LOSSLESS SECRET IMAGE SHARING USING IMAGE ENCRYPTION AND SHARING MATRIX

Mrs.P.Induja1,G.Placeius Nishiga2,N.Poorvja3
MEPCO SCHLENK ENGINEERING COLLEGE, SIVAKASI

induja.r.s@gmail.com1,nishigadennis@gmail.com2,poojakumar2697@gmail.com3

Department of Electronics and Communication,
Sivakasi.

Abstract - This paper introduces combining sharing matrix with image encryption, a lossless \((l,m)\)-secret image sharing scheme. Here an idea is proposed to secretly share an image using sharing matrix algorithm. Initially, the original image is encrypted using substitution technique, where the image is converted into one dimensional noise like data sequence, for the subsequent sharing coding process. There are two sections in the proposed scheme. First section is sharing part and second one is reconstruction part. In the sharing part, the encrypted image is encoded using the sharing encoding method, where, \((l,m)\) sharing matrix is used to obtain the \(m\) shares of one dimensional encrypted image. Then, the 1D encrypted image of \(m\) shares, are converted into 2D. To completely reconstruct the original image, the authorized user should receive \(l\) image shares where \(l\) is greater than or equal to \(l\). In the reconstruction part, firstly the \((l,m)\) sharing matrix is recovered. The combination of all encrypted matrices undergoes decryption to recover the original image.

Index Terms - Secret image sharing, Image encryption, sharing matrix.

I.INTRODUCTION

In today’s computer generation, data security and hiding become important aspects for much organization. This paper the proposed method is used to generate the sharing matrix algorithm. Using the matrix the original image is encrypting into \(m\) different shares. Using \(l(l \leq m)\) or more shares can successfully reconstruct the original image. With less than \(l\) shares, any information of the original image cannot be accessed. Secret image sharing has brought attentions of many scientists. It can be roughly divided into two categories. Visual cryptography (VC) and polynomial-based secret image sharing (PSIS). VC method is proposed by Naor and Shamir [1]. VC is a popular technique also used in many research area of data hiding, securing images, color imaging, multimedia and other fields. Data hiding is a part of VC used in cybercrime, file format etc. [2]. In VC schemes random and meaningless shares are generated to protect and secretly share images. In this technique a secret image is encrypted into \(n\) different shares, where each participant holding one share; If any participant has less than \(l\) shares the original image cannot be retrieved. Only with the \(l\) shares the original image can be revealed. It can be directly recognized by the human visual system [3]. VC technique has certain drawbacks, they are (1) larger pixel expansion; (2) its image shares are at least two times larger than the original image; (3) it requires large transmission and storage cost [4].

Polynomial based secret image sharing (PSIS) is another hand which is proposed by Shamir. Its main idea is to generate the secret images into shares and reconstruct the original image with minimal number of shares and utilize the Lagrange interpolation [5]. However it also has some problems, they are (1) computation cost is high because of Lagrange interpolation; (2) reconstruction of original image is depends on the order and enough image shares [6]. The drawback of the existing methods VC and PSIS can overcome by this sharing matrix algorithm. In this paper developed lossless \((l,m)\)-secret image sharing using image encryption and sharing matrix algorithm. We first generate the \((l,m)\) sharing matrix, which is full of mathematical equation, functions and some important properties are needed for the sharing matrix. Here a chaotic based encryption process was proposed, and also using the sharing matrix with the encrypted matrix the encoded shares were generated. Its computation cost is much lower than the existing methods PSIS and VC. It has a low expansion ratio is used to reduce the cost of transmission and storage. The proposed secret image sharing method is used for various settings of \(l\) and \(m\) and various formats of original images such as binary, grayscale or color images. In reconstruction part has the verification function to identify the fake share, which is most suitable for real time application.
II. SHARING MATRIX GENERATION

In this section, \((l, m)\) sharing matrix was generated by using the mathematical definitions and properties. Here we discussed the mathematical analysis of generating sharing matrix and its advantages. The \((l, m)\) sharing matrix is generated by using three main steps: Generation of Initial matrix, Expansion of matrix, Extraction of rows. Generation of Initial matrix is to create an initial matrix \(\hat{k}_1\). Expansion of matrix is to expand the initial matrix \(\hat{k}_1\) into a new matrix \(k_e\). Extraction of rows is to randomly extracting \(m\) rows from the expanded matrix \(k_e\) and generate the final \((l, m)\) sharing matrix i.e. \(k^{(l, m)}\) sharing matrix.

