International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

An Enhanced Technique for Secure Image Transmission Via Visual Cryptography and Secret Fragment Visible Mosaic Images

Rucha R. Raut[1], Prof. Komal B. Bijwe[2]

[1, 2]Amravati University, P.R. Pote college of Engineering and Management, Kathora Naka, Amravati

Abstract: ***In this papera new type of computer art image called secret fragment visible mosaic image is proposed which transforms automatically a given large-volume secret image into a so called secret fragment visible mosaic image. The mosaic image, which looks similar to an arbitrarily selected target image and may be used as a camouflage of the secret image, is yielded by dividing the secret image into fragments. The information required for recovering the secret image is embedded into the created mosaic image by a lossless data hiding scheme using a key. Shamir secret sharing algorithm plays an important role in this project. Shamir's secret sharing is an algorithm that divides a secret into shares. For encryption of secret image Shamir Encryption method is used and for decryption process Shamir Decryption algorithm is used. Secret can be recovered by combining certain numbers of shares. An additional measure to enhance the embedded data security is also proposed.***

Keywords: Visualcryptography, Secret fragment visible mosaic images, Shamir Encryption, Shamir Decryption,

1. Introduction

The research which is developed using mathematical methods like security of data, properuser authentication, confidentiality, with respect to information security is called as cryptography. But Visual cryptography is a new technique of information security that uses simple algorithm unlike traditional cryptography which incorporates complex, computationally intensive algorithms. Visual information of pictures, text etc. is dealt with in order to encrypt in progressive and unexpanded VC algorithm. We have only a few pieces of shares and get an outline of the secret image. This is done by increasing the number of the shares being stacked. In today's world images from various sources are frequently utilized and transmitted through the internet for various purposes. These images usually contain private or confidential information so that they should be protected from leakages during transmissions. Recently, many methods have been developed for securing image transmission, for which two mostly used techniques are encryption of image and hiding of data. Image encryption is done by using natural property of an image, such as more redundant power and strong spatial correlation, to achieve encrypted image. The encrypted image is a noise image so that no one can obtain the secret image from it unless user has the correct key. However, the encrypted image is not meaningful, which cannot provide additional information before decryption and may arouse an attacker's attention during transmission due to its randomness in form. The another way to avoid this problem is data hiding that hides a secret message into a target image so that no one can realize the existence of the secret data, in which the data type of the secret message investigated in this project is an image. Specifically, if one wants to hide a secret image into a cover image with the same size the secret image must be highly compressed in advance. Shamir secret sharing algorithm it is a form of secret sharing where a secret is divided into parts, giving each participants its own unique part, some of the parts are needed in order to reconstruct the secret counting on all participants to combine together ,the secret might be impractical and therefore sometimes the threshold scheme is used In this project we state the fact that cryptography can be successfully implemented and used into a of computing technology with image. The secret fragment Visible mosaic image and Shamir secret sharing method are used for this project which satisfies the requirement of cryptography This research will include implementation of cryptographic algorithm for embedding secret image over a target image, as well as technique to dynamically decrypted as original.

2. Previous Work

Chin Chen chang, Min- Shian Hwang, and Tung ShouChen[1] have developed a fast encryption algorithm for image cryptosystems in 2001. Vector Quantization, cryptography and other number theorem is the main platform for this cryptosystems. It is anmeangful technique to low bit rate image compression. In VQ first decomposition of images into vectors takes place and then vector by vector then are sequentially encoded

Young-Chang Hou[2] have presented a technique for visual cryptography of color images in 2002 which consist of three methods for visual cryptography of gray-level and color images based on past studies in black and white visual cryptography, the halftone technology method, and the color decomposition method. His technique gives us backward compability with the ols results in black and white VS along with advantages of black and white VS which is very helpful visual system to decrypt secret image without computation like t out of n threshold scheme which can be applied to gray level and colourful images.

Sabu M Thampi[3] have presented a information hiding technique in 2004 in which a brief history of steganography is explained along with techniques that were used to hide secret information. Textual, audio and image based information hiding techniques like Least Significant

bit(LSB) insertion technique in which embed the information in graphical image file, masking and filtering techniques in which by making an image in a manner similar to paper watermarks and transformation techniques which is done by using discrete cosine transformation or wavelet transform.to hide information in significant areas of image.

