Securing Images using Encryption Techniques A Survey

[1] Vrinda A, [2] Mr. Arun Anoop M

[1] Mtech Student, Department Of CSE, MES College Of Engineering, Kuttippuram

[2]Assistant Professor, Department Of CSE, MES College Of Engineering, Kuttippuram

Abstract - In modern world, security is a big issue and securing important data is hence very essential, so that the data cannot be intercepted or misused for illegal purposes. Cryptography is the art or science of encompassing the principles and methods of transforming an intelligible message into that is unintelligible and then retransforming that message back to its original form. Image trafficking across the network is increasing rapidly. Security has become an inseparable issue in digital image transport over the internet. The most widely used and accepted technique for securing digital images is cryptography and various encryption techniques which involves permutation based encryption and visual encryption techniques are summarized here.

***Keywords* - Network Security, Image Encryption, Visual Cryptography.**

1. Introduction

Information and communication technology are developing at a faster pace, and huge data is transmitted over a communication channel, which needs security. Even personal data or secret data should always be kept safe and secure from being misused. Several applications like information storage, information management, patient information security, satellite image security, confidential video conferencing, telemedicine, military information security and many other applications, require information security in their corresponding areas. For this reason, cryptographers are always trying to propose new methods and techniques to keep data/information secure [1].

The image encryption methods [5] are usually classiffied into three types:

(1) Position permutation
(2) Value transformation
(3) Visual transformation

The use of several permutation techniques [5] together will produce effective image encryption. The meaningful information present in images are due to the proper alignment and correlation of pixels in them. This perceivable information can be reduced by decreasing the correlation among bit, pixels and blocks using various permutation techniques.

Visual Cryptography [4] is an encryption technique where a secret image is cryptographically encoded into n shares. In visual secret sharing scheme (k,n) the secret images can be visually revealed by stacking together any k or more transparencies of the shares and by inspecting less than k shares one cannot retrieve the secret image. A nice way of secure communication is obtained through a simple algorithm where decoding is done without any cryptographic computation. Using visual cryptographic scheme, any image or text to be encrypted is fed as an image in the system to generate shares. Shares will be like random noise. Some important goals while developing a visual cryptography scheme is to always have an optimum number of shares ,a good quality of reconstructed image and keeping the size of share so small. Basic VC schemes are used for secured transfer of images, handwritten documents, ,financial documents, text, images, topological maps used in military operations, satellite communication etc. in a secured manner.
A brief overview of image encryption techniques are studied and summarized here.

2. Literature Survey

Several techniques exist in literature for securing digital images over internet. Some innovations are listed here. They are

i. Image encryption using advanced hill cipher algorithm[2]

ii. SD-EI(Combined image encryption technique)[3]
iii. SD-AEI(An Advanced Combined Encryption Technique for Encrypting Images Using Randomized Byte Manipulation)[4]
iv. SD-EI(version 2)(Amalgamation of Cyclic Bit Operation in SD-EI Image Encryption Method: An Advanced Version of SD-EI)[5]
v. Constant Aspect Ratio based (2,2) Visual Cryptography through Meaningful Shares[6]
vi. Enhanced Image Secret Sharing via Error Diffusion in Halftone Visual Cryptography[7]
vii. Enhanced Color Visual Secret Sharing Scheme using modified error diffusion[8]

2.1 Advanced Hill Cipher Algorithm

The core of this algorithm is matrix multiplications. This algorithm during encryption ,takes m successive plaintext letters and instead of that substitutes m cipher text letters[2]. Each character is assigned a numerical value like a = 0,b = 1,..z = 25.The substitution of cipher text letters in place of plaintext letters leads to m linear equations. Decryption uses the inverse of key matrix k .But disadvantage of this method is that inverse matrix does not always exist. So Advance hill cipher which uses an involuntary key matrix [2] is used for encryption. Matrix A is involuntary key matrix if $A = A^{-1}$.

This algorithm works for any images with different grayscale and color images. It is more secure to brute force attacks as compared to original hill cipher algorithm. It is a fast encryption technique.

