Image Encryption using Bi Transform and Chaotic Map

[1]Nainee Patel, [2]Kalpana Rai

[1]MTech Scholar, [2]Professor and HOD
[1,2]Department of Computer Science,
[1]Sagar Institute of Research Technology-Excellence, Bhopal, India

***Abstract*— In image processing applications, transmission security is paramount, thus encrypted data is invaluable. Given its high sensitivity to the initial values of the system parameters and its expansive key space, safe picture encryption benefits from the use of chaotic map and transformations. With the use of the chaotic logistic Map and the Arnold transform with discrete cosine transform, this research presented a reliable solution for the safe encryption and decryption of pictures. Statistical analysis simulations are developed and verified in MATLAB. The technique has been shown to have strong security performance, excellent encryption and decryption effects, and efficient performance in associated simulation tests and performance evaluations.**

***Index Terms*—Image Encryption, chaotic map, Arnold, Logistic, DCT and Image Security**

I. INTRODUCTION :

Nevertheless, despite the many ways in which digital images make people's lives simpler, there are also a number of security dangers presented by them that need to be addressed. In addition, standard encryption algorithms like RSA, DES, and 3DES were designed specifically for text and do not work well with pictures. As a consequence, the development of a reliable method for encrypting images has become an important challenge [1]. Because of its sensitivity to initial values, pseudo-randomness, and unexpected behavior, the chaotic system was first extensively used in picture encryption. This was possible due to the system's unpredictable nature. This was the first application ever submitted for this category. However, due to the fact that its encryption is based on scrambling and diffusion, it is impossible to ensure that digital picture data will remain secure. These two characteristics are the most important parts of the encryption. The chaotic state is defined by a variety of detailed properties, all of which assist to design encryption algorithms that are both safer and more robust. All of these traits contribute to the formation of the chaotic state. The Arnold, Baker, Gauss, Sine, Standard, Tent, Logistic, Lorenz, Henon map are all examples of models that are classified as chaotic [2]. It is possible to observe a reflection of the complicated structure of chaotic mapping in the qualities of some encryption processes that are comparable to perfect ciphers. These characteristics include aliasing, balancing, and diffusion, among others. In recent years, a large number of encryption models have been given in order to meet the requirements for the safety of digital photos [3]. Some of these models are based on chaotic maps, frequency domains, and fractional domains, amongst other things. Examples of frequency domain operations include the DCT, DWT, and DFT.

By combining the integer wavelet transform (IWT) with global bit scrambling (GBS), Jayashree et al. [4] were able to create a chaotic encryption of an image. This was accomplished by using the IWT. At this point in the process, image modifications and decompositions are carried out with the assistance of IWT. Following this, the encryption algorithm receives the coordinates of a map with a random layout as its input. Instead of using pixel scrambling, a key-dependent bit scrambling, also known as GBS, has been used in the encryption process in order to make it safer. In addition to the increased resistance against the assaults of trespassers, it also enhances the dependability of essential components.

Hala et al. present a technique that is both secure and efficient for the encryption and decryption of visual data (DFT) by adding chaotic Baker Maps into the discrete Fourier transform [3]. This approach can be found in their research paper. The adjusted image coefficients are put via an action in the frequency domain that is given by a baker map. This allows the suggested method to reach a high degree of encryption efficiency than it would have otherwise been capable of.An image encryption method that is based on a six-dimensional hyperchaotic system and DNA encoding has been proposed by Mengmeng et al. in order to address the problem of inadequate levels of security that are present in previously developed image encryption algorithms [1]. This method was developed by Mengmeng and his colleagues. Dalia et al. has proposed a picture encryption system that is based on RSA and AES [5]. The purpose of this research is to evaluate the performance of the Advanced Encryption Standard (AES) and the Rivest-Shamir-Adleman (RSA) encryption algorithms in the context of picture encryption using MATLAB. The comparison is going to be based on an analysis of how well each algorithm encrypts pictures, and this analysis will serve as the foundation for the comparison. In addition to this, doing an analysis of the data about the correlation, as well as the histogram. According to the data, the AES approach provides photo encryption of a higher quality than any other method, as seen by the more converging column locations in the histogram. In addition, the AES method has a propensity to have a correlation coefficient that is closer to zero, which is indicative of a stronger link. A novel picture encryption technique that is based on two-dimensional Lorenz and Logistic has been proposed by Tao et al. [6]. Both of these chaotic mapping strategies have a relatively modest level of complexity. The image is encrypted and decrypted using the two-dimensional Lorenz chaotic model, which yields chaotic sequences that are used in both procedures. These sequences are used to encrypt and decrypt the picture. Corina et al. have come up with a better method of encrypting images by using Haar wavelet packets decomposition in conjunction with four chaotic maps [7]. This method was given in their paper. We recommend making use of a permutation that is generated from the Baker chaotic map in order to jumble up the wavelet packets since this is the most effective method. The use of two distinct chaotic maps contributes to an increase in the level

