Dual Tree Complex Wavelet Transform for Image Security using Arnold Method

Arjun Verma
College of Science & Engineering, Jhansi

Abhinav Jain
College of Science & Engineering, Jhansi

Beerendra Kumar
College of Science & Engineering, Jhansi

ABSTRACT
The increasing globalization led to the transmission of vast amount of digital documents like texts, images, videos or audios over the internet from one point to another. However, some of these documents might be highly confidential and its transmission over the internet must be protected from unauthorized access. In this paper, we have proposed a novel hybrid Arnold transform scheme based on dual tree complex wavelet transform with block shuffling internally as well as externally. In this scheme, we have provided double layer of security by utilizing the multi-resolution property of wavelet using Arnold transform andblock shuffling.In contrast to the discrete wavelet transform (DWT), the design of Dual Tree Complex Wavelet Transform poses good directional properties for diagonal features and is rugged to shift Invariance. 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.

Keywords
Arnold transforms; block shuffling; Dual-tree complex wavelet transform.

1. INTRODUCTION
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. 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.

Cryptography can be defined as the processing of information into an unintelligible (encrypted) form for the purposes of secure transmission. Through the use of a "key" the receiver can decode the encrypted message (decrypting) to retrieve the original message. Cryptography today involves the use of advanced mathematical procedures during encryption and decryption processes [1] [2]. Cipher algorithms are becoming more complex daily. There two main algorithmic approaches to encryption, these are symmetric and asymmetric [3]. Symmetric-key algorithms are a class of algorithms for cryptography that use the same cryptographic keys for both encryption of plaintext and decryption of cipher text [4]. The keys may be identical or there may be a simple transformation to go between the two keys [5]. Typical examples symmetric algorithms are Advanced Encryption Standard (AES), Blowfish, Triple Data Encryption Standard (3DES) and Serpent [6]. Enormous number of transfer of data and information takes place through internet, which is considered to be most efficient though it's definitely a public access medium [7]. The cryptography in digital computing has been applied to different kinds of digital file formats such as text, images video etc. Image encryption, also called image scrambling, produces an unintelligible or disorder image from the original image. The existing image encryption algorithms can be classified into two kinds [8]. One is spatial-based method; the other is frequency-based method. The spatial-based algorithms are usually achieved by swapping the pixel positions or altering pixel values. Arnold transform is an efficient technique for position swapping, and widely applied to image encryption [9]. Arnold transform and exclusive OR operation are used to produce scrambled images. Logistic map exploited to improve the security of Arnold transform. Conventional Arnold transform based schemes have a common weakness that image height must equal image width. Considering pixel value modification, an image encryption scheme based on bit shuffling of individual pixels [10]. It doesn't need iterative computations, and then reduce the run time. A well-known image encryption algorithm based on frequency domain is designed. However, the decrypted image isn't totally equal to the original image.

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
The drawbacks in DWT can be eliminated by using an expansive wavelet transform in place of a critically-sampled one. (An expansive transform is one that converts an N-point signal into M coefficients with M > N). DT-CWT provides N multi scales, can be implemented using separable efficient Filter Banks as shown in Fig.1.

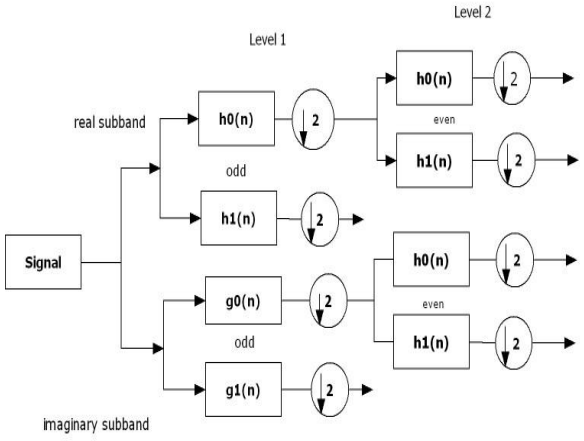


Figure.1. DT- CWT working principle for 1D signal

Here two sets of Filter banks are used, consists of low pass and high pass filters. Down sample the input signal by 2 through a filter of H(z) transfer function and again through G(z) filter. The filters should be Hilbert transform pairs

