]use the Lorenz system as the first encryption stage in a 3- stage encryption process. The other 2 stages involve an S-box and Rule 30 cellular automaton.The authors of apply different scan patterns to each of the RGB color channels of the image to be encrypted. Next, they separate the Lorenz equations and apply the use of each equation on a different color channel.

II. PRELIMINARY OF THE PROPOSED IMAGE ENCRYPTION ALGORITHM

The proposed image encryption algorithm is based on a number of chaotic maps and a mathematical transformation. These are presented next

A.Arnold Cat Map

One of the most important chaotic functions is cyclic chaotic function that each time applied on a square image rearranges its pixels. In order to shuffle the embedding position of the host image, two dimensional Arnold cat map is employed in this scheme. After that logistic map is applied to find an embedding position. The generalized form of Arnold's cat map can be given by the transformation

$\Gamma : T2 \rightarrow T2$

such that:

$x' = x+y$

$y' = x+2y$

Where $x, y \in \{0, 1, 2 ... n-1\}$ and n is the size of a digital image. Let p be the transform period of an $N \times N$ digital image I. Applying ACM for a random iteration of t times ($t \in [1, p]$) to I, a scrambled image I` is obtained which is completely chaotic and different from I. Now I` can be transmitted over the communication channel without revealing any information to the unauthorized receivers .

B.Logistic Map

Logistic map is the most widely used classical map. It is simple and deterministic, with complicated dynamic behavior. The logistic map is

defined as follows:

$X_{n+1} = aX_n\ (1-X_n\ )$

where $0 < X_n < 1$ and $0 < a \leq 4$. The sequences produced by logistic map are controlled by parameter value of a and the initial value of Xn .Recently in literature,LM is used to perform better scrambling of an image[10]..At the receiving end, the process is repeated for (p − t) times to obtain back the original image.

III. METHODOLOGY OF THE PROPOSED IMAGE ENCRYPTION ALGORITHM

A. **THE ENCRYPTION ALGORITHM**
The proposed image encryption algorithm is implemented over a number of steps, as follows.

1) A color image of dimensions N × N, where for example N = 256, is loaded and

color-separated into its 3 RGB channels.
2)Each channel's pixels are then shuffled using the sequence generated from the Arnold Cat map, thus inducing diffusion in the image pixels.
3)Two encryption keys are generated. The first key is generated using the 2D Arnold Cat map.It consists of a 256 × 256 bits matrix.
5)Each channel's shuffled pixels bits are reshaped to 8 × [256 × 256] resulting in 8 sub matrices in each channel to be XORed with the first key generated in a bit–by–bit manner.
6) The Logistic chaotic maps are then employed to generate the second key.

B. **THE DECRYPTION ALGORITHM** The decryption algorithm follows the reverse order of steps of the encryption algorithm, generating and utilizing the same set of keys.

IV. SECURITY ANALYSIS AND NUMERICAL RESULTS

This section provides the computation of the various metrics utilized to gauge the performance of the proposed image encryption algorithm. A number of images popular in the image processing community are employed. Those are Lena, Mandrill and Peppers, all of dimensions 256 × 256. Comparisons with counterpart algorithms from the literature are also carried out.

A. VISUAL AND HISTOGRAM ANALYSES The first and most simple metric for evaluating any image encryption algorithm is through an assessment by the human visual system (HVS). Fig. 1 and Fig. 3respectively show the plain and encrypted images of Lena. Fig. 2 and Fig.4 respectively show the plain and encrypted images of Mandrill.

B. PEAK SIGNAL NOISE RATIO
The peak signal-to-noise ratio (PSNR) is used to evaluate the quality between the attacked image and the original image. Table 1 Shows the PSNR Values for different images.

Figure 1: Plain Lena Image

Figure 2: Plain Mandrill image.