Zhicheng Ni, Yun-Qing Shi, Nirwan Ansari, and Wei Su [4] have proposed a new data hiding technique in 2006, i.e.reversible data embedding technique, which can embed a large amount of data (5–80 kb for a 512 512 8 grayscale image) the PSNR of the marked image versus the original image is guaranteed to be higher than 48 dB which kept a large percentage of visual quality for all natural images. For embedding of data it uses the zero or the smallest point of the histogram and slightly modifies the pixel grayscale values. All types of image are based on this technique.

InKoo Kang, Gonzalo R. Arce and Heung-Kyu-Lee [5] have proposed a new data hiding method in 2009, a color VC encryption method which leads to meaningful shares and is free of the previously mentioned limitations error diffusion and pixel synchronization basic principles used in the generation of shares. Error diffusion is a simple but basic algorithm for image halftone generation. In this technique the quantization error at each pixel is filtered and fed back to future input. for VS.
Monisha Sharma[6], have presented a technique using chaotic schemes for data hiding in 2010.Their techniques basically provide security functions as well as visual check, which might be applicable in some applications.. To deal with the technical challenges, the two major image security technologies are under use: (a) Image encryption techniques to provide end-to-end security when distributing digital content over a variety of distributions systems, and (b) Watermarking techniques as a tool to achieve copyright protection, ownership trace, and authentication. They have done the current research efforts in image encryption techniques based on chaotic schemes are discussed.

I-Jen Lai and Wen-Hsiang Tsai[7]have presented a technique of information hiding in 2011 which consist of secret image is first divided into rectangular shaped small fragments(tile images) and then for creating mosaic image they are fix to its next target image selected from a database. Secret key selects randomly some blocks of mosaic images to embed the information of tile image .A hacker without the key cannot retrieve the secret information as the key can reconstruct the secret image by retrieving the embedded information.

Anuprita U. Mande and Manish N. Tibdewa[8] have presented a technique in 2013 for data hiding used in color video cryptography They introduced an error diffusion technique for generating halftone shares which are more pleasant to human eyes. From the review of Color visual cryptography schemes, it is seen that half toning of images is achieved by various methods in different schemes. In this paper, we will take a review of all these methods. At the same time we will compare all these methods and will adopt the one which will give us the best result with respect to color visual cryptography.

Ya-Lin Lee and Wen-Hsiang Tsai [9] have proposed a new scheme in 2014 for secure image transmission which converts a secret image into a meaningful mosaic image with the same size and looking like a preselected target image. Secret key controls transformation process and that secret image is only recover by that key without any loss from mosaic image The proposed method is extended by Lai and Tsai , in which a new type of computer art image, called secret-fragment-visible mosaic image, was introduced.. The mosaic image is the output of rearrangement of the fragments of a secret image in disguise of another image called the target image preselected from a database.

3. Proposed Work

Proposed Methodology has been divided in 2 Phases:-

1) Mosaic Image Creation & Encryption:-
   In this phase, first pick one target image and one secret image. Resize both the images into 256*256 pixel size. Then perform matching of target image blocks with the secret image block until all the blocks of target image get matched with all the blocks of secret image .Here a new rearranged matched secret image is created called as mosaic image. Now perform Shamir Encryption on this rearranged matched secret image.
2) Secret Image recovery:-
   In this phase, whatever the image is encrypted in first phase that is being decrypted.
   Algorithm for Shamir Encryption:-
   1) Pick a Target Image.
   2) Pick a Secret Image.
   3) Perform Matching of Target Image blocks with the Secret Image blocks to get the rearranged secret image (mosaic image).
   4) Apply Shamir Encryption Algorithm on rearranged Secret Image.
   5) Give value of N<10.
   6) Give value of K<N.
   7) Repeat Step 3 & Step 4 until all blocks of Target Image and Secret Image get matched and Encrypted.
   8) Stop.