2.2 SD-EI(Combined Image Encryption Technique)

The correlation among the bits, pixels and blocks are reduced using certain permutation techniques Here, Image encryption is done in two stages[1].

i. Bits rotation and reversal method
ii. Extended hill cipher algorithm

The password is given along with the input image. Value of each pixel of input image is converted into equivalent 8 bit binary number. Now length of password is considered for bit rotation and reversal. i.e., Number of bits to be rotated to left and reversed [1] will be decided by the length of password. Since the weight of each pixel is responsible for its color, the change occurred in the weight of each pixel of input image due to bits rotation reversal [1] generates the encrypted image. Finally extended hill cipher is applied to make it more secure.

2.3 SD-AEI(An Advanced Encryption Technique)

Here image encryption[3] is a four stage process:

i. Generation of Unique Number from the Key
ii. Bit rotation and reversal
iii. Extended hill cipher algorithm
iv. Modified MSA randomization

Generate a unique number from the password (symmetric key)[3] and use it later for the randomization method, which is used to encrypt the image file. The number generated from the password is unique because it is case sensitive and depends on each byte (character) of the password and is subject to change if there is a slightest change in the password. First multiply 2^i , where i is the position of each byte (character) of the password, to the ASCII value of the byte of the password at position i. And keep on doing this until this method is finished for all the characters present in the password. Then add all the values, which is generated from the above mentioned process.

Password is taken along with the input image and then Number of bits to be rotated to left and reversed[3] will be decided by the length of password. Applying extended hill cipher to ensure more security and finally the image is applied with several randomization functions like left and right rotation and cycling functions. Hence the encrypted image is now completely made random and hence more powerful and secure against security attacks. The randomization is totally depending on the password provided in first stage.

2.4 SD-EI(Version 2)

Here the encryption progresses through three stages:

i. Modified Bits Rotation and Reversal Technique for Image Encryption[4]
ii. Extended hill cipher algorithm
iii. Modified Cyclic Bit manipulation[4]

Generate a number from the password (symmetric key)[4] and use it later for the randomization method in modified cyclic bit manipulation[4], which is used to encrypt the image .The number hence generated is password sensitive.

The extended hill cipher and modified cyclic bit manipulation algorithms [4] are given below in Algorithm 1 and Algorithm 2.

1. An involuntary matrix [2] of dimensions m x m is constructed by using the input password
2. Positions of all the rows of and columns of input image are rearranged in bit reversed order
3. Hill cipher technique is applied to this positional manipulated image generated from step2 and obtain final encrypted image

Algorithm 1: Extended hill cipher algorithm

1. Choose consecutive 8 pixels
2. Convert each pixel value to their corresponding 8 bit binary value
3. Form a 8X8 matrix with the 8 bit values of 8 pixels
4. Perform multi-directional matrix Cyclic operation on that matrix code number of times
5. Convert the modified 8 bit value of each pixel to their corresponding decimal value
6. Put the newly generated value in place of the old value of that pixel
7. Go to Step 1, and continue until and unless all the pixel values of the image are modified

Algorithm 2: Modified cyclic bit manipulation

2.5 Constant Aspect Ratio Based (2,2) VCS

This is (2, 2) visual cryptographic scheme where secret will be revealed directly by stacking two meaningful shares [7] in an arbitrary order but with proper alignment. According to the algorithm, the generated shares are meaningful and the aspect ratio [7] and the dimension of the shares are identical with that of the secret image which ensure optimal space requirement.

The secret image and 2 cover images are considered as binary image and are divided into blocks of 4 pixels. The combinations can be like shown in figure 1.

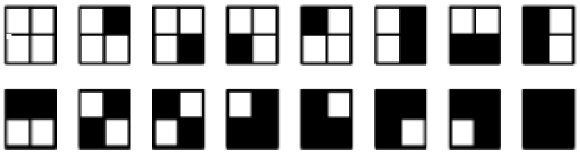

Fig 1:Blocks of secret image

The blocks with hamming weight H(V)=0,1,2 are considered to be white and H(V)=3,4 are considered to be black. The algorithm reads each block at a time and generates blocks of same size. The shares are composed of the white blocks with hamming weight [7] of 2 and black blocks with hamming weight of 3. The possible block combinations of white blocks of generated shares are given below in figure 2.

