A Secure and Efficient Secrete Image Sharing Scheme Using Sharing Matrix

[1]Ms. J.J. Pawar, [2]Prof. J.V. Shinde

[1]M. E. Student, [2]Asst. Professor, Dept. Of Computer Engineering, Late G. N. Sapkal College Of Engineering, SPPU, Nashik, India

[1]*pawar.jayshree19@gmail.com*, [2]*jv.shinde@rediffmail.com*

Abstract - With the tremendous and rapid growth of information interchange through internet transmission, information security has become a major issue to deal with. As because images are being used more in business and industrial process, military and medical and also in scientific researches, it has become the important factor to protect the confidential image data from unwanted access or intruders. Because of development of technology, the hacking techniques, and attacks are also becoming more and more intelligent. As a result, traditional approaches of image encryption are failing to be a good competitor with the attackers. Image encryption has been a wide area of research field. The protection of image data is more important because it contains maximum features of a person or thing. Image encryption is employed to protect an image from unauthorized access and increase image security over internet. Nowadays Internet is used for transmitting and storing huge amount of information. Since the internet has many loopholes and several scopes of hacking or being attacked by intruders. We introduce a (k,n)-sharing matrix generation algorithm combined with image encryption and image hiding using steganography(SSME-SIS). The sharing matrix has the huge potential in sharing the secrete images. Then we combine image encryption with sharing matrix and propose a secure and efficient secrete image sharing scheme. Further we apply this scheme for sharing two images at a time using steganography.

Keywords: Cloud computing, Storage security, Provable data possession, Bidirectional authentication.

I. INTRODUCTION

The transmission of information over the communicating devices over the rapidly growing internet requires to be secured. Conventionally Cryptography is used to convert the original information into an encrypted format known as cipher text and then decrypt the cipher text to retrieve the original information data. With the advancement of technology the intruders or the hackers can easily access or modify the data over the network. Hence it is very necessary to secure the information over the network as there can be loss of data. There can be multiple users accessing the same information through the shared files over the network. This information can be misused by any particular user having access. So this information over the network must be protected by imposing security mechanisms like cryptography. The Cryptography provides the Authentication, Confidentiality and Integrity to the information.

In Visual cryptography (VC) method proposed by Naor et al. [2] the secret image is encrypted into n shares. The n shares are distributed to every participant. Any participant can hold one or more than one shares. To regenerate the original secret image, all the participants collect n shares in (n, n) Visual cryptography scheme. In VC encryption algorithm is used to hide the visual information. The process of decryption is done by human visual system. Encryption process adds some noise in the original image to hide the original information and during the decryption process the noise is reduced to retrieve the original information.

Secret Image Sharing Schemes (SSME-SIS) are useful alternatives. The basic idea behind secret sharing is to transform a secret into n “shadows” or “shares” which can be transmitted and stored disjointedly. The original secret image can only be reconstructed from any k shadows (k<n) and any (k-1) or fewer shadows cannot reveal anything about the secret.

The secure and efficient secret image sharing scheme basically uses the combination image encryption, sharing matrix and steganography. In this scheme first the two images to be shared are combined using steganography in a single image. Then a (k, n) sharing matrix is defined by using simple but efficient algorithm. The secure and

 DOI : 10.18231/2454-9150.2018.0448

efficient secret image sharing scheme combines a sharing encoding algorithm with a chaotic-based encryption process. This method can be used for any values of k and n (k<n) and for various formats of original images like binary, grayscale or color images. It generates various shares with every new execution for the same input. It can also verify a fake share involved in the reconstruction phase, which is very important in real applications

II. RELATED WORK

Secret image sharing has drawn considerable attention in recent years. Naor et al. [2] have proposed the VC method at first. In VC the secret image is encrypted into n shares. The n shares are distributed to every participant. They can hold one or more shares. All the participants combine the n shares together in (n, n) Visual cryptography scheme to reveal the original secret image. The encryption algorithm hides the visual information and the process of decryption is performed by human vision. Encryption process adds some noise in the original image to hide the original information and during the decryption process the noise is reduced to retrieve the original information. In VC, every share is transparent, separate and noise-like. It is applicable for only binary images. Its image shares are noisy which can be easily identified and modified by attackers. The reconstructed image is of low quality. It requires a significantly large transmission and storage costs.

