Pixel chaotic shuffling and Arnold map based Image Security Using Complex Wavelet Transform

ArjunVerma
College of Science & Engineering, Jhansi

Abhinav Jain
College of Science & Engineering, Jhansi

Abstract – Today, security is a challenging issue with the transmission of vast amount of digital documents like texts, images, videos or audios over the internet from one point to another. For confidential, the images may be secured using various methodologies like, DES, RSA, etc. But these methods provide secure images but complexity is also one big issue. In contrast to the discrete wavelet transform (DWT), the design of Dual Tree Complex Wavelet Transform (DT-CWT) poses good directional properties for diagonal features and is rugged to shift Invariance.
To provide security with less complexity, a method is proposed based on dual-tree complex wavelet transform. Where approximation parts are secured using pixel chaotic shuffle method and detail parts are secured using Arnold transform. Our scheme provides high security as even after the extraction of first layer, without knowing the extraction algorithm, original image cannot be recovered in its entirety. The proposed scheme is tested on various test images and the obtained results show the effectiveness of the proposed scheme.

Index Terms – Arnold transforms; block shuffling; Dual-tree complex wavelet transform.

1. INTRODUCTION

In recent years, owing to frequent flow of digital images across the world over the transmission media, it has become essential to secure them from leakages. Many applications like military image databases, confidential video conferencing, medical imaging system, cable TV, online personal photograph album, etc. require reliable, fast and robust security system to store and transmit digital images. The requirements to fulfill the security needs of digital images have led to the development of good encryption techniques. During the last decade, numerous encryption algorithms [1-3] have been proposed in the literature based on different principles. Among them, chaos based encryption techniques are considered good for practical use as these techniques provide a good combination of speed, high security, complexity, reasonable computational overheads and computational power etc. The digital images have certain characteristics such as: redundancy of data, strong correlation among adjacent pixels, being less sensitive as compared to the text data i.e. a tiny change in the attribute of any pixel of the image does not drastically degrade the quality of the image and bulk capacity of data etc [4-6].

Consequently, the traditional ciphers like IDEA, AES, DES, RSA etc. are not suitable for real time image encryption as these ciphers require a large computational time and high computing power. For real time image encryption only those ciphers are preferable which take lesser amount of time and at the same time without compromising security. An encryption scheme which runs very slowly, even may have higher degree of security features would be of little practical use for real time processes [7-8].

The requirements of information security within an organization have undergone two major changes in last several decades. Before the widespread use of data processing equipment, the security of information felt to be valuable to an organization was provided primarily by physical and administrative means. An example of former is the use of rugged filing cabinets with a combination lock for storing sensitive documents. An example of the latter is personnel screening procedures used during hiring process. With the introduction of the computer, the need for automated tools for protecting files and other information stored on the computer became evident [9]. The generic name for the collection of tools designed to protect data and to thwart hackers is *computer security*.

The second major change that affected security is the introduction of distributed systems and the use of network and communication facilities for carrying data between user and computer and between computer and computer. Network security measures are needed to protect data during their transmission [10].

With this motivation, this paper has the following structure: section II is about dual-tree complex wavelet transform, section III gives information on the proposed algorithm employed for the encryption process, section IV represents the results and discussion and section V concluded the paper.

2. DUAL TREE COMPLEX WAVELET TRANSFORM

For the DWT small changes in the input may cause large changes in the wavelet coefficients. Furthermore aliasing occurs due to down sampling. Inverse DWT cancels this aliasing provided if the wavelet and scaling coefficients are not changed. The other disadvantage of DWT is its poor directional selectivity (e.g., inability to distinguish between +45° and −45° spectral features). These problems of Real DWT can be solving during complex wavelets. However, a further problem arises in achieving perfect reconstruction for complex wavelet decomposition beyond level 1. To overcome this, Kingsbury proposed the DTCWT, which allows perfect reconstruction while still providing the other advantages of complex wavelets [13]. DT-CWT provides N multi scales, can be implemented using separable efficient Filter Banks as shown in Fig.1.

