Image Encryption-Decryption using modified Linear Canonical Transformation (LCT) algorithm

Avinash kumar Ahirwar[1], Kalpana Tiwari[2]

[1]M.Tech Scholar, [2]Assistant Professor
Department of Electronics and Communication, VITS, Satna,

***Abstract*: In recent years, the chaos based cryptographic algorithms have suggested some new and efficient ways to develop secure image encryption techniques. In this communication a number of methods have recently been proposed in the literature for the encryption of two-dimensional information by use of optical systems based on the linear canonical transform. Typically, these methods require random phase screen keys for decrypting the data, which must be stored at the receiver and must be carefully aligned with the received encrypted data. Encryption of images is different from that of texts due to some intrinsic features of images such as bulk data capacity and high redundancy, which are generally difficult to handle by traditional methods. Due to the exceptionally desirable properties of mixing and sensitivity to initial conditions and parameters of chaotic maps, chaos-based encryption has suggested a new and efficient way to deal with the intractable problem of fast and highly secure image encryption.**

***Keywords*: Cryptographic algorithms, linear canonical, image encryption**

1. Introduction

Information security is one of the most important issues now-a-days where information is sent from one place to another with fast rates. The multitude of digital data usage in medical, defense, military, banking and other multimedia applications drives the concept of digital data authentication. The best way to transfer a huge amount of digital data is in the form of an image. Due to the inherent property of the image, such as huge information capability and high correlation between pixels, it is chosen for encryption algorithms. There are many image encryption algorithms that used chaotic map, logistic map, advanced encryption standard, Arnold map, affine transform, Fourier transform, and fractional Fourier transform. The researcher has completed the encryption goal only by shrinking image pixels, some have changed the spatial image domain in the frequency domain by using Fourier transform. Some have used the double-coding technique of the Fourier Plane, which uses the two statistically independent random phase masks together with the Fourier transform. Extending Fourier transform is a fractional figurative transformation, which is also largely applied in the field of image encryption. These techniques do not meet the image authentication requirements against malicious users. Recently, canonical linear transformation is applied to the multitude in the double image encryption process due to its inherent property.

2 Image Encryption

Image encryption is the process of encoding the image, so interlocutors or hackers cannot read it, but authorized parties can. In an encryption scheme, the image is encrypted using an encryption algorithm, transforming it into an unread image. This is usually done using encryption keys, which specify how the image will be encoded. Any opponent who can see the encrypted image should not be able to determine anything about the original image. An authorized party, however, is able to decrypt the encrypted image using a decryption algorithm. This usually requires a secret decryption key so that opponents do not have access.

2.1 Image encryption (Security Goals)

There are three security objectives: privacy, integrity and availability. These are described as follows.

Fig. 1.1: Taxonomy of security goals

3. Mathematical modeling

Linear canonical transform

Linear canonical transformation (LCT) is an integral transformation family that generalizes many classical transformations. It has 4 parameters and 1 constraint, so it is a three-dimensional family and can be visualized as the action of the special SL2 (R) linear group on the time-frequency domain (domain).

The LCT generalizes the Fourier, called "linear canonical transformation," is a canonical transformation, a map that preserves the simplex structure, SL2 (R) can also be interpreted as the Sp2 simplex group and thus the LCTs are the linear maps of the frequency domain of time that preserves its simplistic form.

A. Definition

LCT is the generalization of conventional Fourier and Fourier Transform fractional transformation with three parameters including a number of transformations used in digital signal processing and imaging (Adrian Sternet al., 2006). Among its special class are Fourier Transform (FT), Fractional Fourier Transform (FRFT). The LCT of a transformable signal f (t) is defined as:

$$F_{a,b,c,d} = \begin{cases} \sqrt{-i\frac{b}{a}}\, e^{i\frac{d}{2b}u^2} \int_{-\infty}^{\infty} e^{-i\frac{2\pi}{b}ut} e^{i\frac{a}{2b}t^2} f(t)\,dt & \text{when } b \neq 0 \\ \sqrt{d}\, e^{i\frac{(c d u^2}{2}} f(t)\,du & \text{when } b = 0 \end{cases} \qquad (3.1)$$

