IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology
Vol. 3, Issue 6, June 2016

Improved Dynamic S-Box encryption Followed by Inter pixel Displacement for Secure E-Mail

Vaseeja V[1], Logaprakash M[2], Labeed K Abdulgafoor[3]

M.E Computer Science, Dept of Computer Science and Engineering, SVS college of Engineering, Tamilnadu, India [1]

Assistant Professor, Dept of Computer Science and Engineering, SVS college of Engineering, Tamilnadu, India [2]

R&D Engineer, Prominent, TBI, NIT, Calicut, Kerala, India [3]

Abstract: The security of the E-mail messages is an important issue; no such security is supported by the Internet standards. To overcome the attacks and to improve the security a new model is used which is "Secure Mail using Visual Cryptography". In this method the messages have to be transmitted is converted into a gray scale image. Then (2, 2) visual cryptographic shares are generated from the gray scale image. The shares are encrypted using A Chaos-Based Image Encryption Algorithm using Wavelet Transform and authenticated using Public Key based Image Authentication method. One of the shares is send to a server and the second share is send to the recipient's mail box. The two shares are transmitted through two different transmissions medium so man in the middle attack is not possible. If an adversary has only one out of the two shares, then he has absolutely no information about the message. At the receiver side the two shares are fetched, decrypted and stacked to generate the grey scale image. From the grey scale image the message is reconstructed .But in this can see an outline of image from one share. And also Encryption techniques used for encrypting textual data does not work with images, so separate encryption techniques are required for images. So, we proposed here a new scheme for image encryption which is helpful for end to end secure transmission of digital information on open network using explosive block displacement followed by inter-pixel.

Keywords: chaos based image encryption algorithm, low frequency wavelet coefficient, visual cryptography, dynamic s-box algorithm, wavelet decomposition, Image Encryption, Block, Transformation, Inter-Pixel.

I. INTRODUCTION

Due to the advancement in the software and hardware technology, images in the present scenario are holding more confidential information and in the IT world of presentations, images are vastly in use. In most of the presentations images are widely used in presenting the company information, charts etc. and low cost availability of open networks [1], professionals often transfer these highly critical information over network and unauthorized access to this information can lead to vital loss to company.

In the same manner images are commonly used in other domains where they are used to store confidential information of different processes in the company. Apart from this professional use, images are used to store the genetic information of human being since birth and which further used by different organizations as a password to differentiate between authorized and unauthorized access because every single man has biological differences like no two man can have same finger scan [2]; now a days finger scan is in very common use for marking the attendance [3] in the offices by employees and concept of marking attendance follow the same rule that no two person can have same finger scan

II. EXISTING SYSTEM

In the secure mail using visual cryptography the message to be transmitted is converted into a gray scale image. By converting the message to grey scale image the size of the message can be reduced to 1/5 of the original message.

Then (2, 2) visual cryptographic shares are generated from the gray scale image. The idea of (2, 2) Visual Cryptography is to split secret 'a' into 2 pieces called shares. If an adversary has only one out of the two shares, then he has absolutely no information about the secret 'a'..

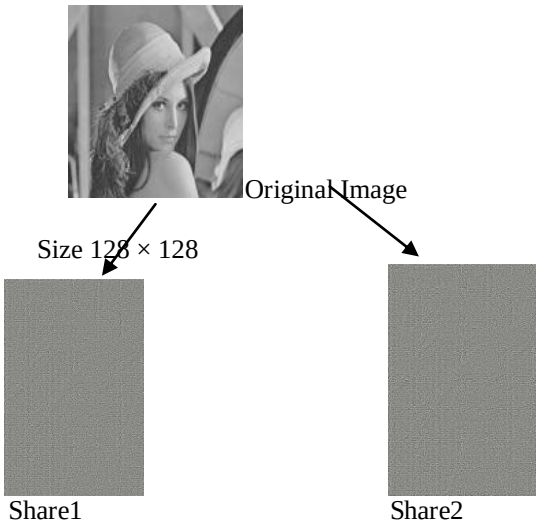
A. Visual Secret Sharing Scheme using Greyscale Images
The idea of (2, 2) Visual Cryptography is to split secret 'a' into 2 pieces called shares. If an adversary has only one out of the two shares, then he has absolutely no information about the secret a.