A. Generation of Initial matrix:

In generation of initial matrix, we first construct a matrix \(N_i\) with size of \((2l-2)\times 1\). The matrix \(N_i\) has \((l-1)\) ones and \((l-1)\) zeros. For example, consider \(l = 3\) the matrix \(N_i = [1 \ 1 \ 0 \ 0]^T\). The possible permutations of \(N_i\) is denoting, \(N_i, i = 2, \ldots, M\) where \(M = \frac{(2l-2)!}{(l-1)! (l-1)!}\) is the total number of permutation of matrix \(N_i\). These matrices are combined together to generate the initial matrix \(\hat{k}_1\) with size of \((2l-2)\times M\) as shown in the Eq. (1)

\[
\hat{k}_1 = [N_1, N_2, \ldots, N_M]
\]

B. Expansion of matrix

The expanded matrix \(k_e\) is generated by using the initial matrix \(\hat{k}_1\) with large size according to the value of \(m\). The iteration value, \(T = \max\left\lceil \log_2\left(\frac{m}{(2l-2)}\right) \right\rceil\) where \(\left\lceil z \right\rceil\) is the ceiling function is used to obtain the least integer value is greater than or equal to \(z\). Note that the initial matrix is also a \((l, m)\) sharing matrix where \(m = 2l-2\). If \(m < 2l-2\), iteration value \(T=0\), no matrix expansion is needed and \(k_1 = k_e\). If \(m > 2l-2\), the matrix \(k_e\) is expand to generate the new matrix \(k_e\) using self-repeating. The self-repeating process is explained below. The matrix \(k_e, i = 1\) is equally divided into \(l-1\) sub matrices in the vertical direction for \(i^{th}\) iteration. Then in \(k_e, i = 1\) matrix, "1" of each column is replaced by \(j^m\) \((1 \leq j \leq l-1)\) matrix, "0" of each column is replaced by all ones with the same size of each sub matrix. By using this self-repeating process the initial matrix become expanded as \(k_e\) with size of \((2l-2)\times M_e\), where \(M_e = M^{T+1}\).

C. Extraction of rows:

Row extraction is to randomly selecting \(m\) rows from the expanded matrix \(k_e\) to generate the final \((l, m)\) sharing matrix \(k^{(l, m)}\) with size of \(m \times M_e\).

III. SECRET IMAGE SHARING SCHEME

In this process, first the original image is converted into noise-like random sequence with hiding keys into an image. The keys are used for the purpose of no information leakage. In the sharing part the original image become encrypted using substitution technique. Combining the sharing matrix and image encryption, \(m\) number of noise-like random sequences is generated. In reconstruction part, decryption keys are successfully retrieved to obtain the original image. The decryption process is combining all decoded matrix and sharing matrix to obtain the original image. The important property is, when the encoded shares \((l, m)\) are greater than or equal to \(l\), then only the original image can retrieved successfully.
The encryption process is to transfer a $B \times L$ original image into one dimensional noise-like data sequence for the subsequent encoding process. The Tent map using the Eq. (2) and (3) are generating a random chaotic sequence. Initially C number of random security keys are generated by, 
$$C = \{ c_1, c_2, \ldots, c_{192} \}$$
where $C \in [0, 1]$, $1 \leq y \leq 192$. Using C, two set of initial parameters $(a_1, P_1(1))$ and $(a_2, P_2(1))$ for the tent map generated using Eq.(2) and (3).