.
Algorithm for Shamir Decryption:-

1. Select Created N shares in Encryption phase
2. Apply Shamir Decryption on created N shares.
3. Give Values of K (must be less than value of N).
4. Decoding each pixel (0-255).
5. Decrypted Secret image.
6. Generate final original secret Image.
7. Stop

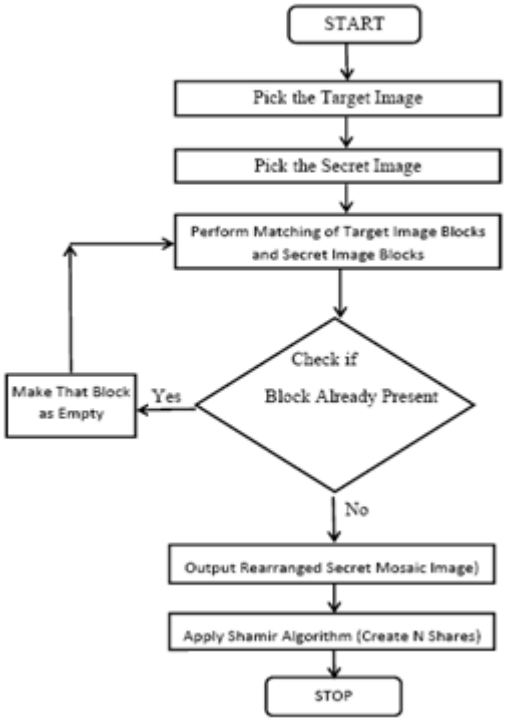

Figure3.1: Flow of Secret Image Encryption

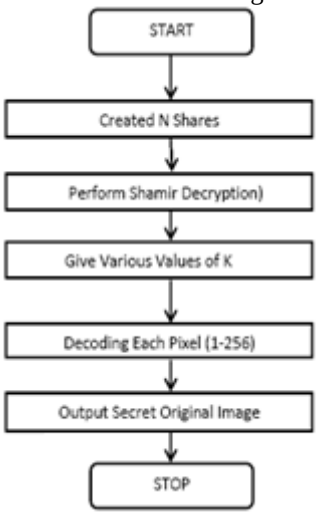

Figure 3.2: Flow of Secret Image Decryption

4. Implementation of Shamir encryption Algorithm

Step1: (Initialization Process)
Initially for image encryption the user has to use Load Target Image button and load Secret Image button from menu.. Target images as well as secret image which require for image Encryption are loaded here. Resize both the images into 256*256 pixel size.

Step2: (Pre-processing)
Perform matching on loaded Target Image blocks and Loaded Secret Image blocks by using knn classifier. The secret image gets rearranged into rearranged matched secret image called as mosaic image.

Step3: (Secret Image Encryption)
In this step Shamir Encryption process is performed on rearranged matched secret image which creates shares of that rearranged matched secret image (N).N must be less than 10 as there is given limit to create shares function in encryption process. Secret Imageencryption operation is performed using Shamir Encryption algorithm.

Step4: (Creating Shares)
Rearranged Matched Secret image get divided into number of shares i.e. N and N must less than 10. Some of these shares (K) are needed to retrieve the secret image at decryption module. Let us see implementation with example as follows. Splitting rearranged secret image intoN shares(N=6). In a Proposed Method, there is creation of shares of rearranged matched secret image as given below.

Figure3.3: Rearranged Secret Image (Mosaic image)

In Shamir's Secret Sharing Algorithm partition of the secret is done by following polynomial:
$F(x1) = y+m_1X_i+m_2X_i^2+\ldots\ldots m_{(k-1)}X_i^{(k-1)} \bmod (p)$, i=1, 2…n
Where y is the share, S_1, pis a prime number and the coefficients of the k-1 degree polynomial m_i are chosen randomly and then the shares are evaluated as S1=F(1),S2=F(2),…Sn=F(n)

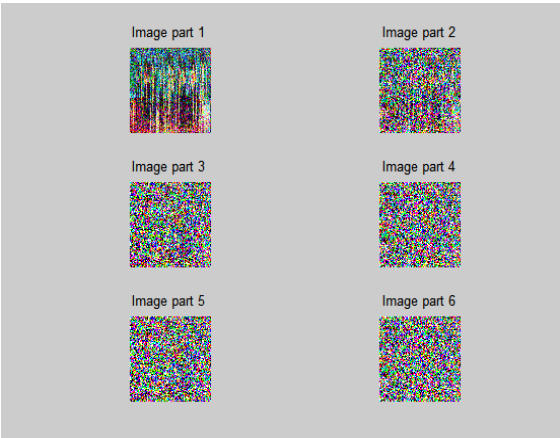

Figure 3.4: Rearranged Secret Image with 6 shares

Implementation Shamir Decryption Algorithm
This module focuses on the implementation aspects of Secret Image Decryption. Following are the steps for the Image Decryption
Step1: (Initialization Process)
Initially for Secret image recovery the user has to select perform Shamir Decryption menu.
Step2: (Pre-processing)
User have to give threshold value means K Means out of N shares how many shares are needed to retrieve the secret image..