First of all each pixel value in a grayscale block is transformed into binary representation. For example take a grayscale block and transform into binary blocks. Take each binary block and go for different possible combinations of that block, and design the block into different shares

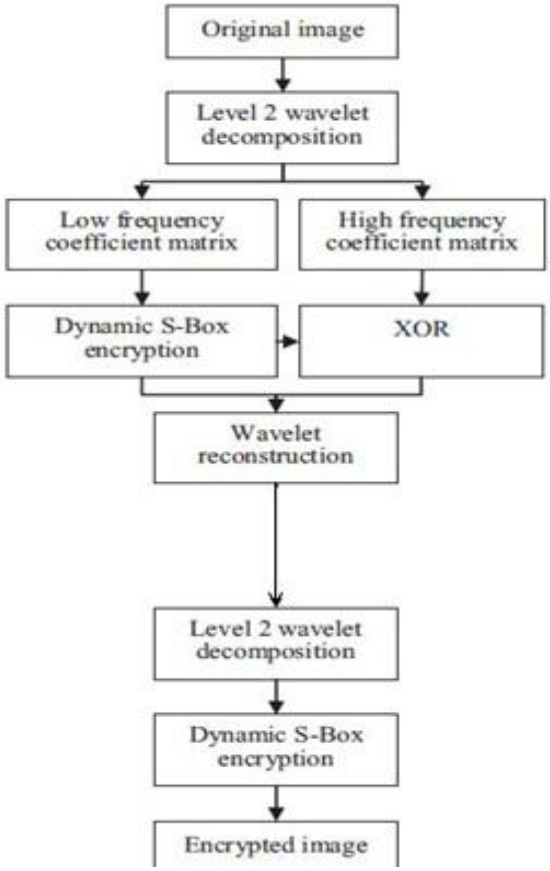
Combining the two shares will give the exact bit and by doing the same procedure for the whole grayscale block gives the perfect high quality image when reconstructed without any loss of contrast.

Generating two separate shared transparencies for gray-level visual cryptography

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Vol. 3, Issue 6, June 2016



B. Encryption



Encryption of Low Frequency Coefficient Matrix:

Step 1: Input the original image and 4 32-bit unsigned integer keys: key1, key2, key3, key4.

Step 2: First, 2 level wavelet decomposition is applied to original image. The main information of image Pm*n is thus concentrated in low-frequency part, which is LL2 part in Fig.2. Second the Dynamic S-Box Algorithm [13] encrypt the low-frequency wavelet coefficients (LL2),there are 4 32- bit unsigned integer keys: key1, key2, key3, key4.

Step 3: Apply an XOR operation to the high-frequency part (Apart from the LL2 part) and the encrypted part in Step 1 as the key stream. Then a wavelet reconstruction is used for the result.

Step 4: For the result of Step 3, use the Arnold matrix for scrambling. Scrambling method is generated through (x,y),

Step 5: Change the value of key1 and key3, key2 and key4.

Apply Step 2 to the result of Step 4. Finally output the cipher image to complete the encryption process.

Encryption of High Frequency Coefficient Matrix:
An XOR operation is used for high-frequency wavelet coefficients and the encrypted low-frequency wavelet coefficients (as a key stream), so that the image information contained in high-frequency wavelet coefficients is hidden. The low frequency wavelet coefficient LL2 shown in Fig. 2 is encrypted using dynamic S-box algorithm. The high frequency wavelet coefficients HL2, LH2, HH2 are encrypted by XORing with encrypted LL2 part. The high frequency wavelet coefficients HL1, LH1, HH1 after first level wavelet coefficients are encrypted by XORing with LL1 which is reconstructed from the encrypted LL2, HL2, LH2 and HH2 parts.