$$a_{s} = (\sum_{i=1}^{4} r_{i} \cdot 2^{4i} + r_{s}) \mod 0.4 + 3.6 \quad (2)$$

$$P_{s}(1) = (\sum_{i=1}^{4} r_{s} \cdot 2^{4i} + r_{i,2}) \mod 1 \quad (3)$$

For i=1, 2, 3, 4. The two random sequence $P_1$ and $P_2$ are generated by using Eq. (4).

$$P_{s}(y) = \begin{cases} 
    P_{s}(l) & \text{if } y = 1 \\
    \frac{1}{2} a_{s} P_{s}(y-1) & \text{if } y \neq 1 \text{ and } P_{s}(y-1) < 0.5 \\
    \frac{1}{2} a_{s} [1 - P_{s}(y-1)] & \text{if } y \neq 1 \text{ and } P_{s}(y-1) \geq 0.5 
\end{cases} \quad (4)$$

Where $y = 1, 2, \ldots, B \times L$. Using the two random sequence $P_1$ and $P_2$, the original image is transfer into 1D matrix $Z$. Applying these two values in Eq. (5) the substitution process encrypts matrix $Z$ into 1D matrix $S_{2}(j)$.

$$S_{2}(y) = \begin{cases} 
    S_{1}(y) & \text{if } y = B \times L \\
    \left[ \left( S_{1}(y) + [P_{s}(y) \times 10^{4}] + S_{1}(y) \mod 2^{25} \right) \right] \mod 2^{25} & \text{Otherwise} 
\end{cases} \quad (5)$$

Where $\left[ \right]$ is a floor function and mod is modulo operator.

$$S_{1}(j) = \left[ \left( z(y) + [P_{s}(y) \times 10^{4}] + z(y) \mod 2^{25} \right) \right] \mod 2^{25} \quad (6)$$

The encrypted data matrix $S_{2}$ with the security key $C_{s}$ are combined together to obtain the encrypted data sequence $S$. 

Fig.1. Proposed Method for lossless secret image sharing using $(l, m)$ sharing matrix
$S = (C_s, S_2)$ \hspace{1cm} (7)

Where $C_s = \{ C \oplus \big\| \sum S_2 \big\| \}$. An integer value into a binary sequence is obtained by using the symbol $\big\| \sum S_2 \big\|$ and $\oplus$ is the bitwise XOR operator. The summation value $\sum S_2$ of all pixels in $S_2$ is converted into 192 bits because the key $C$ contains 192 bits as well. The binary sequence is converted into 24 integers by using the function $\{ \}$, where each one is produced by 8 binary bits. The size of encrypted matrix $S$ is $1 \times (B \times L + 24)$.

### B. Encoding

In the encoding process, encoding matrix $W'$ will be generated by using some reference process. The reference process is done by sharing matrix. If the value is same as the position of sharing matrix, then it will be taken as a data sequence. But if its relating value in the sharing matrix is zero, the encrypted matrix will be removed. At the end of encoding, 1D encoded shares will be generated by using the encoding matrix $W'$. Each 1D share of $E'$ consists of three parts.

$E' = (U, V', W')$ \hspace{1cm} (8)

Where $U$ is a 1D matrix with size of $1 \times 2$. It can be calculated by utilizing and store the value of $M_s$.

$$U(1) = \left\lfloor \frac{M_s}{256} \right\rfloor$$ \hspace{1cm} (9)

$$U(2) = M_s \mod 256$$ \hspace{1cm} (10)

Where $V'$ is also a 1D matrix with size of $1 \times \left\lfloor \frac{M_s}{256} \right\rfloor$.

