INTERNATIONAL JOURNAL OF ENHANCED RESEARCH IN SCIENCE TECHNOLOGY & ENGINEERING

VOL. 2 ISSUE 1, JAN.-2013 ISSN NO: 2319-7463

An efficient image compression algorithm with reduced complexity

Madhu Sharma[1], Swati Jain[2]
[1]Biyani Group of Colleges, Jaipur, INDIA
[2]M. Tech Scholar, Jagannath University, Jaipur, INDIA
jpr.madhu@gmail.com, swatijain2323@gmail.com

Abstract: In the current scenario and with the increase in development and usage of internet and wide applications of multimedia technology, people can communicate through the digital multimedia information systems with others, very conveniently over the internet. In many cases, especially when we want to transmit a secure image data over a network and we don't want that to be browsed or processed by illegal receivers. In such cases, we would opt for a secure transaction mechanism for data transmission. Therefore, the security of digital image attracts much attention recently and many different methods for image encryption have been proposed earlier also. Image encryption has been very difficult than that of texts due to some intrinsic features of images such as bulk data capacity, high correlation among pixels and high redundancy. So the computation time of these image compression methods has a vast role. In this paper, we have proposed the enhancement and modifications to reduce the computation time in the existing image encryption-decryption methods. For this improvement, we have focussed on the image compression properties of the Discrete Wavelet Transform.

Keywords: Discrete wavelet Transform, Fractional Fourier Transform, Image Compression, Encryption, Decryption.

Introduction

In today's arena, where the internet has become the fastest and efficient medium to communicate; the security of the communication of the key entities like data, images, graphs, etc. is also extremely important and necessary. In this paper we are mainly concerned with the security of digital image as the image compression is difficult in comparison to the text compression due to its various features such as bulk data capacity, high correlation among pixels and high redundancy. Fast and efficient image encryption has been an area of interest for researchers due to the need of real-time image encryption-decryption in various fields of secret data transmission especially in case of nation's army relevant requirements and image transmission [13]. Till now various methods have been proposed earlier to encrypt the image [1]-[7]. Among those, Optical systems are of growing interest for image encryption due to their distinct advantages of processing 2-dimensional complex data in parallel and high speed. In the past, a number of optical methods have been proposed [1],[2],[4],[6],[10],[11]. Among them the most widely used and highly successful optical encryption scheme is double random phase encoding mechanism [4]. As the generalization of the conventional Fourier transform and the fractional Fourier transform has recently shown its potential in the field of optical security [1],[2],[4],[6],[11]. A number of random phase encoding schemes has been proposed [4]. It can be shown that if these random phases are statistically independent white noise then the encrypted image is also a stationary white noise. In some schemes, chaos based functions are used to generate random phase mask [2],[3],[5],[13]. In this paper, we have focussed on the issue of minimizing the computation time of image compression technique. Here, we have discussed about the image encryption and decryption methods, then the existing methodology. At last, we have introduced an algorithm to compress the image using FRT (Fractional Fourier Transform) and DWT_2 (2-dimensional discrete wavelet transform) with the reduced complexity.

Image Encryption and Decryption

As we know that an image consists of three primary colours R, G and B. Initially, an image is segregated into these three coloured channels and then the compression methods are applied on the input image channels by using DWT_2. The compressed image is encrypted using 2-D FRT and random phase masks in two successive steps. The encrypted channels are merged using $IDWT_2$, generating a coloured encrypted image. The decryption is the inverse of the encryption process. We know that a colour image $I = f(x, y)$ of size $M * N$ consists of three primary colour channels viz. RED, GREEN and BLUE. For simplicity, we assume the image size to be $N * N$. A general overview of this encryption and decryption process is as follows. As shown in fig.1, initially, the RED, GREEN and BLUE channels of the original image are segregated. Rests of the following operations are applied concurrently to these channels. Initially, the DWT_2 operation is performed over each channel to give us:

$DWT_2\{f_i(x,y)\}, \ 1 \le i \le 3$

This distribution is encoded by the first CRPM (chaotic random phase mask) which is mathematically expressed as the phase function $(i\frac{\pi}{2}S_1(x,y))$, where $S_1(x,y)$ is the random number sequence generated by the chaos function. The first 2-D FRT operation is then performed over to give us:

VOL. 2 ISSUE 1, JAN.-2013 ISSN NO: 2319-7463

$$F_{\gamma,\delta}\left\{ \mathrm{DWT}_2\{f_i(x,y)\} * \exp\left(i\frac{\pi}{2}S_1(x,y)\right)\right\}$$

Where γ, δ are the fractional orders of the first 2-D FRT and * denote the element multiplication between two matrices of the same order. The resultant is encoded by the second CRPM which is mathematically expressed as the phase function $exp(i\frac{\pi}{2}S_2(x,y))$, where $S_2(x,y)$ is the random number sequence generated by the chaos function for a different seed value than the first CRPM. The second FRT operation is then performed over this to give us:

$$F_{\alpha,\beta}\left\{F_{\gamma,\delta}\left\{ \mathrm{DWT}_2\{f_i(x,y)\} * \exp\left(i\frac{\pi}{2}S_1(x,y)\right)\right\} * \exp\left(i\frac{\pi}{2}S_2(x,y)\right)\right\}$$

where α,β are the fractional orders of the second 2-D FRT. Each channel is now operated with $IDWT_2$ to produce R, G and B channel of the encrypted image g(x,y) as per the following formulae:

$$I_1 = g(x,y) = \mathrm{IDWT}_2\left\{F_{\alpha,\beta}\left\{F_{\gamma,\delta}\left\{ \mathrm{DWT}_2\{f_i(x,y)\}\exp\left(i\frac{\pi}{2}S_1(x,y)\right)\right\} * \exp\left(i\frac{\pi}{2}S_2(x,y)\right)\right\}\right\}$$

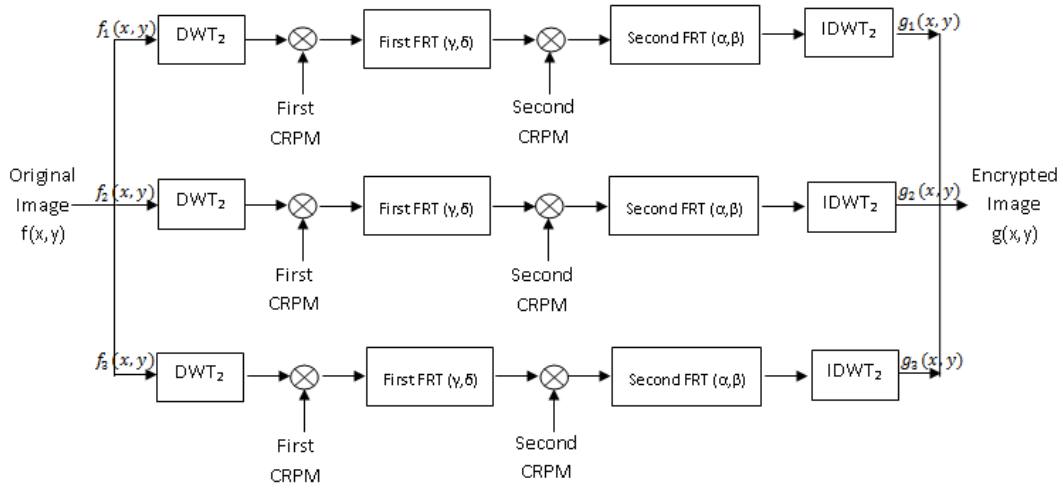

Fig. 1: Encryption process using DWT_2 in proposed algorithm

The decryption process as shown in fig 2, is the inverse of the encryption process. The DWT_2 operation is performed over g(x,y), the encrypted image, to give us:

