International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161

Available at http://inpressco.com/category/ijcet

Research Article

A secure and lossless (k,n) secret image sharing using sharing matrix scheme

Shubham B. Bhokare and Prof. Archana S.Vaidya

Department of Computer Engineering G.E.S. R.H. Sapat College of Engineering, Nashik

Received 10 Nov 2020, Accepted 10 Dec 2020, Available online 01 Feb 2021, **Special Issue-8 (Feb 2021)**

Abstract

The majority of generated information includes images as they are widely used in the industrial process, businesses, military, scientific and researches. Information security has become a serious issue as a huge amount of information is exchanged via the internet. It needs to protect the confidential data in the image from unauthorized access or intruders. Advancement in hacking techniques has failed traditional image encryption approaches. Image encryption is applied to increase its security when used over the internet and to protect an image from unauthorized access. Nowadays the Internet is being used by everyone for sharing, transferring and storing huge amounts of data. The Internet has many drawbacks and there exist possibilities of hacking or being attacked by intruders. Hence we are introducing a algorithm - (k,n) Sharing Matrix Generation. The sharing matrix is reliable when images are being shared over the internet. The sharing matrix generation algorithm is then used with image hiding using Steganography and Image Encryption. Further, we are combining image encryption and sharing matrix that will allow the sharing of secret images in a secure and lossless manner.

Keywords: *Image Encryption, Secret Image Sharing, Sharing Matrix, Visual Cryptography.*

Introduction

The information generated from devices over rapidly growing internet needs to be secured. Most often cryptography is used to secure information. Original readable information is encrypted and converted into ciphertext and then decrypted to retrieve original information in a readable format. With rapid development in technology, intruders or hackers can find a way to access or modify confidential data. So this information, when shared over a network, must be protected by applying security techniques like cryptography. Cryptography provides Authentication, Confidentiality, and Integrity to the information when shared.

The secret is encryption into n shares in a method proposed by Naor at al. [1] in visual cryptography (VC) These n shares are then distributed to every participant in the system. Any participant in the system can have either one or more share(s). To retrieve this original secret image, all the participants must gather n shares in the (n,n) VC Technique. Different algorithms are used to hide the visual information in VC Encryption.The decryption process is done by the human visual system. Encryption inserts some noise data in the original image and during decryption noise data is either reduced or removed to regenerate that original image.

One of the alternatives to this is Secret Image Sharing Schemes (SISS) The SISS scheme converts a secret image into n shadows or shares which can be later shared. Then original secret image can be regenerated only from any k shares/shadows (k <n) and any (k-1) or less shadows/shares cannot reveal anything about the secret image. A secure and lossless secret image sharing scheme uses the combination of Image Encryption, Steganography and Sharing Matrix. In this scheme first, (k,n) sharing matrix is generated using a simple yet efficient algorithm. Then it is combined using a chaoticbased encryption process with a sharing encoding algorithm. This process can be applied on any values of k and n (k <n). It supports various formats of original images like grayscale, binary or color images. It generates different, unique shares with all new execution for the same input values. It also supports the verification of fake shares when included in the reconstruction phase. This feature is very necessary for real-world applications.

Literature Survey

Secret image sharing has attracted significant consideration in recent years. At first, Visual Cryptography methods were proposed by Naor et al. [1] The secret image in VC is encrypted into n shares/shadows. These n shares are allocated to each participant. They can have either one or more shares.

All the participants in the system have to combine n shares in (n, n) VC scheme to regenerate the original image. The Encryption process hides visual data and the decryption is performed by human vision. Encryption process inserts some noise data in the original image so as to hide the information and while decryption, the noise data is reduced or removed to regenerate original information. In VC,

- Every share is transparent, independent and noise-like.
- It supports only binary images.
- Attackers can identify and modify image shares as they are noisy in nature.
- Reconstructed image is always of low quality.
- Large transmission and storage costs is required.

Shamir et. al. [2] proposed Polynomial-based Secret Image
Sharing (PSIS). Lagrange interpolation was used to generate shares of the secret image and retrieve original with minimum number of shares. However,

- It requires a huge computations cost in the regeneration phase.
- Successful regeneration depends on number of shares and the sequence in which they appear and
- The results are in a different data range from one of original image.

Yang et al. [3] 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 the same as the conventional VSS schemes. They have also demonstrated that the conventional VSS scheme can be changed to a probabilistic VSS scheme by using the transfer function.

