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

An Entropy Based Color Image Encryption Based on Arnold Transform and Pixel Chaotic Shuffling Method

Vineeta Singh*, Vipin Dubey

Saroj Institute of Technology & Management,

Lucknow, Uttar Pradesh, India

Abstract— Privacy is one of the key issues information Security addresses. Through encryption one can prevent a third party from understanding raw data during signal transmission. In this paper, we have proposed a novel hybrid Arnold transform scheme based on DWT on color images. In this scheme, we have provided entropy based double layer of security by utilizing the multi-resolution property of wavelet using Arnold transform and chaotic logistic mapping. Our scheme provides high security where the texture information is high. The color components are extracted and secured using proposed algorithm. 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

Nowadays, applications of digital imaging are prevalent and are still continuously and rapidly increasing today. Unlike text messages, image data have special features such as bulk data capacity, high redundancy, and high correlation among pixels, and usually are huge in size, which together make traditional encryption methods difficult to apply and slow to process.

Since digital media such as image, audio, and video are easy to copy, edit and transfer, the emergence of powerful tools raises a series of problems. For example, one can easily process the copyright images and redistribute them. Thus, the content protection becomes an important problem. In general, there are two ways. One is watermark; the other is encryption. The watermark-based techniques embed an invisible signal into the media to form a watermarked version [1]. At the receiver's end, the integrity of media contents can be verified by authenticating the embedded signal [2]. For encryption algorithms, they usually convert the meaningful media into the meaningless media. In this work, we focus on image encryption.

The chaotic confusion and pixel diffusion methods was proposed using a chaotic 2-D combined with alterations of Grey-Level values of each pixel in a sequential manner [3]. Repetitive rounds of permutations and changes were used to achieve higher security. It was experimentally verified that the amount of time overhead in performing complex calculations and the complex diffusion process had led to large time complexity of the system [4]. This paper proposes an image based encryption technique by developing a cipher algorithm for image encryption of m*n size by shuffling the RGB pixel values. The algorithm ultimately makes it possible for encryption and decryption of the images based on the RGB pixel. The paper has the following structure: section II is about related works, section III gives information on the proposed algorithm employed for the encryption process, section IV represents the results & discussion and section V concluded the paper.

II. RELATED WORK

A new cryptographic scheme proposed for securing color image based on visual cryptography scheme where a binary image was used as the key input to encrypt and decrypt a color image [5]. The secret color image which needs to be communicated was decomposed into three monochromatic images based on YCbCr color space. Then these monochromatic images were then converted into binary image, and finally the obtained binary images were encrypted using binary key image, called share-1, to obtain the binary cipher images. During their encryption process, exclusive OR operation was used between binary key image and three half-tones of secret color image separately [6]. These binary images were combined to obtain share-2. In the decryption process, the shares were decrypted, and then the recovered binary images were inversed half toned and combined to get secret color image [7].

With the exceptionally good properties in chaotic systems such as sensitivity to initial conditions and control parameters, chaos-based image encryption algorithms have been widely studied and developed in recent years [8]. Standard map is chaotic and it can be employed to shuffle the positions of image pixels to get a totally visual difference from the original images [9] [10]. Different from the conventional schemes based on Standard map, they disordered the

pixel positions according to the orbits of the Standard map [11]. The proposed shuffling schemes didn't need to discretise the Standard map and own more cipher leys compared with the conventional shuffling scheme based on the discretised Standard map. The shuffling schemes were applied to encrypt image and disarray the host image in watermarking scheme to enhance the robustness against attacks [12]. Image Encryption Based on Explosive Inter Pixel Displacement of the RGB Attribute of a Pixel: In this method focus was more on the inter pixel displacement rather than just manipulation of pixel bits value and shifting of pixel completely from its position to new position. RGB value of pixel was untouched in this method, but R value of pixel jumps to another location horizontally and vertically same as in chaotic method [13]. In the similar manner, G and B values of pixel. With the proposed method in this paper, the shuffling of the image will be done by displacing the RGB pixels with their respective components.