If the constants a, b, c, d are linked to the unitary matrix M, also called a modular unit matrix and represented as:

$$M=\begin{bmatrix} a & b \\ c & d \end{bmatrix} \quad (3.2)$$

With constraint ad - bc = 1. The elements a, b, c, d transmit the same information as the three parameters α, βand γ which convey that define LCT. Its relation to elements a, b, c, d is given below:

$$M=\begin{bmatrix} a & b \\ c & d \end{bmatrix}=\begin{bmatrix} \frac{\gamma}{\beta} & \frac{1}{\beta} \\ -\beta+\frac{\alpha\gamma}{\beta} & \frac{\alpha}{\beta} \end{bmatrix}$$

$$=\begin{bmatrix} \alpha/\beta & -1/\beta \\ \beta-\alpha\gamma/\beta & \gamma/\beta \end{bmatrix}$$

FRFT can be converted from LCT if the following constraints are complied with.

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}=\begin{bmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{bmatrix} \quad (3.4)$$

The LCT calculation can be made from the two different methods. The first method is based on LCT decomposition in fractional Fourier transform followed by scaling and multiplication of Chirp. The second method is based on LCT decomposition in Chirp multiplication, Fourier transform and scaling.

4. Results and Discussion

Fig: 4.1: image encryption decryption

Fig: 4.2 select image

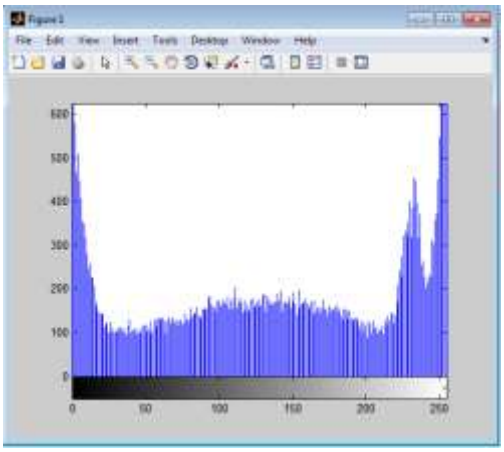

Fig: 4.3 graph

Fig: 4.4 encrypt image

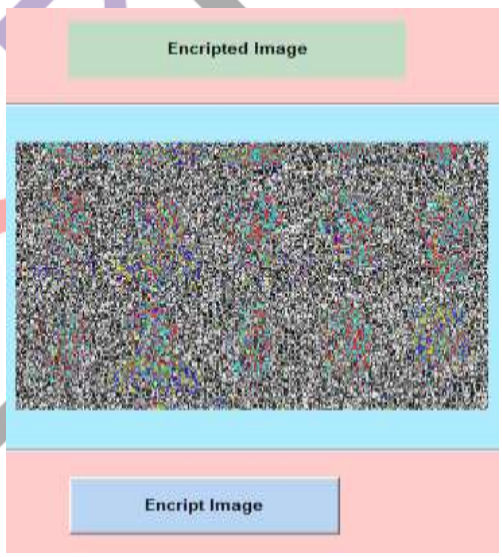

Fig: 4.5 encrypted image

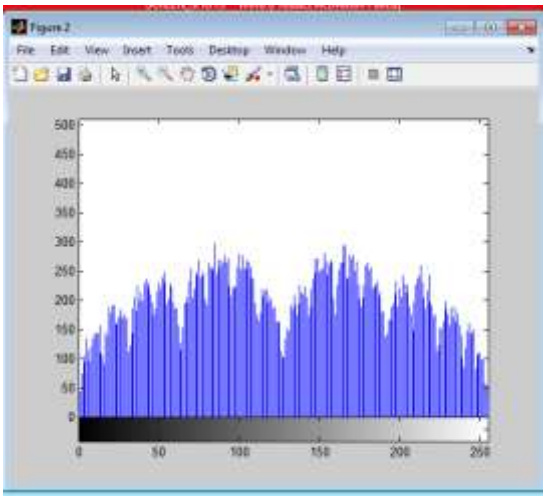

Fig: 4.6 encrypted image graph

Fig: 4.7 encrypted image

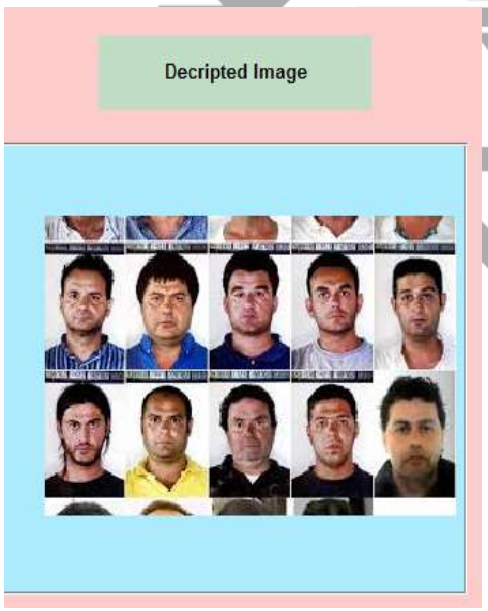

Fig: 4.8 decrypted image

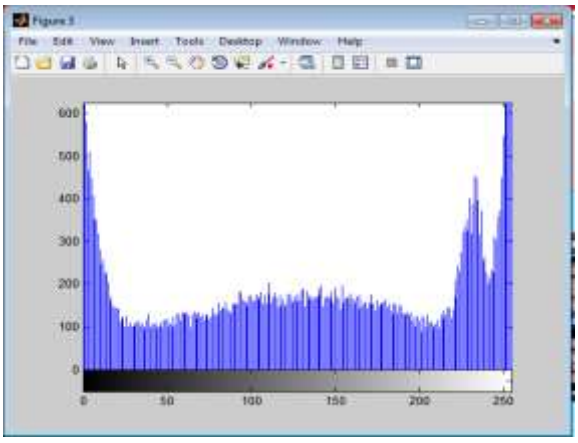

Fig: 4.9 image decrypted graph

Fig: 4.10 image decrypted graph and image

Conclusion

In this communication, a new way of image encryption scheme have been proposed which utilizes two chaotic logistic maps and an external key of 80-bit. The initial conditions for both the logistic maps are derived using the external secret key by providing weightage to its bits corresponding to their position in the key. In the proposed encryption process, eight different types of operations are used to encrypt the pixels of an image and which operation will be used for a particular pixel is decided by the outcome of the logistic map. To make the cipher more robust