Polynomial-based secret image sharing (PSIS) was proposed by Shamir[3]. It uses the Lagrange interpolation to generate shares of the secrete image and regain the original image with a minimum number of image shares. However, it requires a large computation cost in the regenerating phase; a successful regeneration depends on number of image shares and the order in which they appear; and the results are in a data range different from one of the original image.

Yang et al. [4] has also suggested novel (k, n) probabilistic visual secret sharing (VSS) schemes with non-expandable sizes of shares. They have presented various (k, n) schemes depending on the probability technique. The contrast level of this method is same as the conventional VSS schemes. They have also demonstrated that the conventional VSS scheme can be changed to probabilistic VSS scheme by using transfer function.

Alex et al. [5] used various methods for error diffusion to improve the quality of image in the halftone shares of the secrete image to be shared. They have used halftoning in which the continuous-tone image is transformed into a binary image by applying visual secret sharing (VSS) and then use visual cryptography (VC). The halftoning of images is used to add the secret information pixels into a not coded halftone shares. The secrete image is converted into halftone image by gaining visual information. It gets this significant visual information by applying error diffusion to halftone shares simultaneously. The regenerated image is obtained by gathering the qualified shares together. It does not suffer from cross interference of shared secrete images.

Tso et al. [6] introduced a novel image sharing method to satisfy numerous problems such as problem of pixel expansion, low quality of reconstructed image and creating useless shares for image sharing. This method firstly decomposes the secret image to be shared then encodes them into n number of shares. These image shares are then implanted into cover images. This approach is useful for constructing the meaningful shares of the images to be shared. The size of both the original secret image and the generated share is the same. On the receiver side when all the shares are combined together to form a stack the quality of the reconstructed image is better and it has no distortion.
Teng Guo et al. [7] introduced a (k, n) threshold secret image sharing scheme, which is well known as (k, n)-TSISS. It breaks a secrete image to be shared into n number of shares such as any k number of shares can be combined together to regenerate the original secrete image, but no less than k shared shadows can provide any information about the secret image. They have added an AES encryption process previous to the sharing process to generate a computationally secure (k, n)-TSISS. It combines the advantages of small share size with the guarantee of computational security.

Z. Wang et al. [8] have introduced halftone visual cryptography (HVC) via error diffusion, which generates the shadows of pleasing visual information. They have used Error diffusion to construct the shadows such that the noise brought by the current pixels is diffused away while generating the halftone shadows. The secret image data is then naturally embedded into the halftone shadows. The isotropic and homogeneous distribution of the current pixels imposes the minimal noise in error diffusion, leading to shares with very good image quality. It follows the basic principle of visual cryptography, guaranteeing the security of the construction scheme. A large quality index leads to visually pleasing halftone shadows, but it also brings higher contrast loss in the regenerated images. This method gives visually pleasing halftone shadows.

III. SYSTEM ARCHITECTURE

The SSME-SIS has four major functionalities viz. Steganography, Encryption, Sharing Matrix generation, Image reconstruction. Figure 1 shows all the the models of the system.

 DOI : 10.18231/2454-9150.2018.0448

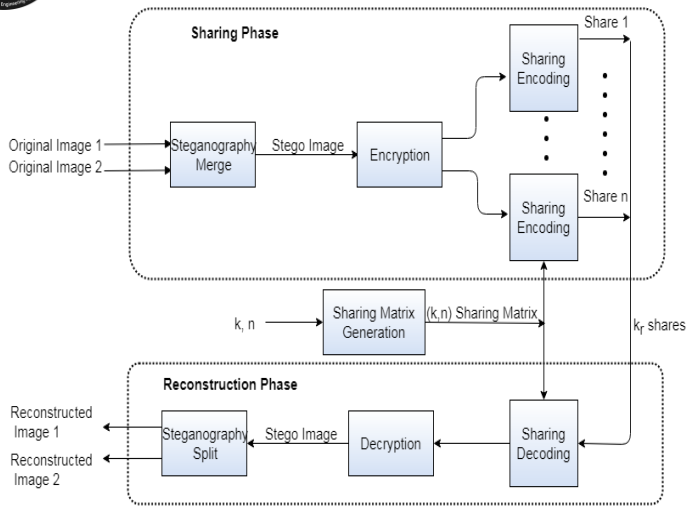

Figure 1: System Architecture

A. *Steganography:*

Steganography is the practice of hiding a file, message, image, or video within another file, message, image, or video. We can describe a digital image as a finite set of digital values, called pixels. Pixels are the smallest individual element of an image, holding values that represent the brightness of a given color at any specific point. So we can think of an image as a matrix of pixels which contains a fixed number of rows and columns. Each pixel has three values (RGB), each RGB value is 8-bit and the rightmost bits are less significant. So, if we change the rightmost bits it will have a small visual impact on the final image. This is the steganography key to hide an image inside another. Change the less significant bits from an image and include the most significant bits from the other image. This process is shown in the Figure2. Thus the image is hidden inside another image without much loss of image quality.