Step3: (Decoding pixel)
Decoding of each pixel takes place.From 0-255 each pixel gets decoded.

Step4: (Decrypting image)
After each pixel get decode our original secret image gets decoded here and each extracted image share is present in encrypted form. Therefore, all shares are decrypted using Shamir Decryption algorithm.

Step5: (Combining Shares)
All decrypted shares are finally combined to get original secret image.

Shamir's Secret Sharing Algorithm reconstruction of shares is done by using Lagrange interpolation as follows

Given any kpairs of the share pairs $\{(i,S_i)\}$,i=1,2…n. We can obtain the coefficients m_i ofF(x) by largrange interpolation as follows:

$$S= (-1)^{(k-1)}\left[F(X_1)\frac{(x2)(x3).....(xk)}{(x1-x2)\ (x1-x3)\ ....(x1-xk)} + F(X_2)\frac{(x1)(x3).....(xk)}{(x2-x1)\ (x2-x3)\ ....(x2-xk)} +.... + F\ (X_k)\frac{(x1)(x2).....(xk-1)}{(xk-x1)\ (xk-x2)\ ....(xk-xk-1)}\right]$$

Figure:3.4:Secret image

5. Result Analysis

Analysis with respect to TimeConstrain and PSNR value. The term Peak-Signal-to-Noise-Ratio, often abbreviated PSNR, is an engineering term for the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. Because many signals have a very wide dynamic range, PSNR is usually expressed in terms of the logarithmic decibel scale.

PSNR is most commonly used to measure the quality of reconstruction of image. The signal in this case is the original data and the noise is the error introduced by image encryption in it.The higher the PSNR, better the quality of the original image. PSNR represents a measure of the peak error.

When we concerned with timing constrain of encryption and decryption of an image, there is essential conditions that the time required for encryption is greater than time required for decryption. In the result analysis section we compare these timing constrains and comparative study PSNR for encryption and decryption

Table 4.1 Execution Total Time Difference in Encryption & Decryption when created 6 shares

Name of input Target Image	Name of input secret Image	Size of Target Image	Size of Secret Image	Total time for Encryption	Total time for Decryption
Timg1.jpg	Simg1.jpg	800×600	1600×1200	183.27s	64.17s
Timg2.bmp	Simg2.bmp	240×320	240×320	264.09s	74.04s
Timg3.png	Simg3.png	610×466	1024×768	326.82s	65.37s
Timg4.jpg	Simg4.jpg	135×90	1332×1760	664.97s	88.33s
Timg5.jpg	Simg5.bmp	168×1200	200×200	343.72s	107.02s

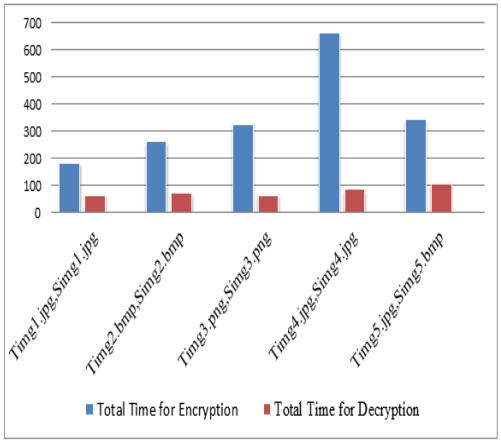

Figure 4.1: Graph shows relation betweenTotal Time of Encryption & Total Time of Decryption when created 6 shares

Table 4.2: Comparison table of PSNR of Encryption & PSNR Of Decryption when created 6 shares

