International Journal of Engineering, Applied and Management Sciences Paradigms, Vol. 15, Issue 01, May 2014
An Indexed and Referred Journal
ISSN (Online): 2320-6608
www.ijeam.com

A Survey on Chaos Based Image Encryption and FRFT

Charu Rohatgi[1], Saroj Behal[2]

[1]M.Tech. Scholar, C.B.S Group of Institutions, Fatehpuri, Jhajjar
[2]Assistant professor, C.B.S Group of Institutions, Fatehpuri, Jhajjar
[1]*charu2010dia@gmail.com*

Abstract

Image encryption is the process to convert a image into a unreadable format. The image encryption is necessary for security in various transmissions. The encryption technique must be reliable and lossless i.e. no loss after decryption as compared to original image. FRFT i.e. is generalized version of fourier transform can be used for image encryption. This paper describes the image encryption and various schemes of image encryption. The paper also reviews FRFT and work done in image encryption.

Keyword: *FRFT, FT, Image encryption, CHAOS.*

Introduction

Images are generally the collection of pixels. Basically Image Encryption means that convert the image into unreadable format. Many digital services require reliable security in storage and transmission of digital images. Due to the rapid growth of the internet in the digital world today, the security of digital images has become more important and attracted much attention. The prevalence of multimedia technology in our society has promoted digital images to play a more significant role than the traditional texts, which demand serious protection of user's privacy for all applications. Encryption techniques of digital images are very important and should be used to frustrate opponent attacks from unauthorized access [1].

Data Encryption is one of the widely used techniques for data protection.[2] In Data Encryption, data is converted from its original to other form so that information cannot be accessed from the data without decrypting the data as shown in figure 1 i.e the reverse process of transforming cipher text back to plain text is called as decryption [3]. The original data is usually referred as plain data and the converted form is called cipher data. Encryption can be defined as the art of converting data into coded form which can be decode by intended receiver only who poses knowledge about the decryption of the ciphered data. Encryption can be applied to text, image, video for data protection [2].

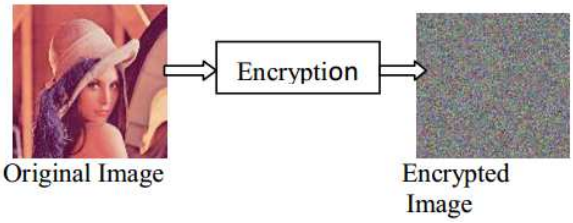

Figure 1: Image Encryption [3]

It can be noticed that most of the image encryption designs are in the form of block cipher, which is usually considered faster than its counterpart, stream cipher, that processes data byte-by-byte (or in other data format sequentially), although stream cipher may provide better security under the concept of perfect security. In this paper, it is demonstrated that a well-designed chaos-based stream cipher can be a good candidate and may even outperform the block cipher, on speed and security [4].

Chaos-based image encryption scheme:

H.S. Kwok [4] proposed a chaos-based image encryption system, in the framework of stream cipher architecture The block diagram of the system is shown in Fig. 2. An image is firstly converted to a binary data stream. By masking these data with a random key stream generated by a chaos-based pseudo-random key stream generator (PRKG), the corresponding encrypted image is formed. The details of each component are to be discussed in the following sections. As demonstrated in their simulation, this approach is light-weighted and performed well both in security and speed [4].

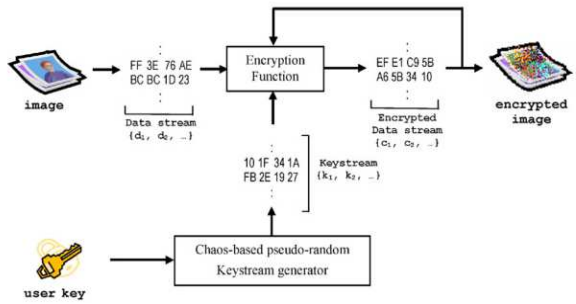

Figure 2: Chaos-based image encryption scheme [4]

In common usage, chaos means a state of disorder. Since there is no universally accepted mathematical definition of chaos, a commonly used definition is that, for a dynamical system to be said as chaotic, it must have the following properties: 1) It must be sensitive to initial conditions, 2) Its periodic orbit must be dense, and 3) It must be topologically mixing. Sensitive to initial conditions means that a small difference in the initial conditions will produce widely diverging outcomes for chaotic systems, so that long-term prediction is impossible. The topological mixing (or topological transitivity) property ensures the ergodicity of a chaotic map, which means that if we partition the state space into a finite number of regions, no matter how many, any orbit of the map will pass through all these regions [5]

Jinhui Lai, Song Liang, Delong Cui, [6] proposed a novel image encryption algorithm based on chaotic system and fractional Fourier transform. The image encryption process includes two steps: first the image is encrypted by employing Fractional Fourier domain double random phase, then the confusion image is encrypted by using confusion matrix which is generated by chaotic system, and finally the cipher image is obtained. The security of the proposed algorithm depends on the sensitivity to the randomness of phase mask, the orders of FRFT and the initial conditions of chaotic system [6].