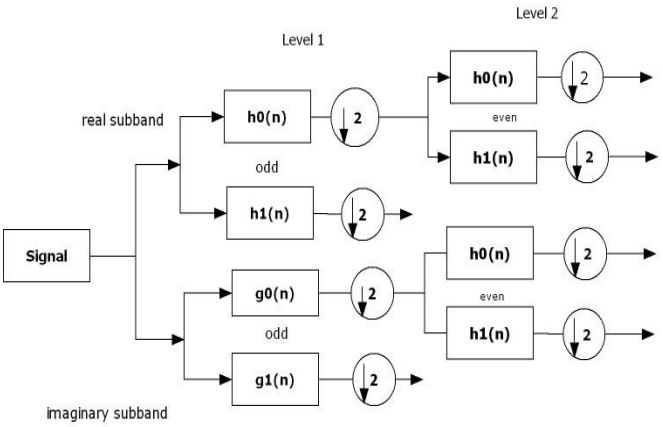

Figure.1. DT- CWT working principle for 1D signal

Here two sets of Filter banks are used, consists of low pass and high pass filters. The sub band signals of the upper DWT can be interpreted as the real part of a complex wavelet transform, and sub band signals of the lower DWT can be interpreted as the imaginary part. Equivalently, for specially designed sets of filters, the wavelet associated with the upper DWT can be an approximate Hilbert transform of the wavelet associated with the lower DWT. Then designed, the dual-tree complex DWT is nearly *shift-invariant* and *strong directional* in contrast with the critically-sampled DWT.

2D DTCWT produces six high-pass bands as well as two low-pass bands at each level of decomposition, L represents low-pass filters and H represents high-pass filters. Each filtering operation is followed by a down sampling by two. Six directional wavelets of DTCWT are obtained by taking sum (Σ) and difference (Δ) of highpasssubbands which have the same pass bands.

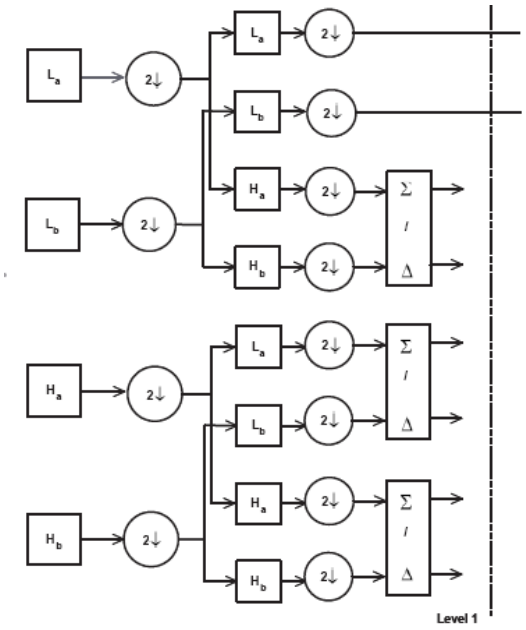

Figure.2. Decomposition of DT-CWT for 2D image

3. PROPOSED ARCHITECTURE OF IMAGE ENCRYPTION

The following flow chart as shown in fig.3 is showing the overview for an image encryption where block-wise Arnold map and pixel chaotic shuffle is used. Dual-tree complex wavelet transform is also used as secured structures so that the original information of edges may not loose.
The image encryption architecture is proposed as shown in figure 3, where following steps are processed as:

Step 1: Perform Dual-tree complex wavelet transform (DT-CWT) to obtain two approximations and six detail parts.

Step 2: Approximation and detail parts of image are divided into n number of blocks where some parts of block are overlapped.

Step 3: Apply Arnold equation for each block of Approximation parts where Arnold transformation changes the coordinate (x, y) to the (x', y') by using below formula:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \times \begin{bmatrix} x \\ y \end{bmatrix} \ mod\ n$$

Step 4: Over the detail parts, encryption is applied using pixel chaotic shuffle method so that the detail parts can also be encrypted.

a) Select proper initial values and system parameters to create chaotic variable sets.
b) Prepare the chaotic sequences (according to sorting algorithm).
c) Transfer MxN matrix as MNx1.
d) Perform the shuffle function on each pixels of matrix.