Alex et al. [4] used various methods for error diffusion to improve quality of the image in the halftone shares of the secret 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 secret information pixels into not coded halftone shares. The secret image is converted into a 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 qualified shares together. Cross-interference of shared secret images does not hamper anything.

Tso et al. [5] introduced a novel image sharing method to satisfy numerous problems such as

- Pixel Expansion problem.
- 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 to form a stack the quality of the reconstructed image is better and it has no distortion.

Teng Guo et al. [6] introduced (k,n) - TSISS - a (k,n) threshold based secret image sharing scheme. It breaks a secret image to be shared into n number of shares such as any k number of shares can be combined to regenerate the original secret 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. [7] 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.

Problem Definition

To design and develop a system which can address the limitations of previous methods such as Visual Secret Sharing (VSS), Polynomial Based Secret Image Sharing (PSIS), Visual Cryptography (VC) and provide a secure, efficient and lossless solution for sharing the secret images.

Proposed Methodology

A. Architecture

Fig 1 shows overall architecture of proposed scheme There are three major functional components in this system.

1) Encryption
2) Sharing Encoding
3) Image Reconstruction

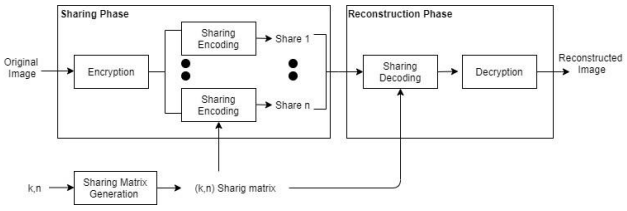

Fig. 1. Block Diagram of Proposed System

1) : Encryption The encryption is implemented as a process which transfers an original image into one-dimensional noiselike data sequence.

1) By using a chaotic map, random sequences are generated.
2) In the beginning, a random number generator is used to produce a security key.
3) 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.
4) Then the random sequences are applied to the substitution process which encrypts the data matrix into a onedimensional matrix.
5) This encrypted one-dimensional data matrix is at last combined with the security key and the final encrypted data sequence is obtained.

2) Sharing encoding: The system uses four major steps to generate sharing encoding. The first step is to produce the (k, n)-sharing the matrix as shown in fig 2. We repeat the process to generate the (k, n) sharing matrix in order to make the sharing matrix be of the same size as encrypted data as the reference for sharing encoding. The (k, n) sharing matrix consists of 0 or 1 values. Every single value from the encrypted data matrix is checked against its corresponding value from the sharing matrix from a 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, the encoded matrix is generated from the encrypted data matrix and sharing matrix. After generating the 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 Fig 2

Fig. 2. The generation of (k,n) sharing matrix

The steps involving generation of sharing matrix are explained as below

1) Generation of initial matrix.

In Generation of the initial matrix, a matrix M1 with the 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 concerning 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.

3) Image Reconstruction: To completely construct image again the original image from total n shares, the authorized users should receive

k_r,(k_r >= k)

image shares. The regeneration procedure of the original secret image is not related to the particular order of shares of the 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 the 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 an encrypted form by combining the last data of each received share by using the recovered sharing matrix as a reference. This encrypted matrix is divided into two parts, the key, and the data. At last original image is reconstructed using the encryption key applied to the data.

B. Algorithm

1) Image sharing Algorithm:

i) Transfer the original image to be shared into a onedimensional noise-like data sequence. ii) Produce security keys.

iii) Generate the final encrypted data sequence by combin-ing outputs of step-1 and step-2.
iv) Construct a matrix M1 of the size of (2k -2) x 1 suchthat it contains (k - 1) zeros and (k - 1) ones
v) Obtain all possible permutations of M1 viz. M2, M3, ...,Mn.
vi) Concatenate all the permuted matrices obtained in step5,together to generate the initial matrix S0 such as S0 =

[M1, M2.., MN] vii) According to the value of n, generate a new expansion matrix Se with a large size.

viii) Select n random rows of elements from expansion matrixSe to generate the final (k,n) sharing matrix.
ix) Perform point to point multiplication on matrices ob-tained in step3 and step8 to obtain the encrypted data sharing matrix R.

2) Reconstruction Algorithm:

i) Collect at least k shadow images.
ii) Generate a matrix Rm with the same size that of R.
iii) Generate a reconstructed matrix Rr by using a bit-levelBoolean function-or. iv) Extract the decryption key from the extracted encrypted image.

v) Recover the original image.