Fractional Fourier transform (FRFT)

FRFT is a generalization of FT. It is not only richer in theory and more flexible in application, but is also not expensive in implementation. It is a powerful tool for the analysis of time-varying signals. With the advent of FRFT and related concepts, it is seen that the properties and applications of the conventional FT are special cases of those of the FRFT. However, in every area where FT and frequency domain concepts are used, there exists the potential for generalization and implementation by using FRFT [7].

FT of a function can be considered as a linear differential operator acting on that function. The FRFT generalizes this differential operator by letting it depend on a continuous parameter a. Mathematically, a^{th} order FRFT is the a^{th} power of FT operator [7].

The FRFT of a function $s(x1)$ can be given as:

$$F^a[s(x_1)] = S(x)$$
$$= \frac{exp\ i(\frac{\pi}{4}-\frac{\pi}{2})}{\sqrt{2\pi \sin\alpha}} \exp\left(-\frac{i}{2}x^2 \cot\alpha\right) \int_{-\infty}^{\infty} \exp\left(-\frac{i}{2}x^2 \cot\alpha - \frac{ix_1x}{\sin\alpha}\right) s(x_1)dx_1 \quad (1)$$

and the inverse FRFT can be given as

$$F^{-a}[s(x_1)]$$
$$= \frac{exp\ -i(\frac{\pi}{4}-\frac{\pi}{2})}{\sqrt{2\pi \sin\alpha}} \exp\left(+\frac{i}{2}x^2 \cot\alpha\right) \int_{-\infty}^{\infty} \exp\left(+\frac{i}{2}x^2 \cot\alpha - \frac{ix_1x}{\sin\alpha}\right) s(x_1)dx_1 \quad (2)$$

where $\alpha = a\pi/2$.

Different cases are discussed :

(1) When $\alpha = \pi/2$, i.e. a = 1

$$F^a[s(x_1)] = F^1[s(x_1)]$$
$$= \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} s(x_1) \exp(-ixx_1)\, dx_1 \quad (3)$$

is the ordinary Fourier transform

(2) When $\alpha = 0$, i.e. a = 0, the transform kernel reduces to identity operation. When α aapproaches 0, $\sin\alpha$approaches α,

$\cot\alpha$ approaches $1/a$ and using the fact in the sense of generalized functions

$$\lim_{\varepsilon\to 0}\frac{1}{\sqrt{i\pi\varepsilon}}\exp\left(-\frac{x^2}{i\varepsilon}\right)=\delta(x)$$

$$F^0[s(x_1)]=\int_{-\infty}^{\infty}\delta(x-x_1)s(x_1)\,dx_1 = s(x_1) \quad (4)$$

(3) When $\alpha=\pi$, i.e. a = 2 and the result turns out to be

$$F^2[s(x_1)]=\int_{-\infty}^{\infty}\delta(x+x_1)s(x_1)\,dx_1 = s(-x_1) \quad (5)$$

So, for an angle from 0 to 2π, they have the values of a from 0 to 4. It can be shown that the transform kernel is periodic with a period 4. Table I gives the various kernels of FRFT for variation of a from 0 to 4.

The FRFT of a function is equivalent to a four-step process:

1. Multiplying the function with a chirp,
2. Taking its Fourier transform,
3. Again multiplying with a chirp, and
4. Then multiplication with an amplitude factor.

The above-described type of FRFT is also known as Chirp FRFT (CFRFT)

Related Work

Bhagyashri R.Pandurangi [8] discussed various techniques for image encryption using fractional Fourier transform and chaotic functions are . Fractional Fourier transform is one of the efficient tools in signal and image processing and encryption, pattern recognition and classification. Chaotic functions are characterized by sensitive dependence on initial conditions, similarity to random behavior. These two functions can be combined to encrypt and decrypt the image reliably.

Yan Zhang [9] proposed a new algorithm for optical image encryption based on iterative FRFT. Comparing with the conventional Fourier transform, FRFT can provide more parameters which can serve as keys to make encryption system more secure. It is very difficult for an unauthorized person to access the right encrypted image. Furthermore, the complexities can be controlled by manipulation of the number of iterations and of the fractional order. When K= 2 and P = 1, the simple architecture we proposed will reduce to the configuration proposed by Javidi et al. The results have shown the validity of this new algorithm and its optical implementation configuration was suggested.