Name of input Target Image	Name of input secret Image	Size of Target Image	Size of Secret Image	PSNR of Encryption	PSNR of Decryption
Timg1.jpg	Simg1.jpg	800×600	1600×1200	54.49db	77.48db
Timg2.bmp	Simg2.bmp	240×320	240×320	55.06db	86.20db
Timg3.png	Simg3.png	610×466	1024×768	55.05db	84.40db
Timg4.jpg	Simg4.jpg	135×90	1332×1760	55.34db	81.53db
Timg5.jpg	Simg5.bmp	168×1200	200×200	55.14db	83.38db

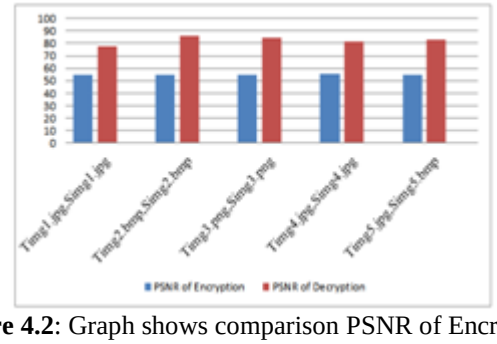

Figure 4.2: Graph shows comparison PSNR of Encryption & PSNR of Decryption when created 6 shares

6. Conclusion

In today's world where nothing is secure, the security of images is very important. A new secure image transmission method has been proposed, which can transform a secret image into a mosaic one and provide more image security.

Also, the original secret images can be recovered by using Shamir encryption and decryption algorithm, in which by combining minimum number of shares the original secret image can be retrieved. The proposed algorithm is more challenging as well, because there is a significant cryptography provided for image security

7. Future Scope

In this dissertation work, we pick a target and secret image of different sizes and for proper output we resize the image into 256*256 so that the final generated image is of size 256*256. But it may possible in future to modify the algorithm so that it can be managed to remain the size of final generated image means secret image of the same size preselected from the database and may be images of color models other than RGB as well as to developing more information hiding applications for images and video using the proposed secret-fragment-visible mosaic images.

References

[1] Chin chenChang,MinShian Hwang and Tung Shou Chen," A new image encryption algorithm for image cryptosystems", *the journal of system and software 58(2001)*
[2] Young-ChangHou" Visual cryptography for color images" *Pattern Recognition 36 (2002)* .
[3] SabuM.Thamp,"Information Hiding Techniques: A Tutorial Review*", ISTE-STTP on Network Security &Cryptography , LBSCE2004.*
[4] Zhicheng Ni, Yun-Qing Shi, Nirwan Ansari, and Wei Su," Reversible Data Hiding", *IEEE transactions on circuits and system for vedio technology, vol. 16, no. 3, march 2006*
[5] InKoo Kang, Gonzalo R. Arce and Heung-Kyu-Lee," color extended visual cryptography using error diffusion", *978-1-4244-2354-5/09/$25.00 ©2009 IEEE*
[6] Monisha Sharma," Image encryption techniques using chaotic schemes: a review", *International Journal of Engineering Science and Technology Vol. 2(6), 2010, 2359-2363*
[7] I-Jen Lai and Wen-Hsiang Tsai,"] Secret-Fragment-Visible Mosaic Image–A New Computer Art and Its Application to Information Hiding", *IEEE transactions on information forensics and security, vol. 6, no. 3, September 2011*.
[8] Anuprita U. Mande and Manish N. Tibdewal," Parameter Evaluation and Review of Various Error-Diffusion Half toning algorithms used in Color Visual Cryptography", *International Journal of Engineering and Innovative Technology (IJEIT) Volume2,Issue8,February2013*
[9] Ya-Lin Lee and Wen-Hsiang Tsai," A New Secure Image Transmission Technique via Secret-Fragment-Visible Mosaic Images by Nearly Reversible Color Transformations", *IEEE transaction on circuits and system for video technology, vol. 24, no. 4, April 2014*

Author Profile

Rucha R. Raut received B.E from PRMITR, Badnerain 2013 from Amravti and pursuing M.E from P.R.Pote College of Engg& Technology, Amravati.

Komal B. Bijwe received B.E from H.V.P.M College of Engg.& Technology in 2007 and M.E from the Prof. Ram Meghe college of Engg.andResearch in 2014. Working as assistant professor in P.R.Pote(Patil) College of Engineering and Management, Amravati.