III. PROPOSED ARCHITECTURE OF IMAGE ENCRYPTION

The following flow chart as shown in fig.1 is showing the overview for an image encryption where Arnold map and chaotic method are jointly used. 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. Wavelet transform is also used as edge preserving so that the original information of edges may not loose. 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.

Algorithm:

Step 1: Input color image and extract the color components, 'r' as red, 'g' as green and 'b' as blue.
Step 2: Apply discrete wavelet transform on each component obtain from step 1.
Step 3: Store the detail part of each component for preserving structure.
Step 4: Apply Arnold transform of each component based on entropy.

a) Each component's Approximation part of Image is divided into n*n blocks.
b) Each block of each component is shuffled row wise as well as column wise.
c) Calculate Entropy (log energy) of each block of each component
d) Calculate average Entropy from blocks of their respective components.

$$\text{LE} = \sum_i \log(X_i)^2$$

e) Compare Entropy of each block from average Entropy. If Entropy is less than average Entropy, Move to next step. Else do transpose of block and perform shuffling row wise and column wise.
f) Arnold transform is applied to each shuffled block of each component. 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 5: Perform concatenation of stored detail coefficients. Also, for encrypted red 'r', green 'g' and blue 'b' components.
Step 6: Inverse wavelet transform is performed to reconstruct the image using encrypted approximation part and stored detail coefficients.
Step 7: Over the reconstructed encrypted image, another layer of encryption is applied using entropy based pixel chaotic shuffle method so that the detail parts can also be encrypted.

a) Outcome of step 6, Divided into number of large blocks.
b) Select proper initial values and system parameters to create chaotic variable sets of each block.
c) Prepare the chaotic sequences (according to sorting algorithm) of each block.
d) Transfer MxN matrix as MNx1 of each block.
e) Perform the shuffle function on each pixels of matrix of each block.
f) Calculate Entropy (log energy) of each block and also calculate average entropy.
g) Compare Entropy of each block from average Entropy. If Entropy is less than average Entropy, Move to next step. Else do transpose of block and perform shuffling again.

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 layer encryption is used. First layer is structure preserving encryption and second layer is provided secured structure using pixel chaotic shuffle method. Entropy gives the average amount of information. Where entropy is high, that block is more secured in both layers.

