Volume 5, Issue 2, February 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Two Level Image Security based on Arnold Transform and Chaotic Logistic Mapping

Vineeta Singh*, Vipin Dubey
Saroj Institute of Technology & Management,
Lucknow, Uttar Pradesh, India

Abstract— In today's growing world of digital technology, access to the multimedia content is very easy and for some sensitive applications such as medical imaging, military system, legal problems, it is very essential to not only reinstate the original media without any loss of information but also to increase content's security. In this paper, we have proposed a novel hybrid Arnold transform scheme based on DWT. In this scheme, we have provided double layer of security by utilizing the multi-resolution property of wavelet using Arnold transform and chaotic logistic mapping. 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; chaotic logistic mapping; discrete wavelet transform; encryption; mean error.

I. INTRODUCTION

Earlier before the arrival of the internet, security of sensitive documents was depended on filing cabinets with a combination lock for storing paper- based files or documents. Introduction of computers in handling businesses in an organization, with the advancement in networking and communication technology has revolutionized the concept of data transmission over the internet. The increasing globalization (in which an organization enters a new place for trading purpose) led to the transmission of vast amount of digital documents like texts, images, videos or audios over the internet from one point to another [1]. However, some of these documents might be highly confidential and its transmission over the internet must be protected from unauthorized access [2].

In cryptography, encryption is the process of transforming information using an algorithm to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key [3]. The result of the process is encrypted information. The reverse process is referred to as decryption. Cryptography today involves the use of advanced mathematical procedures during encryption and decryption processes [4]. Cipher algorithms are becoming more complex daily. There two main algorithmic approaches to encryption, these are symmetric and asymmetric. 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 [5]. The keys may be identical or there may be a simple transformation to go between the two keys [6]. Typical examples symmetric algorithms are Advanced Encryption Standard (AES), Blowfish, Triple Data Encryption Standard (3DES) and Serpent [8]. 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 [9]. 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 [10]. 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 [10] [11]. 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 [11] [12]. 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. In other words, the algorithm is lossy. For wavelet domain, a method for partial-scrambling of JPEG 2000 images using public-key encryption has been proposed. It has backward compatibility with a standard JPEG 2000. This means that the encrypted images can be decoded by a standard JPEG 2000 decoder [7]. With the rapid development of Internet technology and digital signal processing technology, the secure transmission of image data is becoming a most important problem. Due to some intrinsic features of images, such as bulk data capacity and high redundancy, we must consider image compression except for image encryption.

On one hand, for the purpose of reducing the image size for easy storage and fast transmission, the study on image compression has been carried out for a long time. From various research papers, we see that the compression performances are good. However, the current methods are not confidential because they do not have the encryption effect.

On the other hand, chaotic systems demonstrate excellent permutation and diffusion properties for effective ciphers [4]. It is thus clear that based on all kinds of visible field, a variety of methods has been put forward. According to the characteristics of digital image information people has put forward a lot of digital image encryption algorithm based on chaotic system encryption technology since it has good effect and speed of encryption got an extensive use of research. The paper has the following structure: section II is about discrete 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.

II. DISCRETE WAVELET TRANSFORM (DWT)

2-D Discrete Wavelet Transform is widely used transform in image processing. DWT is based on the concept of wavelets. It is localized both in frequency and time domain. This reveals spatial and frequency aspects simultaneously. It is used for analyzing an image at different resolutions into different frequency components.

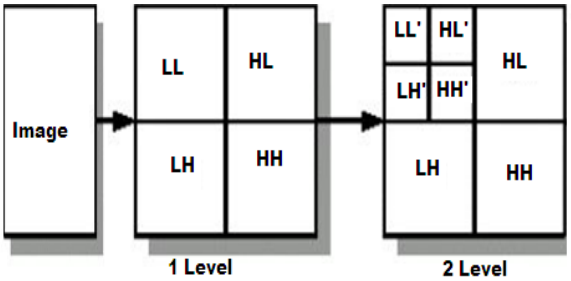


Figure 1: First and Second Level 2-D Wavelet Decomposition

Figure 2: Lena Image and Its First Level 2-D Wavelet Decomposition

Due to multiresolution property, features that may go unnoticed at one resolution, may be easily detected at another. Multiresolution analysis comprises image pyramid and subband coding theory. For obtaining 2-D wavelet decomposition, 1-D DWT can be applied on image first in horizontal and then in vertical direction using different filters. 2-D DWT decomposes the image into two parts: Approximation and Detailed part. Approximation part contains one low frequency subband LL and detailed part contains three high frequency subbands LH, HL and HH. Approximation part can be further decomposed into four subbands as shown in Figure 1. First level decomposition of lena image is shown in Figure 2. Decomposed subbands can be used to reconstruct the original image using Inverse DWT.

