International Journal of Engineering Sciences Paradigms and Researches (IJESPR)
(Vol. 21, Issue 01) and (Publishing Month: June 2015)
(An Indexed, Referred and Impact Factor Journal)
ISSN (Online): 2319-6564
www.ijesonline.com

Enhanced Image Encryption using Fractional Fourier Transform

Sunil Kumari[1] and Kavita Kathuria[2]

[1]M. Tech. Scholar, Department of Computer Science & Engineering, Shri Baba Mastnath Engineering College, Rohtak (Haryana)
sunilkumari127012@gmail.com

[2]Assistant Professor, Department of Computer Science & Engineering, Shri Baba Mastnath Engineering College, Rohtak (Haryana)

Abstract

Image encryption is the process to convert an image to non-understandable form. The image encryption must be highly secured so that the un-authentic person can't get the original image. The paper proposes a technique that uses the scrambling of the DCT blocks of original image Then the fractional Fourier transform makes the process highly secured. The resultant is highly random and the randomness of the image is shown using the entropy values. The proposed technique is better than the existing due to higher value of entropy.

Keyword: *DCT, FRFT, image encryption, block scrambling.*

Introduction

The field of encryption is becoming very important in the present era in which information security is of utmost concern. Security is an important issue in communication and storage of images, and encryption is one of the ways to ensure security. Image encryption has applications in internet communication, multimedia systems, medical imaging, telemedicine, military communication, etc [1]. Images are different from text. Although we may use the traditional cryptosystems to encrypt images directly, it is not a good idea for two reasons. One is that the image size is almost always much greater than that of text. Therefore, the traditional cryptosystems need much time to directly encrypt the image data. The other problem is that the decrypted text must be equal to the original text. However, this requirement is not necessary for image data. Due to the characteristic of human perception, a decrypted image containing small distortion is usually acceptable [1]. The initial message prepared by the sender is then converted into ciphertext prior to transmission. The process of converting plaintext into ciphertext is called *encryption*. The encryption process requires an encryption *algorithm* and a *key*. The process of recovering plaintext from ciphertext is called *decryption*. The accepted view among professional cryptographers (formalized in KIRKHOFF's law) is that the encryption algorithm should be published, whereas the key must be kept secret. In applications requiring transmission the image is first compressed, because it saves bandwidth. Then the image is encrypted, as depicted in Figure 1 [2].

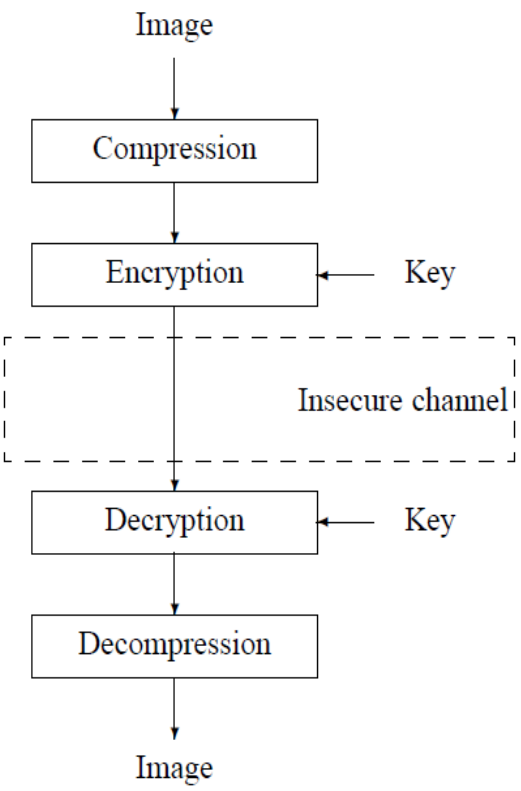

Figure 1: Encryption Of An Image[2]

The removal of redundancy enhances robustness as it squeezes out information that might be useful to a cryptanalyst. However it also introduces known patterns in the compressed bitstreams, like headers or synchronization stamps (called *markers*), that eases plaintext attacks
on the signal. An alternative would be to compress after encryption, but it would not be as efficient in terms of bandwidth because encrypted information looks random and is therefore hard to compress [2]. It is worth noting that, in schemes combining compression and encryption like the one shown in Figure 1,

- there are two kinds of information: the image and the key.
- the subjective significance of information contained in the image is ignored. For example, there is no distinction between Most Significant Bits (MSBs) and Least Significant Bits (LSBs).