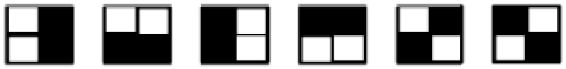

Fig 2:White block of shares

According to the requirement of desired white or black colour the algorithm chooses appropriate combinations given below in the figure 3 along with their permutations.

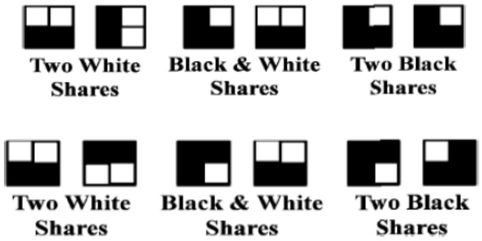

Fig 3: Combinations for white and black

2.6 Enhanced Image Encryption Using Error Diffusion in Halftone Visual Cryptography

Here continuous -tone image is first transformed into a binary image via half toning[10] technique. Then binary error diffusion process is carried out as shown in figure 4.

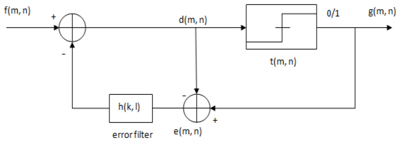

Fig 4:Binary error diffusion

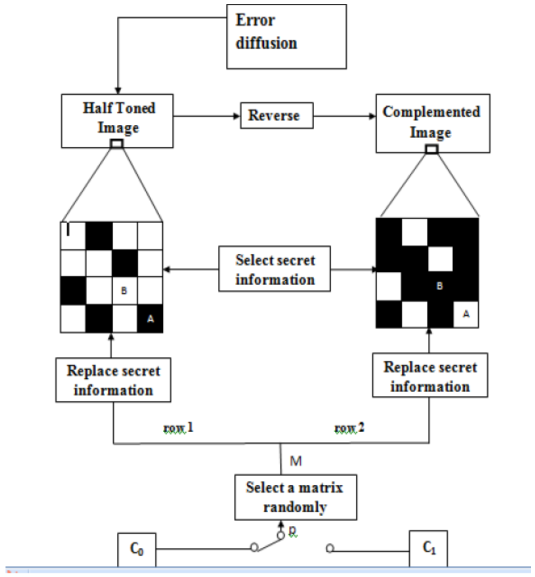

Fig 5:Share Generation Process

The decoding process is done by stacking together the meaningful shares [8].

2.7 Color Visual Secret Sharing Using Modified Error Diffusion

It is based on visual information pixel synchronization (VIP)[9] and Modified threshold error diffusion[9] to attain a color visual cryptography encryption. VIP synchronization retains the positions of pixels carrying visual information of original images throughout the color channels and error diffusion generates shares pleasant to human eyes. The simple halftone method introduces more error in images during quantization. So to reduce these errors we use modified error diffusion technique[9] as illustrated in figure 6.

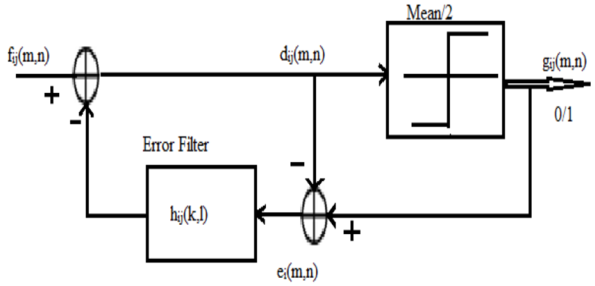

Fig 6:Modified error diffusion

The meaningful share generation involves through two steps:

1. The matrix derivation[9] with VIP synchronization using standard VC matrices
2. The matrix distribution[9]

To get the decrypted secret image, we simply need to stack (OR operation) the encrypted meaningful shares.