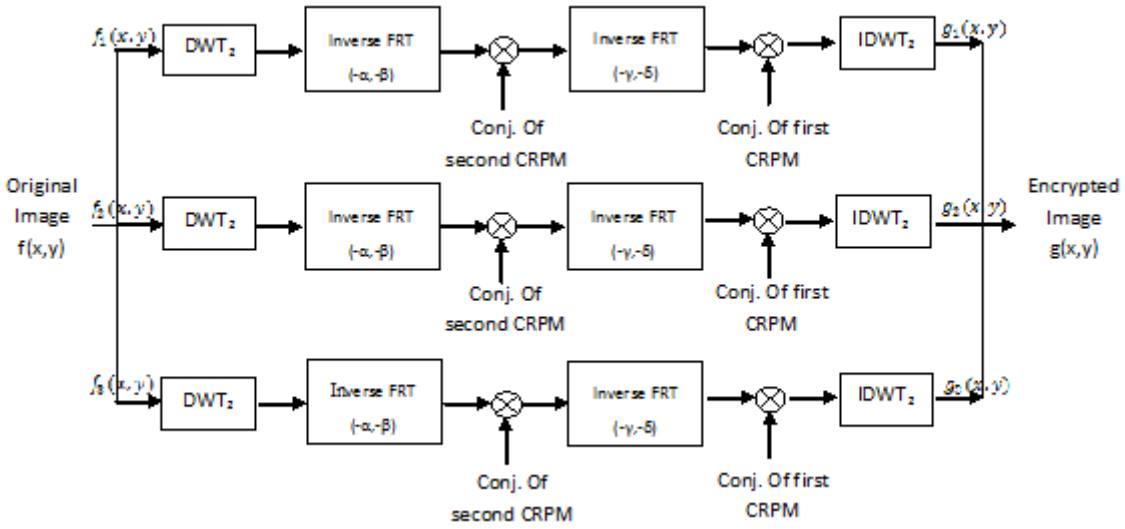

Fig. 2: Decryption process using $IDWT_2$ in proposed algorithm

VOL. 2 ISSUE 1, JAN.-2013 ISSN NO: 2319-7463

The first inverse FRT (of order -α,-β) is now applied and followed by a multiplication by conjugate of second CRPM, thus giving us:

$$F_{-\alpha,-\beta}\{DWT_2\{g(x,y)\}\} * conj\left(exp\left(i\frac{\pi}{2}S_2(x,y)\right)\right)$$

On the output obtained, the second FRT (of order -γ,-δ) is performed and then multiplied by the conjugate of first CRPM. The decrypted image from this outcome is now obtained by performing $IDWT_2$ as follows:

$$F'(x,y) = IDWT_2\left\{F_{-\gamma,-\delta}\left\{F_{-\alpha,-\beta}\{DWT_2\{g(x,y)\}\} * conj\left(exp\left(i\frac{\pi}{2}S_2(x,y)\right)\right)\right\} * conj\left(exp\left(i\frac{\pi}{2}S_2(x,y)\right)\right)\right\}$$

Proposed Algorithm for Image Encryption Decryption

This algorithm uses DWT_2 (The 2-dimensional discrete wavelet transform), $F_{\alpha,\beta}$ (The two dimensional fractional Fourier transform) in encryption process and $IDTW_2$ (The 2-dimensional inverse discrete wavelet transform), $F_{-\alpha,-\beta}$ (The 2-dimensional inverse fractional fourier transform) in decryption process as per the general encryption and decryption schemes already discussed. Both of the random phase functions are generated as a 2-d sequence of random numbers and they are not chaos based in this algorithm.

Computational complexity of encryption algorithm

Let the input image, I be of size N*N. Image encryption process involves following steps:

1. Application of DWT_2 on the primary color channels $f_i(x,y)$ of original image.
2. Encoding by first random phase function.
3. Application of first 2-D FRT.
4. Encoding by second random phase function.
5. Application of second 2-D FRT.
6. Application of $IDWT_2$ on the R, G and B channels obtained after step 6.

In step 1, each of the primary color channels of original image is operated using DWT_2, which is an O(N)algorithm. Thus step 1 takes O(N) time and produces an output image of size $\frac{N}{2} * \frac{N}{2}$. Therefore, steps 2 to 6 are to be applied on a smaller sized image than the original. The computation of 2-D FRT of an image of size N*N is a $O(2N^2 + Nlog_2 N)$ process [1]-[7]. Also, the generation of first and second random phase function is an $O(2N^2)$ process. But now, as the image size for steps 2 to 6 has reduced to $\frac{N}{2} * \frac{N}{2}$,

(i) Step 2 takes $O\left(2\left(\frac{N}{2}\right)^2\right) = O\left(\frac{N^2}{2}\right)$ computation time.