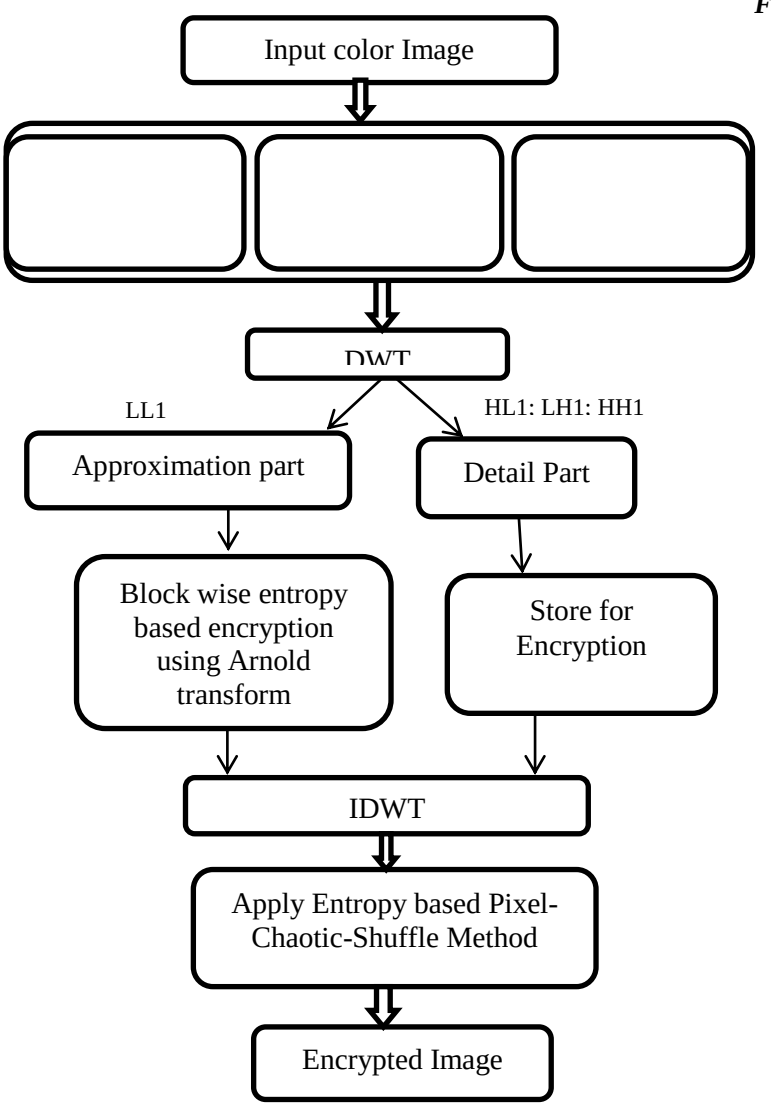


Figure 1: Proposed Architecture of image encryption

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 2, fig 3, fig 4 and fig 5. Original images are fig 2(a), fig 3(a), fig 4(a) and fig 5(a). Encrypted images are fig 2(b), fig 3(b), fig 4(b) and fig 5(b) and Decrypted images are 2(c), fig 3(c), fig 4(c) and fig 5(c).

(a) (b) (c)

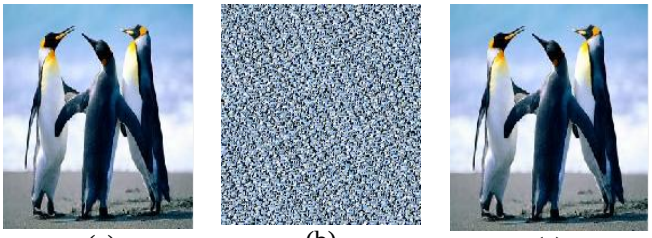
Figure 2: (a) Original image: Lena (b) Encrypted image and (c) Decrypted image

(a) (b) (c)

Figure 3: (a) Original image: Chrysanthemum (b) Encrypted image and (c) Decrypted image

(a) (b) (c)

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



(a) (b) (c)

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

The images used will have their RGB colors extracted and their RGB values transposed and shuffled to obtain ciphered images. The ciphering of the images for this research will be done by using the RBG pixel values of the images only. In this method, there were no changes of the bit values of the images used and there was no pixel expansion at the end of the encryption and the decryption process. The numerical values of the pixels were displaced from their respective positions and the RGB values were interchanged with respective components to obtain the ciphered images. This implies that, the total change in the sum of all values in the image is zero. The images were looked at as a decomposed version in which the three principle component which forms the image was chosen to act upon by the algorithm. The RGB components were considered as the triplet that forms the characteristics of a pixel. The pixel is the smallest element of an image that can be isolated and still contains the characteristic found in the image. The RGB values were shifted out of their native pixel positions and interchanged within the image boundaries.

The Shift displacement of the R G and B Values known as the component displacement factor array was different for the R, G and B. Mean error for original and decrypted images are calculated and given in Table 1.

Table 1: Mean error

Input Images	**Mean error**
Phantom	0.0312
Lena	0.0981
cameraman	0.0109
Penguins	0.0320

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.

V. CONCLUSIONS

This paper gives a new image scrambling algorithm, by using image scrambling to encrypt the image to improve the security of image. The transposition and reshuffling of the RGB values of the image in steps has proven to be really effective in terms of the security analysis. The encryption of R G B components has increased the security of the image against all possible attacks available currently. Entropy based encryption using Arnold and pixel chaotic shuffling increases the level of security. Computed Mean error indicates that decrypted image is almost same as original image. By using multi-region scrambling, it can more effectively improve the security of image, lead decipher even more difficult. It simulates scrambling under Matlab 7.1 to confirm it. Apart from the security consideration, running speed of the algorithm is also an important aspect for a good encryption algorithm.

REFERENCES

[1] X. He, Q. Zhu, and P. Gu, "A new chaos-based encryption using chaotic logistic map," Image and Vision Computing, vol. 24, no. 9, pp. 926-934, 2006.

[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] Ismet Ozturk and Abrahim Sogukpinar, "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] 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] 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.

[13] 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.