C. Mathematical Model

S is the system of secrete image sharing such that
S = I, M, O
I is the input to the system
M is the system modules
O is the system output
M: M1, M2, M3, M4, M5, M6, M7, M8
M1 = Encryption

M2 = Secrete sharing
M3 = Initial Matrix Generation M4 = Matrix Expansion
M5 = Row Extraction
M6 = Image Reconstruction
M7 = Sharing Decoding M8 = Image Decryption

Result and Discussions

Desktop based application is developed using Java Development Kit-1.8. For secure, lossless and efficient Secret Image Sharing using the sharing matrix. The System is tested on the Core i3 system with 4 GB RAM.

A. Implementation Status

Initial Matrix Generation, Matrix Expansion and Row Extraction have been implemented. These modules generate a (k,n) sharing matrix. The use of the referenced process is done to generate an encoded matrix from the encrypted data matrix and sharing matrix. The final encoded matrix is generated.

B. Performance Measures

1) Pixel Expansion: The ratio between share size and the original secret image size is the Pixel Expansion Ratio. This system reduces the data storage and transmission cost. We can say that the pixel expansion is lower.

2) Distortion Analysis: It is used to evaluate the variations between the reconstructed and original images. This method is used to evaluate the distortion of an image against VC and PSIS methods.

3) Computation Cost: The computation cost of this system is slightly larger. However, the computation cost in the reconstruction phase is significantly reduced when the value of k is small.

C. Result Analysis

An increase in the number of shares increases computation cost in the sharing and reconstruction phase. As shown in the fig below,

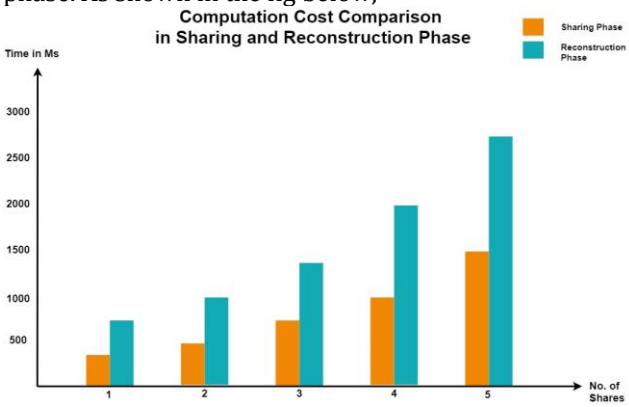

Fig. 3. Cost Comparison

Table I Performance Comparison

Schemes	Pixel Expansion	Data loss	Reconstruction Cost	Original Image
VC	Yes	Large	No	Binary
PSIS	Yes	Small	Large	All Types
Halftone	Yes	No	Small	Binary
SISSM	Negligible	No	Small	All Types

D. Comparison

Table below shows comparison of various Secret image sharing techniques

Conclusion

The secret image sharing scheme using sharing matrix can protect different types of images including binary, gray-scale and color images. It has advantages such as a low pixel expansion ratio to minimize the storage and transmission costs, lossless original image reconstruction, a low computation cost, etc. The security analysis including theoretical and experimental demonstration ensures that the system has a high level of security to tolerate the brute-force attack, differential attacks, and a verification function to detect fake shares.

Acknowledgment

I hereby take this opportunity to thank G.E.S. R.H. Sapat College of Engineering, Nashik for providing the opportunity to showcase my capabilities and skills. I would like to thank my H.O.D. Dr. D. V. Patil, for his 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]. Naor, Moni, and Adi Shamir. "Visual cryptography." Advances in CryptologyEUROCRYPT'94. Springer Berlin/Heidelberg, 1995.
[2]. . Shamir, How to share a secret, Communication of ACM, vol. 22, no. 11, pp. 612613, Nov. 1979.
[3]. Yang, Ching-Nung. "New visual secret sharing schemes using probabilistic method." Pattern Recognition Letters 25.4 (2004): 481-494.
[4]. 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
[5]. Tso, Hao-Kuan. "Secret Sharing Using Meaningful Images." Journal of Advanced Management Science 1.1 (2013).
[6]. 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
[7]. 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.
[8]. Longdan tan, yuliang lu, Weighted Secret Image Sharing for a(k,n)
[9]. Threshold Based on the Chinese Remainder Theorem. vol. 7, Sept 2019.
[10]. Dong Xie, Lixiang Li1, A Secure and Efficient Scalable Secret Image Sharing Scheme with Flexible Shadow Sizes January, 2017
[11]. Sagar Nitharwal, A Boolean-based multi-secret image sharing scheme using bit-reversal, Dec 2017