(ii) Step 3 takes $O\left(2\left(\frac{N}{2}\right)^2 + \frac{N}{2}log_2\left(\frac{N}{2}\right)\right) = O\left(\frac{N^3}{4} + \frac{N}{2}log_2\left(\frac{N}{2}\right)\right)$ time.

Similar to step 2 and 3, step 4 and 5 also take $O\left(\frac{N^2}{2}\right)$ and $O\left(\frac{N^3}{4} + \frac{N}{2}log_2\left(\frac{N}{2}\right)\right)$ computation time, respectively. Step 6 involves computation of inverse wavelet transform, which is also a $O(N)$ function. Therefore, the computation complexity of entire encryption plane is computed as follows:

$$T_{ENCRYPTION} = O(N) + O\left(\frac{N^2}{2}\right) + O\left(\frac{N^3}{4} + \frac{N}{2}log_2\left(\frac{N}{2}\right)\right) + O\left(\frac{N^2}{2}\right) + O\left(\frac{N^3}{4} + \frac{N}{2}log_2\left(\frac{N}{2}\right)\right) + O(N)$$

$$= O\left(\frac{N^3}{2} + N^2 + Nlog_2\left(\frac{N}{2}\right) + 2N\right)$$

$$= O\left(\frac{N^3}{2}\right)$$

Computational complexity of decryption algorithm

Image decryption process involves following steps:

1. Application of DWT_2 on the primary color components $g_i(x,y)$ of encrypted image.
2. Application of 2-D inverse FRT.

VOL. 2 ISSUE 1, JAN.-2013 ISSN NO: 2319-7463

3. Decoding by conjugate of second CRPM.
4. Application of 2-D inverse FRT.
5. Decoding by conjugate of first CRPM.
6. Application of $IDWT_2$ on the R, G, and B channels obtained after step 6.

In step 1 , each of the primary color channels of encrypted image is operated using DWT_2, which is an $O(N)$ algorithm. Thus step 1 takes $O(N)$ time and produces an output encrypted image of size $\frac{N}{2} * \frac{N}{2}$. Therefore, steps 2 to 6 are again, to be applied on a smaller sized image than the original encrypted image. Computation of 2-D FRT of an image of size $N * N$ is an $O(2N^3 + N\,log_2 N)$ process .Also, the generation of first and second random phase function is an $O(2N^2)$ process. But now, as the input image size for steps 2 to 6 has reduced to $\frac{N}{2} * \frac{N}{2}$

(i). Step 2 takes $O\left(2\left(\frac{N}{2}\right)^3 + \frac{N}{2}log_2\left(\frac{N}{2}\right)\right) = O\left(\frac{N^3}{4} + \frac{N}{2}log_2\left(\frac{N}{2}\right)\right)$ time.

(ii). Step 3 takes $O\left(2\left(\frac{N}{2}\right)^2\right) = O\left(\frac{N^2}{2}\right)$ computation time.

Similar to step 2 and 3, step 4 and 5 also take $O\left(\frac{N^3}{4} + \frac{N}{2}log_2\left(\frac{N}{2}\right)\right)$ and $O\left(\frac{N^2}{2}\right)$ computation time, respectively. Step 6 involves computation of inverse wavelet transform, which is also a $O(N)$ function. Therefore, the computation complexity of entire encryption plane is computed as follows:

$$T_{DECRYPTION} = O(N) + O\left(\frac{N^2}{2}\right) + O\left(\frac{N^3}{4} + \frac{N}{2}log_2\left(\frac{N}{2}\right)\right) + O\left(\frac{N^2}{2}\right) + O\left(\frac{N^3}{4} + \frac{N}{2}log_2\left(\frac{N}{2}\right)\right) + O(N)$$

$$= O\left(\frac{N^3}{2} + N^2 + Nlog_2\left(\frac{N}{2}\right) + 2N\right)$$

$$= O\left(\frac{N^3}{2}\right)$$

Thus, the computational complexity of above algorithm is evaluated to:

$T_{total} = T_{encryption} + T_{decryption} = O(N^3)$

Thus complexity is reduced from previous algorithm.