$$y_g(t) = \mathrm{H}\{y_h(t)\} \qquad (1)$$

The filters in the upper and lower DWTs should not be the same, the filters used in the first stage of the dual-tree complex DWT [4] should be different from the filters used in the remaining stages. 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. The designed filter complex wavelet should be analytic and it is

$$\psi_c(t) := \psi_h(t) + j\psi_g(t) \qquad (2)$$

The wavelet coefficients w are stored as a cell array. For j = 1..J, k = 1..2, d = 1..3, w{j}{k}{d} are the wavelet coefficients produced at scale j with an orientation d. The dual-tree complex DWT outperforms well compared to the critically-sampled DWT for applications like image de-noising and enhancement.
DT-CWT for image provides six (d=1…..6) directional high frequency sub bands and two (d=1, 2) low frequency sub bands as shown in fig 2.
The complex-wavelet coefficient is defined as

$$d_c(k,l) = d_r(k,l) + jd_i(k,l) \qquad (3)$$

And its magnitude is

$$|d_c(k,l)| = \sqrt{|d_r(k,l)|^2 + |d_i(k,l)|^2} \qquad (4)$$

When $|d_c(k,l)| > 0$

And phase is given as

$$d_c(k,l) = \arctan q \qquad (5)$$

Where $\theta = \dfrac{d_i(k,l)}{d_c(k,l)}$

Key features of DT-CWT areBetter directionality, anti- aliasing effect; good shift-invariant, geometry of the image features retained from phase, better robustness smooth varying and low computation compared with DWT, three times that of maximally decimated DWT.

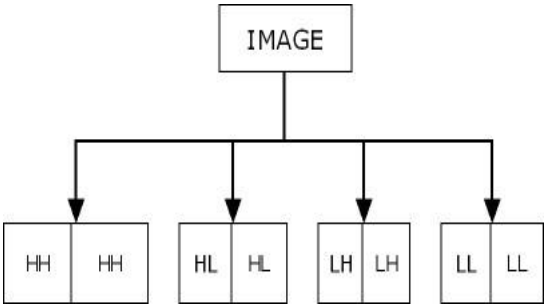


Figure.2. Decomposition of DT-CWT for 2D image

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 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: In, respective approximation parts, each block is shuffled row wise as well as column wise.
Step 4: In detail parts, each block is shuffled as below:

i. All blocks of all detail parts areinter-changed by random generator. (Ex. First block of first detail part is interchanged by third detail parts last block).
ii. In respective detail parts, each block is shuffled row wise as well as column wise.

Step 5: Apply Arnold equation for each block of Approximation parts and detail parts where Arnold transformation changes the coordinate (x, y) to the (x', y') by using below formula:

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

Step 6: 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, Arnold transform is performed on all blocks on both approximation and detail parts. Inverse dual tree complex wavelet transform is applied to get the encrypted image.