of entropy inside the ciphered image as well as within the key space of the cryptosystem. These maps consist of the three-dimensional Arnold map, which is used in a manner that is applied twice, as well as the tent map, which is combined with the logistic map.The authors of this paper presented a technique for encrypting images by making use of a chaos-based algorithm that included Arnold transform and logistic map as well as discrete cosine transform.

II. Related Work:

The generation of non-linear, complicated, and random sequences may be accomplished with the help of chaotic maps. The output of these kind of maps is very sensitive to both the beginning circumstances and the control settings. When we employ chaotic maps in cryptography, these parameters may be handled in the same manner as secret keys. Because of this feature of chaotic maps, using these kinds of architectures in contemporary cryptography seems to be an obvious choice.

Logistic Map:

A chaotic system that uses a logistic map is one example. It is a non-linear map in discrete time that only has one dimension, and its non-linearity is quadratic [8]. The equation of state for the logistic map is as follows:

$$y_{n+1} = u * y_n * (1 - y_n) \qquad (1)$$

Discrete Cosine Transform:

The Discrete cosine transform (DCT), initially described by Nasir Ahmed in 1972, is a generally applied transformation approach for image encryption and reduction. A fixed collection of data sets in proportion to the number of cosine expressions vibrating at different frequencies is known as the DCT [9].

Arnold Transform:

The Arnold transform is a common component of a variety of image processing techniques, including those for stenography, authentication, security controls, self-recovery, and encryption. In each of these instances, the Arnold transform is used as a step in the scrambling process; the number of iterations serves as the key for this phase [10].

III. Method:

In this section, both the encryption and decryption procedures, which are part of the proposed functioning of the cryptosystem, are broken down into their component parts and introduced. The encryption and decryption sequences are shown in **Fig.1** and **2**.

Encryption

The following steps provide an explanation of a procedure for encrypting data in order to convey a picture that has been encrypted:

1. Read an input image I_1 at sender side
2. Apply the Arnold Transform on image I_1 and get image A_1
3. Apply Discrete Cosine Transform A_1 and get image D_1
4. Apply Logistic map on image D_1 and get encrypted image E_1

Fig. 1 Encryption Process

Decryption

As soon as the encrypted picture is sent to the recipient, the process of decryption may begin. This occurs via a series of inverse operations, which can be broken down into the following steps:

1. Read encrypted image E_1 at receiver side
2. Apply the Inverse Arnold Transform on image E_1 and get image A_2
3. Apply Discrete Cosine Transform A_2 and get image D_2
4. Apply Logistic map on image D_2 and get decrypted image I_2

Fig. 2 Decryption Process

IV. RESULTS:

This chapter will employ some standard 256×256 images like Cameraman, Lena in order to demonstrate that the image encryption and decryption techniques discussed in this article are applicable in real-world scenarios. **Fig. 3** and **4** illustrated the original, encrypted, and decrypted images with their histograms respectively. The performance of the system would be evaluated based on a number of well-known metrics, including the Peak Signal to Noise Ratio (PSNR), Correlation Coefficient, and Similarity Index (SSIM) shown in **Table 1**.

The ratio of the greatest potential value (power) of a signal or picture to the power of distorting noise that affects the quality of its representation is referred to as the peak signal-to-noise ratio (PSNR). The structural similarity index, also known as the SSIM index, is a tool for determining the degree to which two photographs are similar to one another. The concept of structural information refers to the notion that the pixels have substantial inter-dependencies, particularly when they are located in close proximity to one another. The correlation coefficient measures the degree to which two adjacent pixels in a picture are related to one another. In general, correlation assesses how similar two pixels are to one another by measuring the degree of similarity. For encrypted image, it should be minimum or negative. **Fig. 5** explains the graphical form of correlation for Cameraman image.