C .Dynamic S-Box Algorithm:
The Dynamic S-Box Algorithm Flow Chart is shown in Fig.3. The dynamic S-box Algorithm is used to encrypt 8*8 pixel blocks division of the image.

Step 1: Input 4 32-bit unsigned integer keys: key1, key2, key3 key4, times represents the number of encryption rounds (Here times is 4). In key generation process, u0 = 1.9999. The initial values of logistic map for the S-box and Chebyshev map for the scrambling are generated by the 128- bit key.

Step 2: sbox_x0[k][j] is the initial value of the S-box in kth round j-th block. First, the original image is divided into 8*8 pixels of blocks, and P0={r, g, b}T ,where P0 is the first pixel in every block.

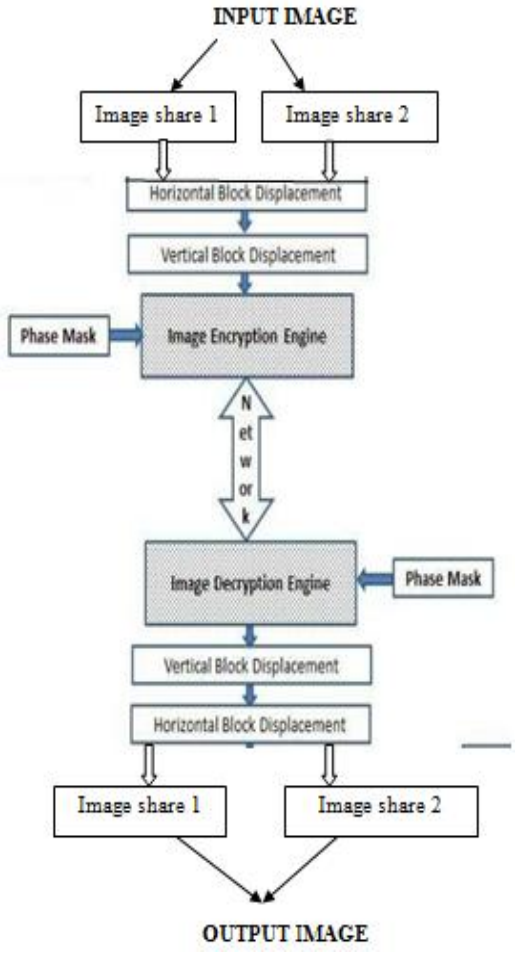
Step 3: Every byte of S-box output is divided into two parts: the high 4-bit, and low 4-bit, then put into sbox_out[0..384]. Second, a length of (8*8-1) *3*2 sequence is generated with initial value P_u0[k] (1). Put s[0..378] in step 2 one-one corresponding to p[0..378], then sort p[0..378] and change pixel position in s[0..378] correspondingly. Third, p[192] is obtained by combining each high 4-bit and low 4-bit. Finally, change the position of the 3 bytes in the front and 3 bytes in the end

III. PROPOSED SYSTEM

As shown in the architectural diagram of proposed method, blocks are identified from the input images as per the criteria then these blocks are passed into the

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Vol. 3, Issue 6, June 2016

displacement phase which consist of two steps i.e. Horizontal displacement and Vertical Displacement. Vertical displacement is applied on the resulted image of horizontal displacement rather than of plain image. Now this image which is obtain after vertical displacement is passes for image encryption process.



A. Displacement method

Unlike in the previous papers where the encryption is applied directly on the plain image, in this proposed scheme of image encryption; In the First step original image is divided into blocks of n*n sizes which were rearranged using an transform algorithm presented in this paper. This transform image is now used for encryption rather than applying encryption procedure on plain image. This transformation of blocks reduces the co- relation between the adjacent pixels and higher entropy. This is being tested by making blocks of different sizes and then their result is being analysed.