From Figure 1, it is clear that the receiver should decrypt the information before it can decompress the image. With the decryption key, the receiver decrypts the bitstream, and decompresses the image. In principle, there should be no difference between a decoded image and an image that has been encrypted and decrypted. However there might be a slight though invisible difference if a watermark message has been inserted in the image. When the decrypting key is unknown, the receiver will still be able to decompress the image, but this image will significantly differ from the original. This scenario is depicted in Figure 2.

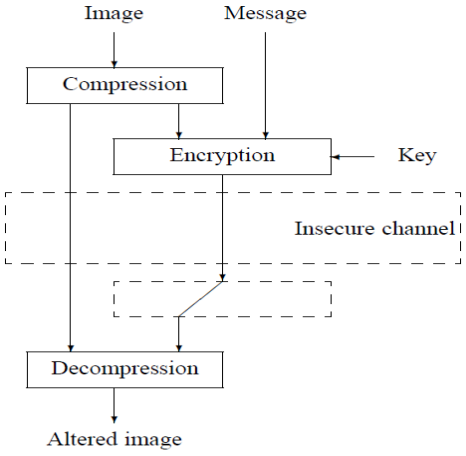

Figure 2: When the decryption key is unknown to the receiver. [2]

Fractional Fourier Transform

A number of optical image encryption systems have been proposed in recent years. A phase-encrypted memory system using cascaded extended fractional Fourier transform (FRT) is implemented. The full phase 2-D image to be encrypted is fractional Fourier transformed three times and random phase masks are placed in the two intermediate planes. The key size is increased by three times after performing FRT. The encrypted image is holographically recorded in a photorefractive crystal and is then decrypted by generating through phase conjugation, the conjugate of the encrypted image. Figures 3, and 4 shows a general scheme for image encryption and decryption, respectively [3].

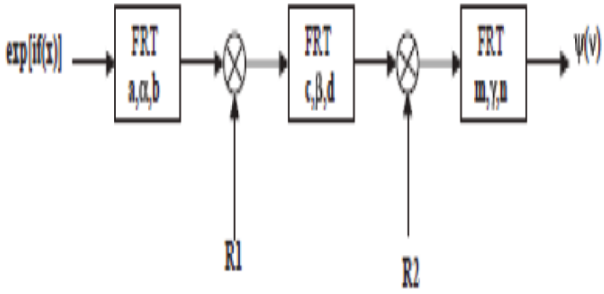

Figure 3: Image Encryption Scheme Using FFT

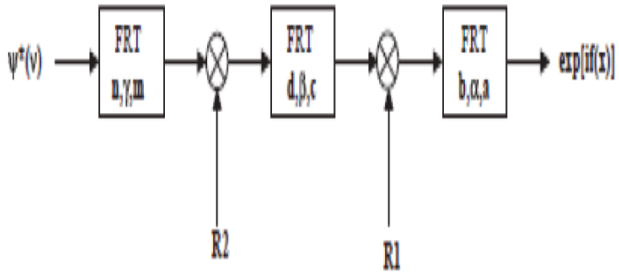

Figure 4: Image decryption scheme using FFT [3]

The encryption process takes the grayscale image and it's placed as the phase of a complex exponential, then is transformed two times and multiplied in intermediate steps by two random phase masks statistically independent, thus to obtain the encrypted image. The fractional orders applied in the transforms are decimal numbers between zero and four, generated from a key alphanumeric of six to ten characters. The decryption procedure is applied in the

inverse sense to the conjugated complex of the encrypted image. The negative of the phase of the resulting image is taken for the decryption process and the original image is obtained this way that had been encrypted. In some of the implemented cryptographic algorithms, multiple keys are used, constituted by multiple fractional orders and two random phase masks. These keys play a vital role in correct decryption providing a high level of security to image for a given application [3].

The FRFT can be seen as a linear transformation, which rotates the signal through any arbitrary angle into a mixed frequency – space domain. It can be applied to the entire field where Fourier transform is

$$\{F_p[x(t)]\}(u) = \int_{-\infty}^{\infty} x(t) K_p(u,t)\,dt$$

applied with better results like image processing, quantum physics and communication. We can define the expression for the *p*-th FRFT of a signal is defined as)[4]

(1)

Here $\alpha = \frac{p\pi}{2}$ is the angle at which FRFT is to calculate. Where *KP* is the kernel defined as

$$K_p(t,u) = \begin{cases} \sqrt{\frac{1-j\cot\alpha}{2\pi}} \exp\left(j\frac{t^2+u^2}{2}\cot\alpha - jut\csc\alpha\right) & p \neq 2n \\ \delta(t-u) & p = 4n \\ \delta(t+u) & p = 4n+2 \end{cases}$$

(2)

The FRFT is periodic with the period of 4, the transform order can be limited in the interval [-2, 2] [4].