Ashutosh [10] said that growing with the fast evolution of digital data exchange, security information becomes much important in data storage and transmission. Due to the increasing use of images in industrial process, it is essential to protect the confidential image data from unauthorized access. The security system based on the fractional Fourier transform (FRFT) is protected by only a certain order of FRFT. In this paper, They proposed a novel method to encrypt an image by using Discrete Fourier Transform (DFT) and Fractional Fourier Transform (FRFT). In this search, they analyze the image encryption using DFT and FRFT based on double random phase matrix. The implementation of both techniques has been realized for experimental purposes.

Rinki Pakshwar [11] focused mainly on the different kinds of image encryption and decryption techniques. In addition focuses on image encryption techniques, As the use digital techniques for transmitting and storing images are increasing, it becomes an important issue that how to protect the confidentiality, integrity and authenticity of images. There are various techniques which are discovered from time to time to encrypt the images to make images more secure. In this search, a Survey of Different Image Encryption and encryption techniques that are existing is given. It additionally focuses on the functionality of Image encryption and decryption techniques.

Mintu Philip [12] Chaotic Encryption Method seems to be much better than traditional encryption methods used today. Chaotic encryption is the new direction of cryptography. It makes use of chaotic system properties such as sensitive to initial condition and loss of

information. Many chaos-based encryption methods have been presented and discussed in the last two decades. In order to reach higher performance, these methods take advantage of the more and more complex behavior of chaotic signals. This search contributes by comparing and analyzing the performance of the past chaotic image encryption schemes.

Conclusion

The paper has studied the fractional Fourier transform and image encryption schemes. The FRFT can be used for image encryption. The paper also describes the various existing image encryption schemes. In future, FRFT can be enhanced to encrypt the image to increase the reliability of encryption.

References

[1] Yadav, Ravi Shanker, M. H. D. R. Beg, and MANISH MADHAVA Tripathi. "Image Encryption Techniques: A Critical Comparison." International Journal of Computer Science Engineering and Information Technology Research 3, no. 1 (2013): 67-74.

[2] Divya, V. V., S. K. Sudha, and V. R. Resmy. "Simple and Secure Image Encryption." International Journal of Computer Science Issues (IJCSI) 9, no. 6 (2012).

[3] Kaur, Rajinder, and Er Kanwalprit Singh. "Image Encryption Techniques: A Selected Review." IOSR Journal of Computer Engineering (IOSR-JCE)e-ISSN: 2278-0661, p-ISSN: 2278-8727Volume 9, Issue 6 (Mar. - Apr. 2013).

[4] Kwok, H. S., and Wallace KS Tang. "A fast image encryption system based on chaotic maps with finite precision representation." Chaos, solitons & fractals 32, no. 4 (2007): 1518-1529.

[5] Ephin M, Judy Ann Joy, N. A. Vasanthi," " Survey of Chaos based Image Encryption and Decryption Techniques", Amrita International Conference of Women in Computing (AICWIC'13) Proceedings published by International Journal of Computer Applications® (IJCA)

[6] Lai, Jinhui, Song Liang, and Delong Cui. "A novel image encryption algorithm based on fractional Fourier transform and chaotic system." In Multimedia Communications (Mediacom), 2010 International Conference on, pp. 24-27. IEEE, 2010.

[7] Saxena, Rajiv, and Kulbir Singh. "Fractional Fourier transform: A novel tool for signal processing." Journal of the Indian Institute of Science 85, no. 1 (2013): 11.

[8] Pandurangi, Bhagyashri R., S. R. Hiremath, and Meenakshi R. Patil. "Fractional Fourier Transform Based Image Encryption using chaos: A review." International Journal of Latest Trends in Engineering and Technology (IJLTET).

[9] Zhang, Yan, Cheng-Han Zheng, and Naohiro Tanno. "Optical encryption based on iterative fractional Fourier transform." Optics Communications 202, no. 4 (2002): 277-285.

[10] Ashutosh, Deepak Sharma "Image Encryption Using Discrete Fourier Transform and Fractional Fourier Transform", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-2, Issue-4, April 2013.

[11] Rinki Pakshwar, Vijay Kumar Trivedi, Vineet Richhariya, "A Survey On Different Image Encryption and Decryption Techniques", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 4 (1) , 2013,

[12] Mintu Philip, Asha Das , "Survey: Image Encryption using Chaotic Cryptography Schemes", IJCA Special Issue on "Computational Science - New Dimensions & Perspectives" NCCSE, 2011.