Horizontal displacement method will identify the number of horizontal and vertical blocks in an image and accordingly it will explosively displace the blocks in horizontal direction in the 1:2:3 manner; according to this method, block at location 1st will to 2nd block position, 2nd block will move to 4th block position and 3rd block will move to 6th block position. This displacement of blocks is circular which further means that there will be no loss of data in displacement. Number of pixels in a block will be determining by bSize, rows and cols are the number of rows and number of cols in the image. After performing the horizontal block displacement, this will invoke the another method

Vertical displacement method will work in the same manner as of horizontal displacement method, but this will displace the blocks in the vertical direction instead of horizontal direction. Rest of functionality is same as per previous method. After performing vertical displacement of blocks, this will invoke the Perform Encryption method.

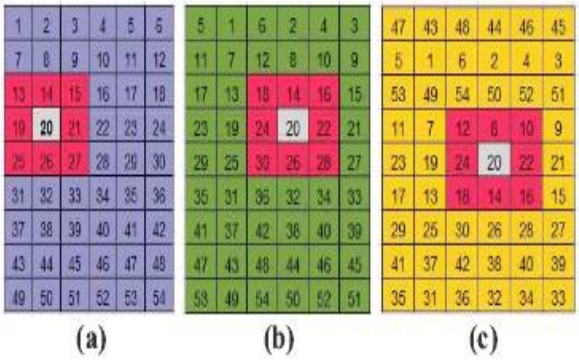


Figure 4.1 (a) Correlation of Pixel blocks with neighbouring pixels in original image. 4.1 (b) shows the block position after horizontal splacement. 4.1 (c) shows the block position after vertical displacement.

B. Authentication

The digital signature scheme is used for the authentication of shares. The process of signature generation is as follows:

1) The sender creates a message.
2) The two shares of the message are created by using Visual cryptography.
3) Then apply a 2-level wavelet transform to each share.
4) SHA-1 is used to generate a 160-bit hash code of the LL2 part of each share.
5) The hash code is encrypted with RSA using the sender's private key, and the result is prepended to each share.
6) The receiver uses RSA with the sender's public key to decrypt and recover the hash code.
7) The receiver generates a new hash code for each share and compares it with the decrypted hash code. If the two match, the message is accepted as authentic.

Transmission of Shares: The two shares are encrypted using Chaos-Based Image Encryption Algorithm Using Wavelet Transform with two different session keys. The session keys are encrypted with RSA using the recipient's public key and are prepended to the shares. The receiver uses RSA with its private key to decrypt and recover the session keys. The shares are added as inline images in e-mail. One share is send to the recipient's mail box and the second share is send to server. The two shares are transmitted through two different transmissions medium so man in the middle attack is not possible. If an adversary has only one out of the two shares, then he has absolutely no information about the message.

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Vol. 3, Issue 6, June 2016

Decryption of Share: At the receiver side the two shares are fetched one from the server and the other from the mail box. The receiver uses RSA with its private key to decrypt the session key part and recover the session keys. Two shares are decrypted using A Chaos-Based Image Encryption Algorithm Using Wavelet Transform with the session keys. In the decryption process first two level wavelet decomposition is applied to each share. The low frequency wavelet coefficient LL2 shown in Fig. 2 is decrypted using dynamic S-box algorithm.

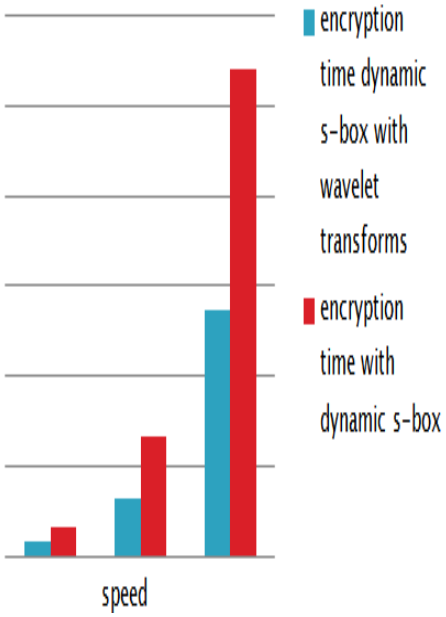
The receiver uses RSA with the sender's public key to decrypt and recover the hash code. The receiver generates a new hash code for each share and compares it with the decrypted hash code. If the two match, the message is accepted as authentic. After that the two shares are stacked to generate the grey scale image. From the grey scale image the message is reconstructed.