III. PROPOSED ARCHITECTURE OF IMAGE ENCRYPTION

The following flow chart as shown in fig.2 is showing the overview for an image encryption where Arnold map and chaotic method are jointly used. Wavelet transform is also used as edge preserving 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 discrete wavelet transform (DWT) to obtain approximation and detail parts.

Step 2: the detail parts wavelet coefficients are stored for encryption purpose.

Step 3: Approximation part is encrypted using Arnold transform.

a) Approximation part of Image is divided into n*n blocks.

b) Each block is shuffled row wise as well as column wise.

c) Arnold transform is applied to each shuffled block. The Arnold transformation that change the coordinate (x, y) to the (x', y') by using 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: Inverse wavelet transform is performed to reconstruct the image using encrypted approximation part and stored detail coefficients.

Step 5: Over the reconstructed encrypted image, another layer of 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 6: From all above process, an encrypted image is received. For decryption, put the same sequences of shuffling and sorting.

In the above proposed algorithm, the two level encryption is used. On first level the structure is preserved so that for decryption time, the decrypted image can be achieved with accuracy. In second level the structure is also secured using pixel chaotic shuffle method.

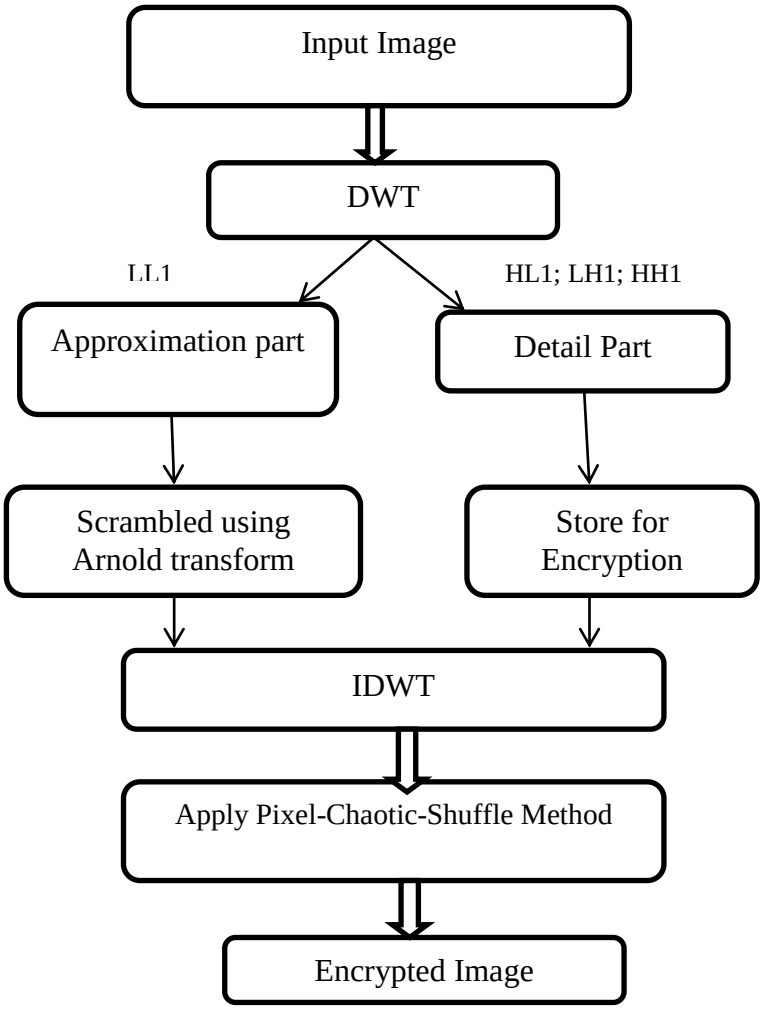
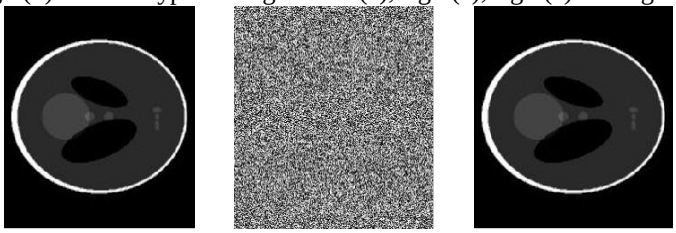


Figure 3: Proposed Architecture of image encryption

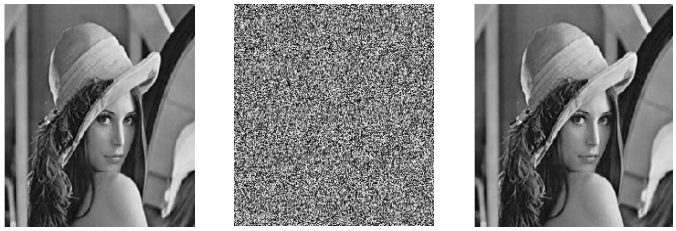
IV. RESULTS OF EXPERIMENT AND ANALYSIS

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).