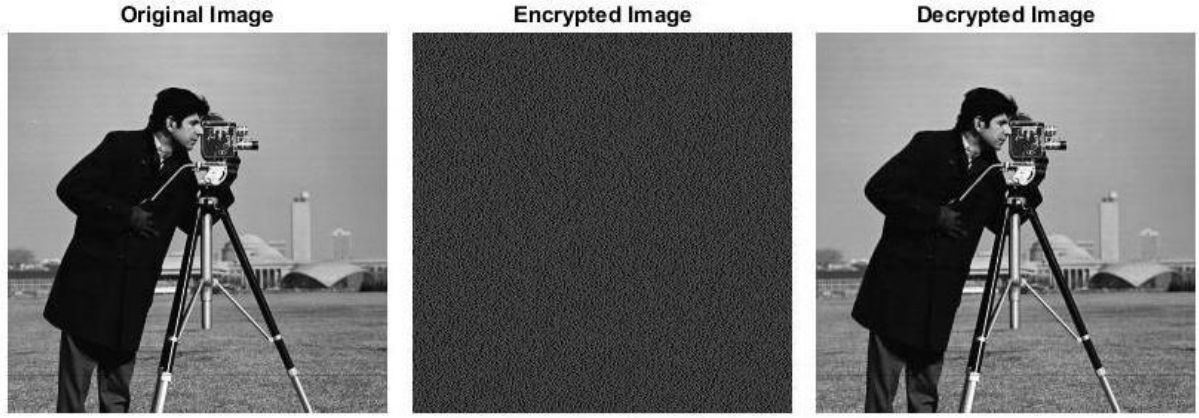

Fig. 3 Simulation results in image form

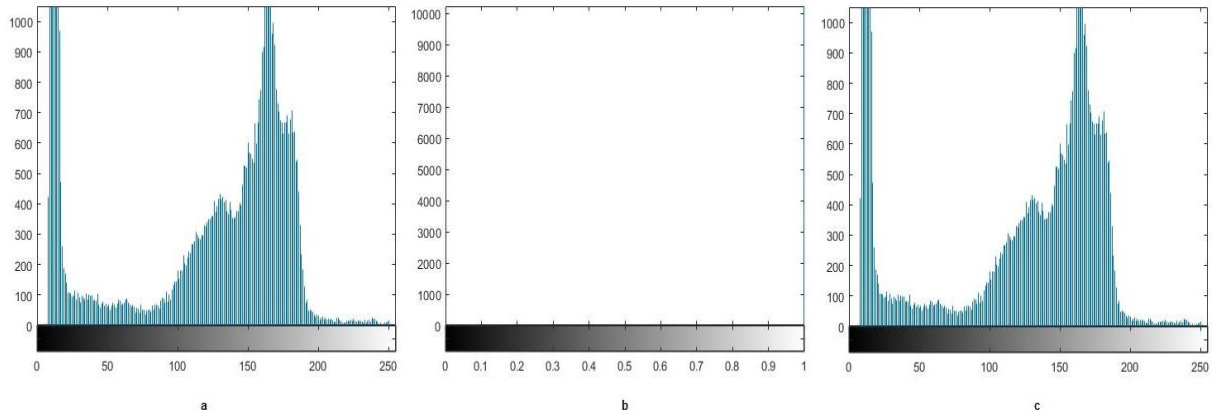

Fig. 4 Simulation results in histogram form

Table 1 PSNR, SSIM and Correlation analysis on proposed method

Image	*PSNR*	*SSIM*	*Horizontal Correlation of Encrypted Image*	*Vertical Correlation of Encrypted Image*	*Diagonal Correlation of Encrypted Image*
Cameraman	Inf	1	-0.3864	0.0354	-0.0261
Lena	Inf	1	-0.4088	0.0118	-0.0023