Step 5: Apply Inverse dual-tree complex wavelet transform, to reconstruct the image using encrypted approximation and detail coefficients.

In the above proposed algorithm, block wise internal shuffling process on approximation parts and external shuffling on performed detail parts is performed. After this process, Pixel chaotic shuffle method is performed on all blocks of approximation parts and Arnold transform is performed on all blocks of detail parts. Inverse dual tree complex wavelet transform is applied to get the encrypted image.

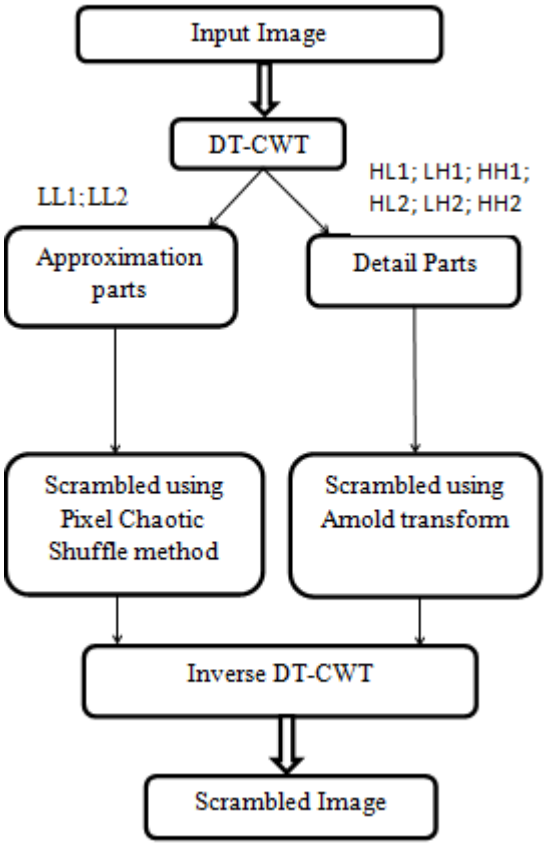

Figure 3: Proposed Architecture of image encryption

4. RESULTS OF EXPERIMENT AND ANALYSIS

The experimental evaluation is performed on images with size 512x512 using proposed method. Apart from the security consideration, running speed of the algorithm is also an important aspect for a good encryption algorithm. Results are shown in fig 4, fig 5, fig 6 and fig 7. Original images are fig 4(a), fig 5(a), fig 6(a) and fig 7(a). Encrypted images are fig 4(b), fig 5(b), fig 6(b) and fig 7(b) and Decrypted images are 4(c), fig 5(c), fig 6(c) and fig 7(c).

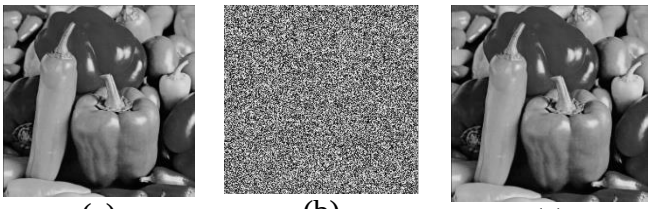

Figure 4: (a) Original Peppers: Jellyfish (b) Encrypted image and (c) Decrypted image