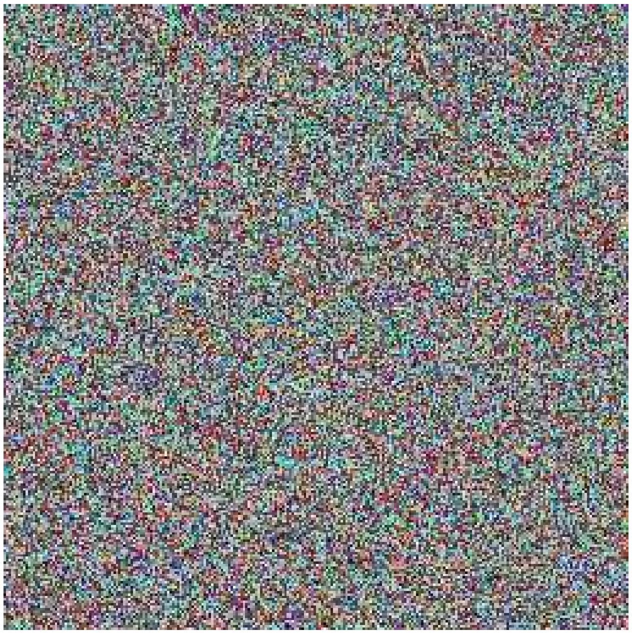

Figure 3:Encrypted Lena Image

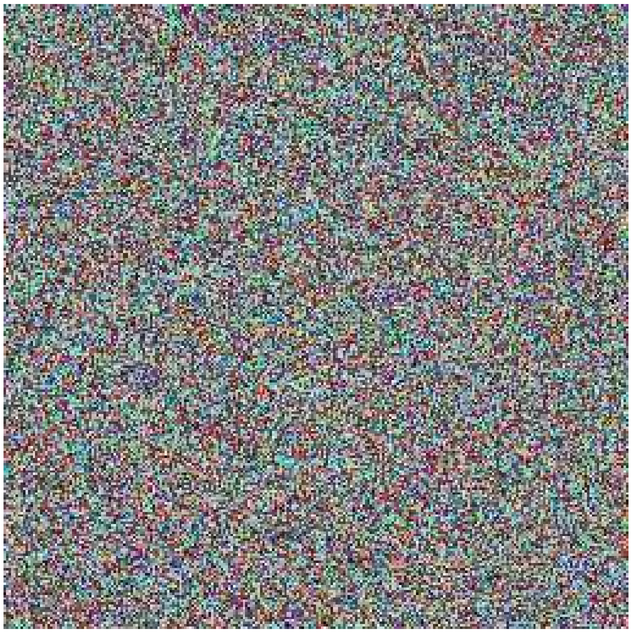

Figure 4:Encrypted Mandril Image

TABLE 1: PSNR values comparison for different images

	Proposed	[20]	[3]
Lena	**8.6510**	7.7677	8.23
Mandril	**8.1422**	5.4556	8.01
Pepper	**8.9652**	6.3423	7.65

C. CORRELATION COEFFICIENT

Analysis of correlation coefficient, r, is another metric that is highly important in evaluating the performance of an encryption algorithm. The correlation coefficient between 2 pixels x and y resulting in a value that varies between −1 and 1. For an encryption scheme to be resilient against statistical attacks, the correlation coefficient between adjacent pixels in all three directions, horizontally (H), vertically (V) and diagonally (D), should be close to zero to indicate no correlation. Otherwise, values close to −1 indicate strong negative correlation and values close to 1 indicate strong positive correlation, which make it feasible for an encrypted image to be exposed by statistical attacks. Table2 clearly shows a strong correlation between the adjacent pixels of the plain image.

TABLE 2: Correlation coefficients of adjacent pixels in plain images.

	Horizontal	Diagonal	Vertical
Lena	0.96734	0.94821	0.98276
Mandril	0.9554	0.9321	0.9675
Pepper	0.9876	0.9543	0.9754

V. CONCLUSIONS AND FUTURE WORKS

In this paper, we proposed a color image encryption algorithm based on a number of chaotic maps. The various maps were utilized to implement Shannon’s ideas of confusion and diffusion for better cryptographic security. The performance of the proposed algorithm was evaluated using various metrics, including a visual comparison, PSNR and correlation coefficient analysis.

The outcome of the various conducted analyses showcase the ability of the proposed image encryption algorithm to withstand various cryptanalytic attacks, including visual, statistical, differential and brute-force attacks. Finally, upon comparing the values of the various metrics of the proposed algorithm, it was shown to exhibit a comparable or superior performance when compared to most of those computed for its counterparts from the literature.

REFERENCES

1. P.Shanthi, R.S Bhuvaneswaran “Robust Chaos Based Image watermarking Scheme For Fractal-Wavelet” ispublished in Applied Mathematical s Sciences Vol. 8 No.32,1593-1604 (2014).
2. P.Shanthi, “Chaotic based Image Cryptography using Wavelet Transform” is published an “International Journal of Engineering Research in Computer Science and Engineering ” Volume-5, Issue-3, (2018)Sciences Vol. 8 No.32,1593-1604 (2014)
3. David Raymond Anderson. Model based inference in the life sciences: a primer on evidence, volume 31. Springer, 2008.
4. Tahir Sajjad Ali and Rashid Ali. A new chaos based color image encryption algorithm using permutation substitution and boolean operation. Multimedia Tools and Applications, 2020
5. Wassim Alexan, Mohamed ElBeltagy, and Amr Aboshousha. Rgb image

encryption through cellular automata, s-box and the lorenz system. Symmetry, 14(3):443, 2022.

6. Wassim Alexan, Mohamed ElBeltagy, and Amr Aboshousha. Image encryption through lucas sequence, s-box and chaos theory. In 2021 8th NAFOSTED Conference on Information and Computer Science (NICS), pages 77–83. IEEE, 2021.
7. Abdulrahman Al-Khedhairi, Amr Elsonbaty, Abdelalim A Elsadany, and Esam AA Hagras. Hybrid cryptosystem based on pseudo chaos of novel fractional order map and elliptic curves. IEEE Access, 8:57733–57748, 2020.