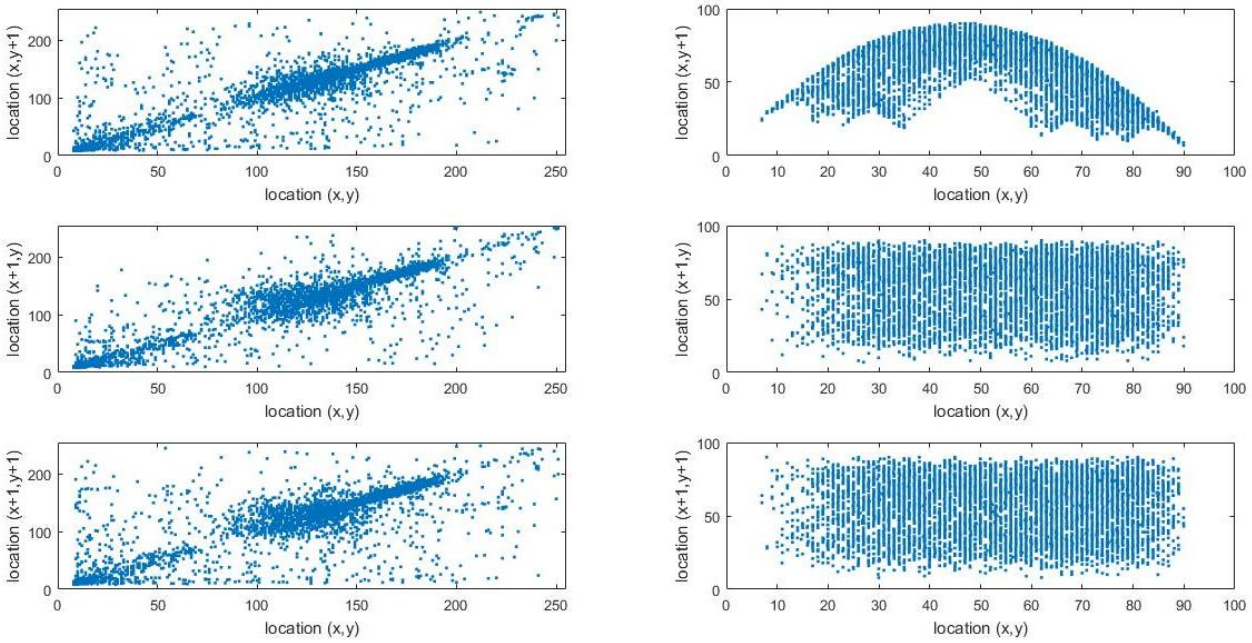

Fig. 5 Correlation analysis of Cameraman image

V. CONCLUSION:

In the suggested study, an easy-to-implement approach for encrypting confusion images was presented. The chaotic logistic map, Arnold, and the discrete cosine transform were used in both the encipherment and decipherment procedures. Several different types of security checks are performed on the proposed method. The findings demonstrate a low degree of correlation between neighboring pixels, a strong encryption effect, and resistance to statistical analysis and simulation results have shown that the proposed technique is both fast and secure.

REFERENCES:

[1] M. Zhang and W. Wu, "Research on Image Encryption Technology Based on Hyperchaotic System and DNA Encoding," in 2021 IEEE International Conference on Artificial Intelligence and Industrial Design, AIID 2021, 2021, doi: 10.1109/AIID51893.2021.9456457.

[2] G. Veena and M. Ramakrishna, "A Survey on Image Encryption using Chaos-based Techniques," Int. J. Adv. Comput. Sci. Appl., vol. 12, no. 1, 2021, doi: 10.14569/IJACSA.2021.0120145.

[3] H. S. El-Sayed, A. Afifi, M. A. AlZain, and O. S. Faragallah, "An image cryptosystem using chaotic baker map in DFT," in 2021 International Conference of Women in Data Science at Taif University, WiDSTaif 2021, 2021, doi: 10.1109/WIDSTAIF52235.2021.9430208.

[4] J. Karmakar and M. K. Mandal, "Chaos-based image encryption using integer wavelet transform," in 2020 7th International Conference on Signal Processing and Integrated Networks, SPIN 2020, 2020, doi: 10.1109/SPIN48934.2020.9071316.

[5] D. M. Alsaffar et al., "Image Encryption Based on AES and RSA Algorithms," in ICCAIS 2020 - 3rd International Conference on Computer Applications and Information Security, 2020, doi: 10.1109/ICCAIS48893.2020.9096809.

[6] T. Li, B. Du, and X. Liang, "Image Encryption Algorithm Based on Logistic and Two-Dimensional Lorenz," IEEE Access, vol. 8, 2020, doi: 10.1109/ACCESS.2020.2966264.

[7] C. MacOvei, M. Raducanu, and O. Datcu, "Image encryption algorithm using wavelet packets and multiple chaotic maps," in 2020 14th International Symposium on Electronics and Telecommunications, ISETC 2020 - Conference Proceedings, 2020, doi: 10.1109/ISETC50328.2020.9301088.

[8] B. Ahuja and R. Doriya, "A novel hybrid compressive encryption cryptosystem based on block quarter compression via DCT and fractional Fourier transform with chaos," Int. J. Inf. Technol., 2021, doi: 10.1007/s41870-021-00759-y.

[9] P. Sreenivasulu and S. Varadharajan, "Algorithmic Analysis on Medical Image Compression Using Improved Rider Optimization Algorithm," in Lecture Notes in Networks and Systems, vol. 103, 2020.

[10] P. K. Kulkarni and G. Kulkarni, "A Copyright Protection Scheme for Grayscale Images Using Wavelet Transform and Arnold Transform," in Proceedings of B-HTC 2020 - 1st IEEE Bangalore Humanitarian Technology Conference, 2020, doi: 10.1109/B-HTC50970.2020.9298018.