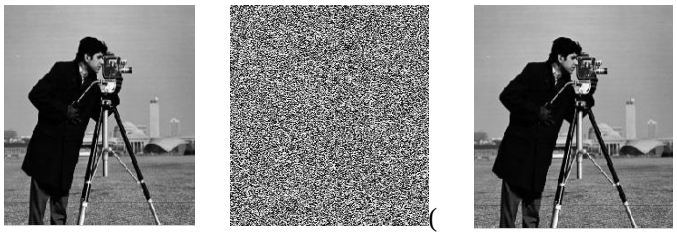
(a) (b) (c)

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



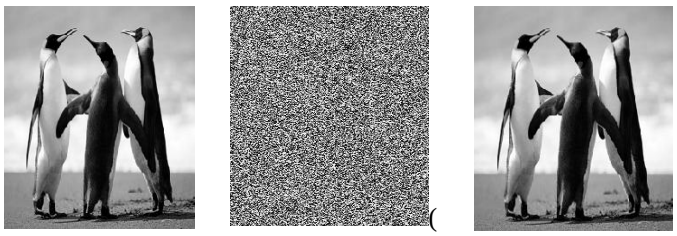
(a) (b) (c)

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



(a) b) (c)

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



(a) b) (c)

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

Mean error for original and decrypted images are calculated and given in Table 1. From table 1, we can analyse that the value of mean error 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**
Phantom	0.0139
Lena	0.0503
cameraman	0.0428
Penguins	0.0644

V. CONCLUSIONS

The proposed encryption algorithm uses two level encryption algorithms. One algorithm is for divide the image into blocks after that each block is shuffled within image using Arnold transformation which will apply on the shuffled image iteratively. Where wavelet transform is also used to preserve the structure. And another part is based on pixel chaotic shuffling method to secure preserving details. This approach provides us to encrypt the image two times. An initial key is required by secure image cryptosystems, which means that the cipher image cannot be decrypted correctly. This guarantees the security of the proposed technique against brute-force attacks to some extent.

REFERENCES

[1] X. Zhang, and S. Wang, "Fragile watermarking scheme using a hierarchical mechanism," Signal Processing, vol.89, no.4, pp.675–679, 2009.

[2] D. Qi, "Matrix transformation and its application to image hiding," Journal of North China University of Technology, vol.11, no.1, pp.24–28, 1999.

[3] L. Zhu, W. Li, L. Liao, and H. Li, "A novel algorithm for scrambling digital image based on cat chaotic mapping," In: Proc. of IIH-MSP '06, pp.601–604, 2006.

[4] Z. Shang, H. Ren, and J. Zhang, "A block location scrambling algorithm of digital image based on Arnold transformation," In: Proc. of the 9th International Conference for Young Computer Scientists, pp.2942–2947, 2008.

[5] Z. Tang, X. Lu, W. Wei, and S. Wang, "Image scrambling based on bit shuffling of pixels," Journal of Optoelectronics • Laser, vol.18, no.12, pp.1486–1488, 1495, 2007.

[6] D. V. D. Ville, W. Philips, R. V. de Walle, and I. Lemanhieu, "Image scrambling without bandwidth expansion," IEEE Trans. Circuits Syst. Video Technol., vol.14, no.6, pp.892–897, 2004.

[7] O. Watanabe, A. Nakazaki, and H. Kiya, "A fast image-scramble method using public-key encryption allowing backward compatibility with JPEG2000," In: Proc. of ICIP '04, pp.3435–3438, 2004.

[8] W. Sun, "The periodicity of Arnold transformation," Journal of North China University of Technology, vol.11, no.1, pp.29–32, 1999.

[9] R. Venkatesan, S.-M. Koon, M. H. Jakubowski, and P. Moulin, "Robust image hashing," In: Proc. of ICIP '00, pp.664–666, 2000.

[10] Z. Tang, S. Wang, X. Zhang, W. Wei, and S. Su, "Robust image hashing for tamper detection using nonnegative matrix factorization," Journal of Ubiquitous Convergence and Technology, vol.2, no.1, pp.18–26, 2008.

[11] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," Int. J. Bifurcation and Chaos, vol. 8, no. 6, pp. 1259-1284, 1998.

[12] G. Chen, Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic maps," Chaos, Solitons & Fractals, vol. 21, no. 3, pp. 749-761, 2004.