Existing Encryption Algorithm

The existing technique of image encryption of [5] includes two steps: The original image was divided into blocks, which were rearranged into a transformed image using a transformation algorithm, and then the transformed image was encrypted using the fractional Fourier transform base algorithm. The detail of original image was divided into blocks and rearranged into a transformed image using a transformation algorithm.

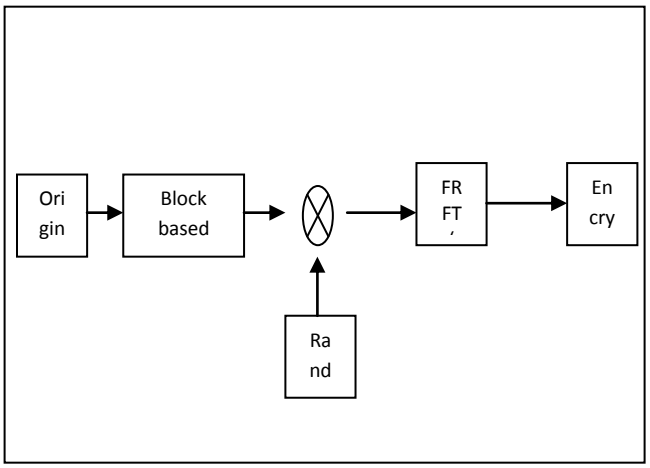

Figure 5: General block diagram of the Existing method of image encryption

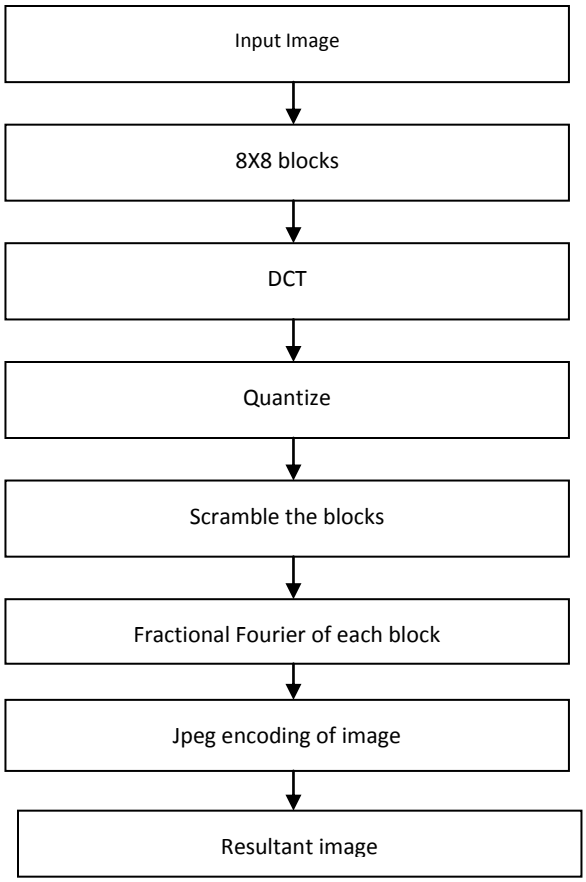

Figure 6: Proposed Image Encryption Scheme

The secret key of this approach is used to determine the seed. The seed plays a main role in building the transformation table, which is then used to generate the transformed image with different random number of block sizes. The transformation process refers to the operation of dividing and replacing an arrangement of the original image. The image can be decomposed into blocks; each one contains a specific number of pixels. The blocks are transformed into new locations. For better transformation the block size should be small, because fewer pixels keep their neighbors. In this case, the correlation will be decreased and thus it becomes difficult to predict the value of any given pixel from the values of its neighbors. At the receiver side, the original image can be obtained by the inverse transformation of the blocks. The post-processed algorithm is encryption by FRFT. Every components of block image is encrypted by employing Fractional Fourier domain random phase and the cipher image is obtained. The fractional orders applied in the transforms are decimal numbers between zero and four, generated from a key alphanumeric of six to ten characters. The framework of proposed image encryption algorithm is shown in Figure 3.