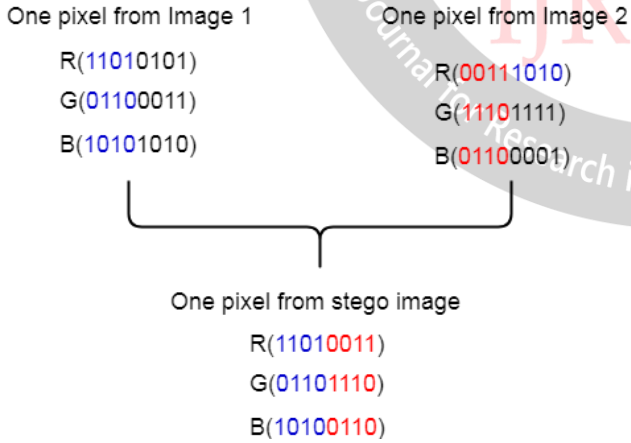

Figure 2: Hiding an image inside another using RGB pixel values

B. *Encryption:*

The encryption is implemented as a process which transfers an original image into one dimensional noise-like data sequence for the further sharing process. Then by using chaotic map random sequences are generated. At the beginning, a random number generator is used to produce a security key. Then the original image is scanned from left to right and then up to down fashion and it is transformed into a one dimensional data matrix. Then the random sequences are applied to the substitution process which encrypts data matrix into a one dimensional matrix. This encrypted one dimensional data matrix is at last combined with the security key and the final encrypted data sequence is obtained.

C. *Sharing encoding:*

The system uses four major steps to generate sharing encoding. The first step is to produce the (k, n)-sharing matrix as shown in the fig 2. We repeat the process to generate the (k, n) sharing matrix in order to make the sharing matrix to be of the same size as encrypted data as the reference for sharing encoding. The (k, n) sharing matrix consist of 0 or 1 values. Every single value from encrypted data matrix is checked against its corresponding value from the sharing matrix from the similar location. If this value is equal to one then it is retained in the data sequence else if the value is zero then it is removed from the data sequence. Thus by using this referenced process, encoded matrix is generated from encrypted data matrix and sharing matrix. After generating encoded matrix, all the important information will be fused into each one dimensional encoded share. Since the final output should be in two dimensions, a transformation from one dimension to two dimensions is applied to each one dimension encoded matrix share. The process of sharing matrix generation is shown in Figure 3.

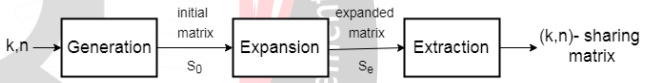

Figure 3: The generation of (k, n)-sharing matrix

The steps involving generation of sharing matrix are explained as below.

1. Initial generation of matrix:

In initial generation of matrix, a matrix M1 with size of (2k-2) x 1 is constructed such that it contains (k - 1) zeros and (k - 1) ones. Then all the possible permutations of M1 are generated as M2, M3, M4, …, Mn. The initial matrix S0 is generated by concatenating all these permuted matrices.

2. Expansion of initial matrix:

The expansion of initial matrix S0 is to generate a new matrix Se of larger size with respect to the value of n. The self-repeating process is used to expand S0 to obtain a new expanded matrix Se.

3. Row extraction:

According to the user's setting or a random sequence, row extraction randomly selects n rows of elements from large expansion matrix to obtain the final (k, n)-sharing matrix.

D. *Image Reconstruction*

To completely reconstruct the original image from total n shares, the authorized users should receive kr (kr >= k)

 DOI : 10.18231/2454-9150.2018.0448

image shares. The regeneration procedure of original secrete image is not related to the particular order of shares of image. In the reconstruction procedure sharing decoding is performed followed by decryption of the image. Firstly Each two dimensional share is transformed to a one dimension sequence of data, then it is divided into three parts, the first two values to recover size of expansion matrix using the inverse processes; next few integers to be transformed to a binary sequence; the last is the rest of the data. The reconstructed matrix is obtained in encrypted form by combining the last data of each received share together by using the recovered sharing matrix as a reference. This encrypted matrix is divided in two parts, the key and the data. At last the original image is reconstructed using the encryption key applied on the data.