IV. PERFORMANCE ANALYSIS

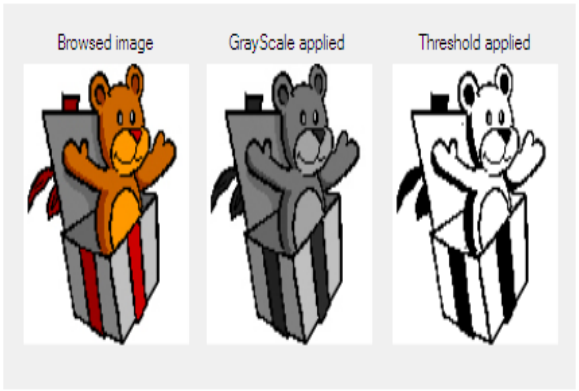
Efficiency

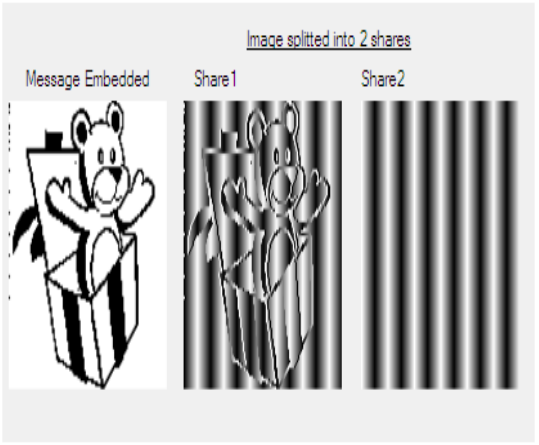
The e-mail security is enhanced by generating two shares and transmitted to the receiver over different channels. If an adversary has only one out of the two shares, then he has absolutely no information about the message. Each share are encrypted two times but only 1/16 of each shares are encrypted S-Box algorithm. The application of wavelet transform in the encryption scheme makes the slow chaotic Dynamic S-Box algorithm apply to the data block which is only 1/16 of the plaintext in terms of size.

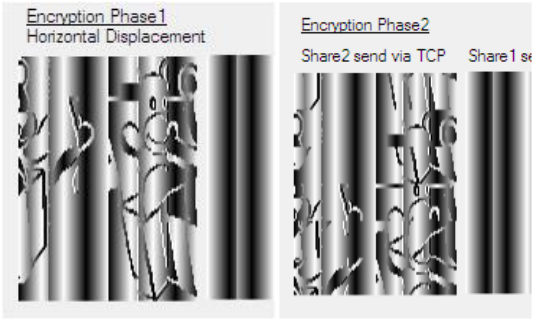
In addition, the adopted XOR operation and diffusion process with 2-D Arnold both have a computing complexity of O(n) (n is the size of plaintext), so, consequently, the efficiency of encryption will increase a lot compared with the Dynamic S-Box. The experiment's results are illustrated in Table I, and the statistic shows that the efficiency doubles. In the (2,2) visual cryptography scheme the quality of the image is maintained perfectly without any loss of generality and without pixel expansion problem.