Conclusion

We have proposed an algorithm for image encryption and decryption and their performance has been analyzed, based on the computation time required by the algorithm. This algorithm works on a strategy that the data size (or image size) for encryption and decryption is reduced by a factor of 4 than the existing algorithms. For this purpose we have efficiently utilized the characteristic of the discrete wavelet transform. In another sense, we conclude that the proposed algorithm is very robust in nature. By this we mean that once we encrypt an image for a particular fractional order of FRT, decryption of this encrypted image is only possible, when the selected fractional order for decryption is exactly the suitable for decryption. This work can be extended for different formats of images. Efficient algorithms for computation of 2-D FRT, DWT_2 ,I DWT_2 AND 2-D inverse FRT may result in reduction of computation times of proposed algorithm. Algorithms, suitable for wireless environment may also be proposed. We may extend this work using other transformation methods also.

References

[1]. Madhusudan joshi, chandrashekhar, kehar singh, “color image encryption and decryption using fractional fourier transform”, optics communication, vol. 279 issue1, pp 35-42, nov., 2007.
[2]. narendra singh, alok sinha, “optical image encryption using fractional fourier transform and chaos”, optics and lasers in engineering, vol. 46 issue 2, pp117-123, feb 2008.
[3]. lin zhang, jianh wu, nanrun zhou, “image encryption with discrete fractional cosine transform amd chaos”, fifth international conference on information assurance and security 2009 ias’09,2009,pp 61-64
[4]. ran tao, yi xin,yue wang, ”Double encryption based on random phase encoding in the fractional domain”,optics Express , vol. 15 issue 24,2007,pp 16067-16079.
[5]. Madhusudan joshi,Chandra shakhar,kehar singh,”Image encryption using chaos and radial Hilbert transform”
[6]. B.M. Hennely,J.T. heridan,”Image encryption and the fractional and the fourier transform”, Optik- International Journal for Light and Electron Optics, Volume 114 issue 6, 2003, pp 251-265

VOL. 2 ISSUE 1, JAN.-2013 ISSN NO: 2319-7463

[7]. Yuhong zhang , Fenxia Zhao," The algorithm of fractional fourier transform and application in digital image encryption", International Conference on information Enginnering and Computer Science,2009, pp 1-4.
[8]. Ismet Ozturk, Ibrahim Sogukpmar," Analysis and comparison of image encryption algorithms", International Journal of information technology, volume 1 number 2
[9]. Anil kumar yadav, Ravinder Kumar Purwar, "Complexity analysis of image encryption technique".
[10]. Cheng Hung Chuang, Guo Shiang Lin,"Data steganography for optical color image cryptosystems", International Journal of image processing (ijip), vol 3issue 6 , January 2010,pp 318-327.
[11]. haldun M. Ozaktas, M. Alper Kutay , Zeev Zalevsky, The fractional Fourier transform: with applications in optics and signal processing, New York, john wiley & sons, 2001.
[12]. N.K. Pareek, Vinod Patidar, K.K. Stud, "Image encryption using Chaotin logistic map", image and vision computing, vol.24,2006,pp 926-934
[13]. I.A. Ismail, Mohammed Amin an Hossam Diab, "An efficient Image encryption Scheme based Chaotic Logistic Maps" , International journal of soft Soft computing, vol.2,2007, pp285-291.
[14]. Rafael C. Gonzalez, Richard Eugene Woods, Steven L. Eddins, Digital image processing using matlab, Delhi, pearson education,2004
[15]. Alexamder D. Poularikas, "Transforms And Applications Handbook" , 3rd ed., New York, CRC press, 1966.
[16]. Stephen Lynch, "nonlinear Discrete dynamical Systems" in dynamical systems with applications using mathematica, New York, Springer,2007,pp 261-292
[17]. Thomas H. Cormen, Charles E. Leisersion, Ronald L. Rivesty, Clifford Stein, "Growth of Fuctions" , Introduction to algorithms, 3rd ed., Cambridge, MIT Press, 2009, pp 43-64.
[18]. Ellis Horowitz, Sartaj Sahni, Sanguthevar Rajasekaran, Fundamental of computer algorithms, 2nd Ed., Hyderbad, Universities press, 2008.