IV. SYSTEM ANALYSIS

E. Algorithm

The secure and efficient secret image sharing scheme using sharing matrix performs steganography on two images and hides one image into another. Then encryption is applied on the combined image to change it into a random noisy sequence then hide the encryption key into secret share itself. Thus, every generated image share is chaotic, and cannot leak any information. In the reconstruction phase, the identity of recovered encrypted image is checked against the encrypted image before secret sharing and then the correct decryption key can be extracted successfully to obtain the original image. This system gives completely unpredictable, various and unique secret shares.
Basic steps of the algorithms used are as follows

1. Image Sharing algorithm
Step1. Get the RGB from the image 1 and image 2 as binary values.
Step2. Merge the most significant bits from the image 1 with the most significant bits from the image 2
Step3. Convert the new binary value to a decimal value: And set it to a new pixel position from the resulted image.
Step4: Transfer the original image to be shared into a one dimensional noise-like data sequence
Step5: Produce the security keys
Step6: Generate the final encrypted data sequence by combining outputs of step1 and step2.
Step7: Construct a matrix M_1 of size of (2k -2) × 1 such that it contains (k - 1) zeros and (k - 1) ones
Step8: Obtain all possible permutations of M_1 viz. M_2, M_3, ..., M_n
Step9: Concatenate all the permuted matrices obtained in step8, together to generate the initial matrix S_0 such as $S_0 = [M_1, M_2, \ldots, M_n]$
Step10: According to the value of n, generate a new expansion matrix S_e with a large size
Step11: Select n random rows of elements from expansion matrix S_e to generate the final (k, n)-sharing matrix
Step12: Perform point to point multiplication on matrices obtained in step3 and step8 to obtain the encrypted data sharing matrix R

2. Image Reconstruction algorithm
Step1: Collect at least k shadow images.
Step2: Generate a matrix R_m with the same size that of R.
Step3: Generate a reconstructed matrix R_r by using bit-level Boolean function "or".
Step4: Extract decryption key from the extracted encrypted image
Step5: Recover the stego image
Step6. Extract each RGB channel as a binary value from the current pixel
Step7. Create a new RGB value by concatenating only the 4 rightmost bits from the current pixel with zero values
Step8. Convert the binary value to a decimal value and set it to the current pixel in the new image

F. Experimental Setup

Desktop Application using Java Development Kit-1.8 is created for Scalable and efficient Secrete Image Sharing using sharing matrix. The System is tested on Pentium IV system with 2 GB RAM.

V. RESULTS AND DISCUSSION

To demonstrate the robustness of SSME-SIS with different (k,n)-sharing matrices. The secret shares are noise-like image, protecting from information leakage. And the k can be set to 3, 4, 5, and other any number users want to use. Most importantly, with enough number of shares, the original image will be reconstructed. When only less than k shares are available, the reconstructed images are noise-like. A higher PSNR or SSIM value means better quality, and thus more similar to the original image. As shown in Figure 4 PSNR of SSME-SIS is slightly lesser than the existing system SMIE-SIS. But it doesn't affect the visual quality of the image much. After combining the steganography with the sharing process the PSNR of one of the image, as shown in the Figure 5, decreases further but it is still visually good reconstructed image. The SSIM values are also compared for both the existing and proposed systems. The SSME-SIS is having an average of 0.98 whereas the SMIE-SIS has SSIM value as 1as shown in Figure 6. This shows that the SSME-SIS is able to achieve secrete sharing of two images at a time of images with not much loss in the quality but much higher security as compared to SMIE-SIS.