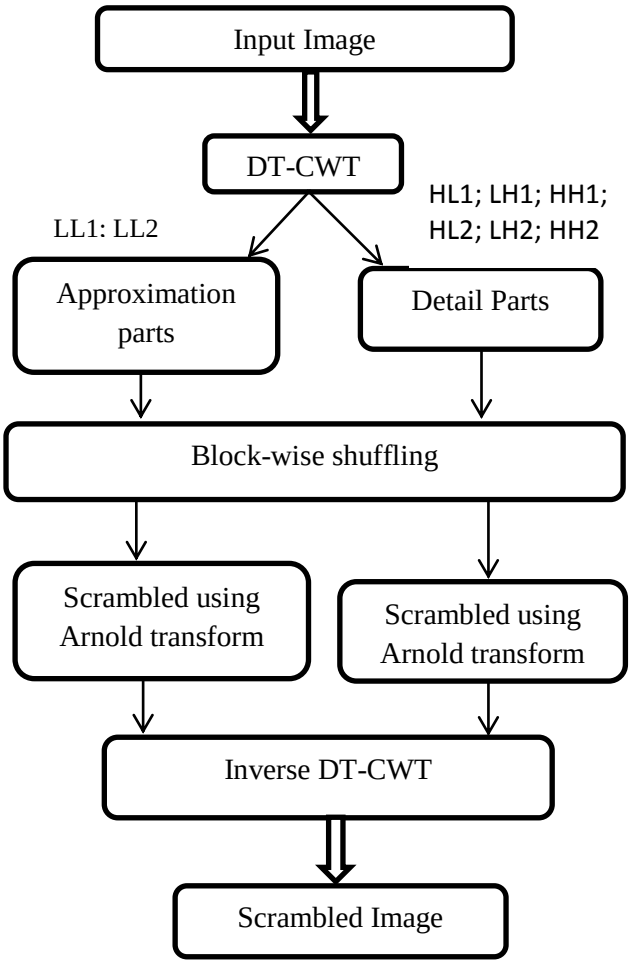
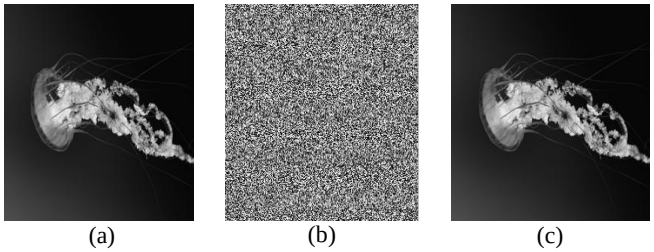


Figure 3: Proposed Architecture of image encryption

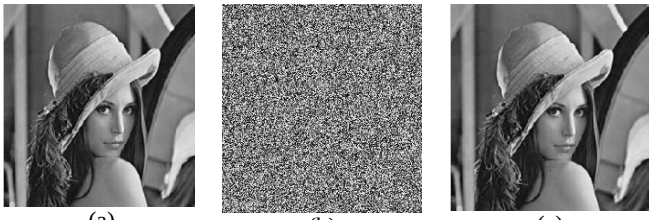
4. RESULTS OF EXPERIMENT AND ANALYSIS

The experimental evaluation is performed on images with size 256x256 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).



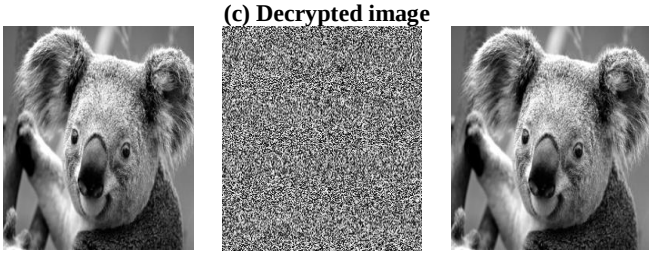
(a) (b) (c)

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



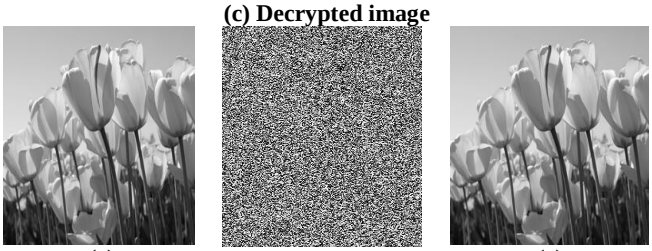
(a) (b) (c)

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



(a) (b) (c)

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



(a) (b) (c)

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

Mean error and entropy difference 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: Mean error

Input Images	Mean error	Entropy difference
Jellyfish	0.0923	0.2310
Lena	0.0162	0.1021
Koala	0.0634	0.0332
Tulips	0.0183	0.5124

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. Compared with the traditional Arnold scrambling algorithm, the proposed multi-area scrambling method in this paper not only can be used for a square image, but for any non-square images. By using multi-region scrambling, it can more effectively improve the security of image, lead decipher even more difficult. 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.

6. 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. BaniYounes and AmanJantan, "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. Venkateshmurthy "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.

[10] J. Fridrich, 2 Lt Arnold C. Baldoza, and Richard J. Simard "Robust digital watermarking based on key-dependent basis functions" 2nd Information Hiding Workshop, Portland OR, April 15–17, 1998.