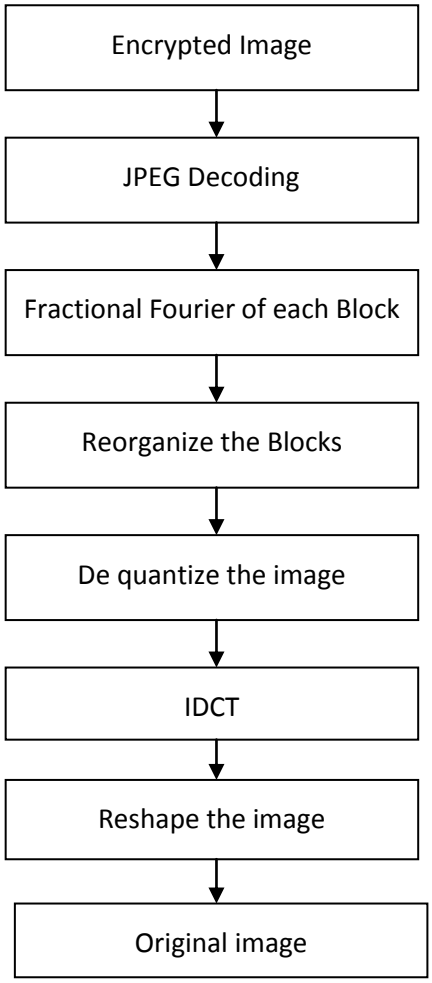

Figure 7: Proposed Image Decryption Scheme

Proposed Technique

The proposed technique uses the DCT and block scrambling and the fractional Fourier transform to encrypt the image. The process of the encryption as well as the decryption can be easily understood by the figure 6 and figure 7.

The figure 6 and 7 explains the proposed process of image encryption and image decryption. The proposed technique is designed by modifying the [4] and [5] paper technique. The effectiveness of the technique can be understood by its analysis sing the entropy parameter. The figure 8 shows the graphical analysis of the comparison.

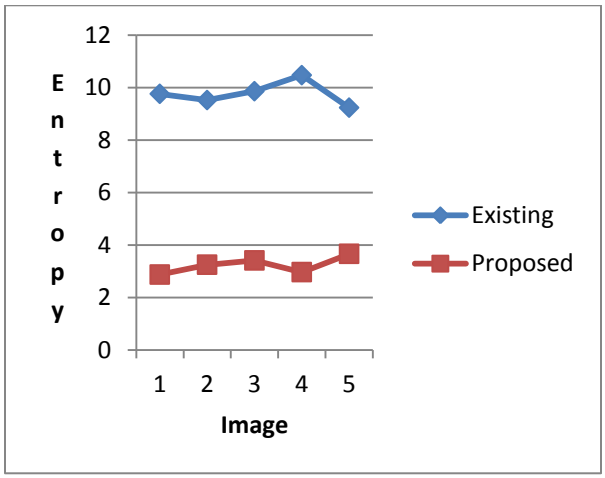

Figure 8: Entropy Comparison

The comparison shows that the entropy of the proposed technique is better than the existing technique. It means the resultant image is more random.

Conclusion

This paper proposes a DCT, fractional transform and the block scrambling based image encryption technique. The proposed technique is implemented using the MATLAB and entropy is analyzed over various images like Lena, baboon, cameraman etc. The comparison shows the better entropy of the proposed technique as compared to the existing. In future the technique can be extended to use the fuzzy sequencing of the blocks.

References

[1] Öztürk, İsmet, and İbrahim Soğukpınar. "Analysis And Comparison Of Image Encryption Algorithms." International Journal of Information Technology 1.2 (2004): 108-114.

[2] M. V. Droogenbroech and R. Benedett, "Techniques for A Selective Encryption of Uncompressed and Compressed Images", In ACIVS02, Ghent, Belgium, Proc. of Adv. Concepts for Intel. Vision Systems, 2002, pp. 90-97.

[3] Pandurangi, Bhagyashri R., S. R. Hiremath, and Meenakshi R. Patil. "Fractional Fourier Transform Based Image Encryption Using Chaos: A Review."

[4] 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.

[5] Cui, Delong, Lei Shu, Yuanfang Chen, and Xiaoling Wu. "Image encryption using block based transformation with fractional Fourier transform." In Communications and Networking in China (CHINACOM), 2013 8th International ICST Conference on, pp. 552-556. IEEE, 2013.

[6] B. K. Shreyamsha Kumar and Chidamber R. Patil, "JPEG Image Encryption using Fuzzy PN Sequences", Signal, Image and Video Processing, Vol. 4, Issue 4, pp. 419-427, Nov 2010.