 DOI : 10.18231/2454-9150.2018.0448

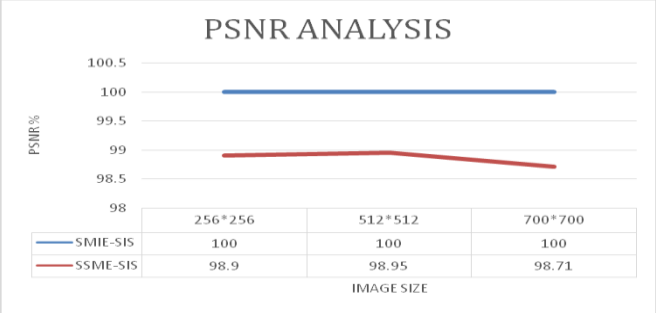

Figure 4:PSNR Comparison

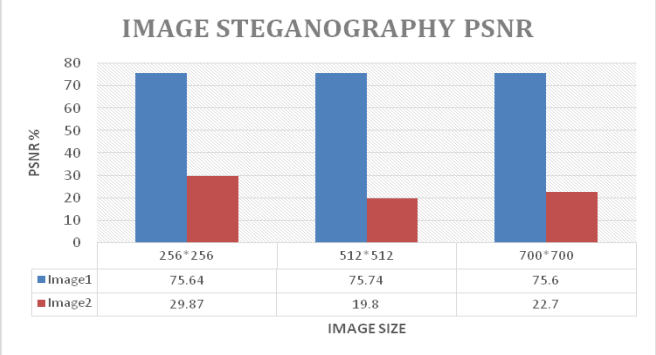

Figure 5: PSNR Steganography

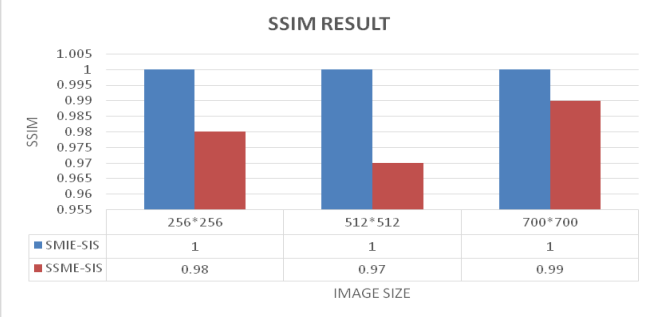

Figure 6: SSIM Results

VI. Conclusion and Future Scope

The secure and efficient secret image sharing scheme using sharing matrix, image encryption and steganography(SSME-SIS) is resilient to protect different types of images including binary, grayscale and color images. It has advantages such as a low computation cost, original image reconstruction, a low storage and transmission costs, etc. The security analysis including theoretical and experimental demonstration shows that the system has a high level of security to tolerate various attacks and a verification function to detect the fake shares. We are further going to implement multiuser image sharing by using hierarchical tree cryptography. The SSME-SIS uses steganography to combine two images ultimately increasing the security to one level along with allowing the user to share two images at a time.

Further the SSME-SIS can be developed to combine multiple images at a time in order to share them. Also various GUIs can be used to decrease the computation cost. The parallel processing can be used by implementing the technology such as openMP.

Acknowledgment

I hereby take this opportunity to thank Late G.N. Sapkal College of Engineering, Nasik for providing the opportunity to showcase my capabilities and skills. I would like to thank my guide, Prof. J. V. Shinde, for her guidance, support and valuable inputs. Also I would take this opportunity to express my heartfelt gratitude towards the people who helped me in presenting the paper directly or indirectly.

References

[1] L. Bao, S. Yi, Y.Zhou. “Combination of sharing matrix and image encryption for lossless (k; n)-secret image sharing.” IEEE transactionms on image processing, 2016

[2] Naor, Moni, and Adi Shamir. ”Visual cryptography.” Advances in CryptologyEUROCRYPT’94. Springer Berlin/Heidelberg, 1995.

[3] A. Shamir, “How to share a secret”, Communication of ACM, vol. 22, no. 11, pp. 612613, Nov. 1979.

[4] Yang, Ching-Nung. ”New visual secret sharing schemes using probabilistic method.” Pattern Recognition Letters 25.4 (2004): 481-494.

[5] Alex, Nitty Sarah, and L. Jani Anbarasi. ”Enhanced image secret sharing via error diffusion in halftone visual cryptography.” Electronics Computer Technology (ICECT), 2011 3rd International Conference on. Vol. 2. IEEE, 2011.

[6] Tso, Hao-Kuan. ”Secret Sharing Using Meaningful Images.” Journal of Advanced Management Science 1.1 (2013).

[7] Teng Guo, Feng Liu, ChuanKun Wu, ChingNung Yang, Wen Wang, and YaWei Ren. Threshold Secret Image Sharing. Information and communication security v 8233 Nov 2013

[8] Z. Wang, G. Arce, and G. Di Crescenzo, Halftone visual cryptography via error diffusion, IEEE Transactions on Information Forensics and Security, vol. 4, no. 3, pp. 383396, Sept 2009.

 DOI : 10.18231/2454-9150.2018.0448