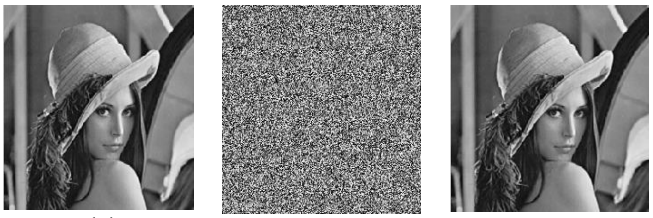

Figure 5: (a) Original image: Lena (b) Encrypted image and (c) Decrypted image

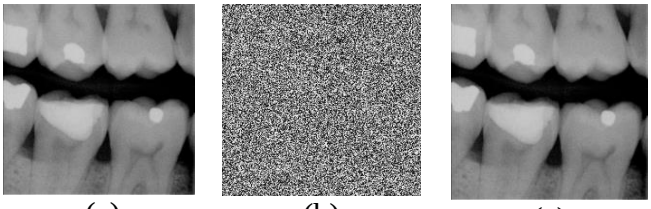

Figure 6: (a) Original image: Teeth (b) Encrypted image and (c) Decrypted image

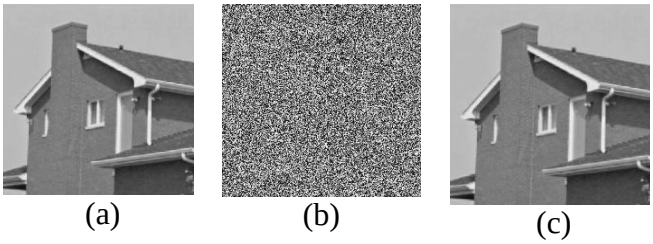

Figure 7: (a) Original image: House (b) Encrypted image and (c) Decrypted image

PSNR, Mean error and entropy difference (ED) for original and decrypted images are calculated and given in Table 1.
From table 1, we can analyze that the value of mean error and entropy difference is very less, near to zero. It means our decrypted image is almost same as original image.

Table 1: PSNR, Mean error and ED

Input Images	PSNR	Mean error	Entropy difference (ED)
Peppers	40.03	0.0314	0.1245
Lena	39.12	0.0126	0.7121
Teeth	39.12	0.0832	0.0351
House	38.91	0.0254	0.0351

5. CONCLUSIONS

This paper gives a new image scrambling algorithm, by using dual-tree complex wavelet transform to encrypt the image to improve the security of image. Images are more secured with less complexity.

Compared with the traditional methods, the proposed method gives better result in terms of decrypted image. The visual quality of decrypted image is more visible in compare of existing methods. Experimental result shows that the improved algorithm is feasible. Mean error and entropy difference indicates that proposed method is giving complete information as original image.

REFERENCES

[1] C.Y. Lin, M. Wu, J.A. Bloom, I. J. Cox, M. L. Miller and Y. M. Lui, "Rotation, scale, and translation resilient watermarking for images", IEEE Transactions, Image Processing, Vol. 10, pp. 767-782, May 2001.
[2] C. Li and G. Chen, "On the security of a class of image encryption schemes," Proceedings of the IEEE International Symposium on Circuits and Systems, 2008.
[3] S. Li, C. Li, G. Chen, and X. Mou, "Cryptanalysis of the RCES/RSES image encryption scheme," available online at http://eprint.iacr.org/2004/376 on 15 Oct. 2008.
[4] Jui-Cheng Yen, Jiun-In Guo, "A new chaotic image encryption algorithm" Department of Electronics Engineering National Lien-Ho College of Technology and Commerce, Miaoli, Taiwan, Republic of China.
[5] M. A. Bani Younes and Aman Jantan, "Image Encryption Using Block-Based Transformation Algorithm"IAENG, 35:1, IJCS_35_1_03, February 2008.
[6] IsmetOzturk and AbrahimSogukpinar, "Analysis and Comparison of Image Encryption Algorithms", World Academy of Science, Engineering and Technology 3 2005.
[7] K.C. Ravishankar, M.G. Venkates hmurthy "Region Based Selective Image Encryption" 1-424-0220-4/06 ©2006 IEEE.
[8] W.Stallings, Cryptography and network security: Principles and Practice. Prentice hall,2010,vol.998.
[9] I.J. Cox and M.L. Miller, "A review of watermarking and the importance of perceptual modeling", Proceedings of Electronic Imaging'97, February 1997.