against any attack, the secret key is modified after encrypting a block of sixteen pixels of the image. We have carried out statistical analysis, key sensitivity analysis and key space analysis to demonstrate the security of the new image encryption procedure. Finally, we conclude with the remark that the proposed method is expected to be useful for real time image encryption and transmission applications.

References

[1] Chuang, C., Lin, G. "Adaptive Steganography-based Optical Color Image Cryptosystems", in IEEE International Symposium on Circuits and Systems, ISCAS 2009, pp.1669- 1672.

[2] Dong, Y. , Liu, L., Zhu, C., Wang, Y., "Image Encryption Algorithm Based on Chaotic Mapping", in 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT), 2010, Vol. 1, pp. 289-291.

[3] Du,N., Devineni, S. and Grigoryan, A. M., "Mixed Fourier Transforms And Image Encryption", in IEEE International Conference on Systems, Man and Cybernetics, SMC 2009, 2009, pp. 547-552.

[4] Fan,J., Zhang, Y., "Color image encryption and decryption based on double random phase encoding technique", in Symposium on Photonics and Optoelectronics, SOPO, 2009, pp. 1-6.
[5] Feng,X., Tian, X., Xia, S., "A Novel Image Encryption Algorithm Based On Fractional Fourier Transform and Magic Cube Rotation", in 4th International Congress on Image and Signal Processing (CISP), 2011, Vol. 2, pp. 1008-1011.
[6] Healy,J. J. and Sheridan, J. T., "Fast linear canonical transforms", in Optical Society of america, 2010, Vol. 27, No. 1, pp. 21-30
[7] Hennelly,B. M. and Sheridan,J. T., "Fast numerical algorithm for the linear canonical transform", in journal optical society of America, 2005, vol. 22, No. 5, pp. 928-937.
[8] Huang, Q. and Liu,J., "Secure Image Encryption Technique Based on Multiple Fresnel Diffraction Transforms", in International Conference on Wireless, Mobile and Multimedia Networks, 2006, pp. 1 4.
[9] Hwang,H., Han, P., "A Novel Wavelet Transform Algorithm for Image Encryption", in Australian Conference on Optical Fiber Technology & Australian Optical Society, 2006, pp. 1.
[10] Jiang,A., Yu, J., Cang, X. "Image Encryption Algorithm Based on Chaos and Contourlet Transform", in First International Conference on Pervasive Computing Signal Processing and Applications (PCSPA), 2010, pp. 707-710.