3. Performance Analysis

A detailed analysis of the techniques seen in section 2 are done here and summarized in Tab 1 and Tab 2

Tab 1: Comparison of Image encryption techniques

Methods	**Performance Criteria**	
	Time to encrypt/decrypt	**Security**
Advanced hill cipher	Less time	Least secure
SD-EI	More time	Secure
SD-AEI	Maximum time	More secure
SD-EI(Version2)	Comparable to SD-EI	More secure than SD-EI

Tab 2: Comparison of visual image encryption techniques

Methods	**Size Of Image**	**Security**	**Image Type**
CARVCMS	Constant	Secure	Binary
Error Diffusion	Twice	Secure	Greylevel
Modified Error Diffusion	Twice	Secure	Color

4. Conclusions

The encrypted images using combinational approach is more scrambled as compared to individual technique. In future, these image encryption techniques can be combined with other Cryptographic methods (Encryption +Steganography) to build a perfectly secure Cryptographic method for high security information transfer. Visual cryptography Scheme (VCS) is an emerging cryptography technology which uses the characteristics of human vision system to decrypt images without involving complex computation. A combination of many of the techniques discussed above could help secure digital image transfer in internets..

References

[1] D. Somdip, “SD-EI: A cryptographic technique to encrypt images,." IEEE International Conference on Cyber Security, CyberWarfare and Digital Forensic (CyberSec), june 2012.

[2] S. K. P. Bibhudendra Acharya, Saroj Kumar Panigrahy and G. Panda, “Image encryption using advanced hill cipher algorithm," vol. abs/vol 1. , International Journal of Recent Trends in Engineering, May 2009.

[3] D. Somdip, “SD-AEI: An advanced encryption technique for images." IEEE Second International Conference on Digital Information Processing and Communications (ICDIPC), 2012,

[4] S. Dey, “Amalgamation of cyclic bit operation in sd-ei image encryption method: An advanced version of SD-EI method: SD-EI ver-2." International Journal of Cyber-Security and Digital Forensics (IJCSDF) 1(3): 221-225 The Society of Digital Information and Wireless Communications (SDIWC), 2012.

[5] S. P. Indrakanti and P.S.Avadhani,” Permutation based image encryption technique," International Journal of Computer Applications, August 2011, p. 0975 8887.,vol 28,No 8.

[6] A. Saroj Kumar Panigrahy, Bibhudendra and D. Jena.,”Image encryption.

using self-invertible key matrix of hill cipher algorithm,." 1st International Conference on Advances in Computing, Chikhli, India, february 2008, pp. 21 22.

[7] S. Ghatak and J. K. Mandal, “Constant aspect ratio based (2, 2) visual cryptography through meaningful shares." IEEE international conference Westbengal, 2011.

[8] L. J. Anbarasi and N. S. Alex, “Enhanced image secret sharing via error diffusion in halftone visual cryptography." IEEE international conference, 2011.

[9] Rajan and J. James, “Enhanced color visual secret sharing scheme using modified error diffusion." International Conference on Research Trends in Computer Technologies Proceedings published in International Journal of Computer Applications,ICRTC, 2013.

[10] G. R. A. F. I. Zhi Zhou Member, IEEE and G. D. Crescenzo, “Halftone visual cryptography." IEEE Transactions on imageprocessing, 2010.

Vrinda A She obtained her BTech in Information Technology from university of Calicut in the year 2007. She was a member of faculty in the department of information technology at Amrita School Of Engineering,ettimadai, Coimbatore from 2007 to 2009.Later she took up employment as lecturer in department of information technology in MESCE,kuttippuram, kerala. Presently she is pursuing her MTech programme in computer science and engineering at MESCE kuttippuram. She has 5 years of teaching experience.Her research interests covers areas of network security, cryptography and mobile ad-hoc networks.

Arun Anoop M He obtained his BTech in Computer Science and Engineering from cochin university in the year 2008.He completed his PG diploma in information security and system administration from DOEACC center, NIT , Calicut and obtained his MTech in Information Technology from kalasalingam university in the year 2011.Presently he is working as Assistant Professor in Computer Science and Engineering, MESCE, kuttippuram, kerala.Before joining MESCE he has worked as teaching assistant in information technology in kalasalingam university, krishnankoil, Tamilnadu. He is having 3.6 years of teaching experience. He has attended many workshops, FDPs and conferences. His areas of interest are network security, wireless sensor networks, protocol design, formal languages and theoretical computer science. He has presented 3 papers in National and International Conferences. He has published 8 journals and guided 6 Mtech students.