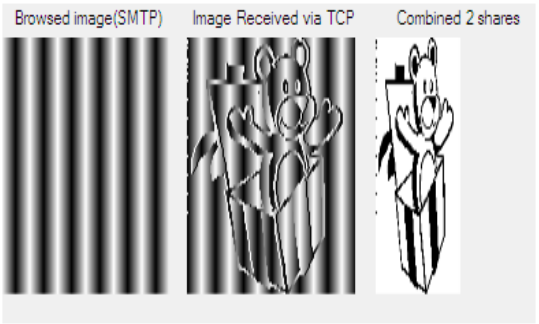


V. EXPERIMENTAL RESULTS









VI. CONCLUSION

In the secure mail using visual cryptography the message to be transmitted is converted into a gray scale image. Then (2, 2) visual cryptographic shares are generated from the gray scale image. The shares are encrypted using A Chaos-Based Image Encryption Algorithm Using Wavelet

Transform. One of the shares is send to a server and the second share is send to the recipient's mail box. The two shares are transmitted through two different transmissions medium so man in the middle attack is not possible. If an adversary has only one out of the two shares, then he has absolutely no information about the message. At the receiver side the two shares are fetched, decrypted and stacked to generate the grey scale image. From the grey scale image the message is reconstructed. Out of one share can see an outline of image, to avoid use image encryption with inter pixel displacement. And also use image with any size. So get a secure mailing system

ACKNOWLEDGEMENT

We would like to appreciate to all of instructors and friends at Department of computer science, professors and assistant professors, Head of department, SVS College of engineering, TAMILNADU,

REFERENCES

[1] Ajish S and Rajasree R Secure Mail using Visual Cryptography (SMVC), 5th ICCCNT 2014July 11- 13, 2014, Hefei, China
[2] Amnesh Goel and Nidhi Chandra A Technique for Image Encryption Based On Explosive n*n Block Displacement Followed By Inter-Pixel Displacement of RGB Attribute of A Pixel , 2012 International Conference on Communication Systems and Network Technologies
[3] William Stallings, Cryptography and Network Security, Pearson Education Inc publishing as Prentice Hall.
[4] Sandeep Katta, Visual Secret Sharing Scheme using Grayscale Images, Department of Computer Science, Oklahoma State University Stillwater, OK 74078.
[5] Zhu Yu Zhou and Zhe Yang Haibing and Pan Wenjie Zhang Yunpeng, A Chaos-Based Image Encryption Algorithm Using Wavelet Transform, 2010 IEEE.
[6] J K Mandal and S Ghatak, Secret Image / Message Transmission through Meaningful Shares using (2, 2) Visual Cryptography, IEEEInternational Conference on Recent Trends in Information Technology, ICRTIT 2011.
[7] Zhou Zhe and Yang Haibing and Zhu Yu and Pan Wenjie and Zhang Yunpeng, A Block Encryption Scheme Based on 3D Chaotic Arnold Maps, 2009 International Asia Symposium on Intelligent Interaction and Affective Computing.
[8] Seyed Hossein Kamali and Reza Shakerian, A New Modified Version of Advanced Encryption Standard Based Algorithm for Image Encryption, 2010 International Conference on Electronics and Information Engineering (ICEIE 2010).
[9] Xiping He and Qionghua Zhang, Image Encryption Based on Chaotic Modulation of Wavelet Coefficients, 2008 Congress on Image and Signal Processing, May, 2008, Sanya, Hainan, China.
[10] Serge Mister and Robert Zuccherato, An Attack on CFB Mode Encryption As Used By OpenPGP, Entrust, Inc., 1000 Innovation Drive, Ottawa, Ontario, Canada K2K 3E7.
[11] Guanrong Chen and Yaobin Mao and Charles K. Chui, A symmetric image encryption scheme based on 3D chaotic cat maps, Chaos, and Fractals, 2004, 749-761.
[13] Stephane G Mallat, A Theory for Multiresolution Signal Decomposition: The Wavelet Representation, IEEE Transaction on Pattern Analysis and Machine Intelligence, Vol 11, No. 7, July 1989..
[12] S Behnia and A Akhshani and S Ahadpour and H Mahmodi A fast chaotic encryption scheme based on piecewise nonlinear chaotic maps, Physics Letters A, 2007, 391-396.
[13] S R Subramanya and Byung K Digital signatures, 2006 IEEE.
[14] William Stallings Cryptography and Networks Security: Principles and Practices Third Edition, China Publishing House of Electronics Industry, Beijing, 2004