This matrix is used to convert the sharing matrix $k(i, :)$. into a series of 8-bit binary sequence and it can be stored using the Eq.(11)

$$V'(j) = \sum_{j = 8i}^{8i + 7} k(i, j) \times 2^{j-8i}$$ \hspace{1cm} (11)

Here $k(i, :) = (k(i, :], O_{1 \times v})$ and $O_{1 \times v}$ is a 1D zero matrix with size of $1 \times v$, where $v = f(M_s, s)$. The function is defined by Eq.(12).

$$f(x, y) = \begin{cases} 0 & \text{if } x \mod y = 0 \\ y - (x \mod y) & \text{otherwise} \end{cases}$$ \hspace{1cm} (12)

Now, $I_v$ number of 1D encoded share is generated. Each 1D encoded share is transform into 2D shares to obtain the original image.

### C. Decoding

The transformation is done by expanded the 1D encoded share into $F'$ using Eq. (13), and the size of reshape matrix $F'$ is $N \times \left\lfloor \frac{L}{n} \right\rfloor$ where the length of encoded share $E'$ is denoted as $I_1$.

$$F' = \begin{cases} E' & \text{if } (I_1 \mod N) = 0 \\ (E', O_{1 \times z}) & \text{otherwise} \end{cases}$$ \hspace{1cm} (13)

Here $O_{1 \times z}$ is a 1D zero matrix and $z = f(I_1, N)$.

### D. Decryption

Here the original image is decrypt by using the encrypted matrix $S$. The encrypted matrix is divided into two parts:

1. $C_s$ is the first 24 integer and,
2. $S_2$ is rest of data.

Using the Eq. (14) to retrieve the original key $C$ and use the Eq. (15)-(16) to generate two chaotic equations and transfer the 1D matrix $R$ to 2D, the original image $Q$ is reconstructed.

$$C = \| C_s \| \oplus \big\| \sum S_2 \big\|$$ \hspace{1cm} (14)

$$R(j) = \begin{cases} \frac{S_{j}(y)}{(S_{l}(y)+[P_{l}(y) \times 10^9]+S_{l}(y) \mod 256)} & \text{if } y = B \ast L \\ \text{Otherwise} \end{cases}$$ \hspace{1cm} (15)

$$S_{j}(y) = \begin{cases} \frac{S_{j}(y)}{(S_{l}(y)+[P_{l}(y) \times 10^9]+S_{l}(y) \mod 256)} & \text{if } y = 1 \\ \text{Otherwise} \end{cases}$$ \hspace{1cm} (16)
(a) \(\rightarrow\) (e) are different encoded shares are generated using (3, 5) sharing matrix. The original image \(Q\) is reconstructed only if the receiver has \(l \geq l\) shares, else the receiver receives a noise-like image. This proposed method is very effective method to prevent the information leakage.

IV. SIMULATION RESULTS

To demonstrate the lossless secret sharing, the simulation results of a gray scale image are shown below. It is done by using \((l, m)\) sharing matrix. The most important property is if the user has enough number of shares, then only the original image will be reconstructed and the image will retrieve without any data loss. Otherwise noise-like image will be displayed.

This demonstration is very useful to achieve the original image without any loss. If the user has less than \(l\) shares, the user cannot able to reconstruct the original image.

The original image with size of 256 x 256 is shown in fig (2). A shared matrix was generated by using sharing matrix algorithm, it is explained in section II. The generation of random keys is shown in fig (3).

Fig. 3. Generation of keys

Here we choose the value of \(l\) as 3 and \(m\) as 5, and generate the (3, 5) sharing matrix with three steps. First generate the initial sharing matrix using the Eq. (1). The figure (4) shows the initial sharing matrix.

Fig. 4. Initial sharing matrix

After generation of the initial sharing matrix, the matrix will be expanded, as discussed in section II-B. The figure (5) shows the expanded sharing matrix.
Finally the random numbers of rows are extracted from the expanded matrix to get a final sharing matrix, and it was discussed in section II-C. The figure (6) shows the final sharing matrix.

The encryption process is discussed in section III-A. The Eq. (7) shows the encrypted matrix, and it was generated by using the Eq. (5)-(6). The substitution technique is used here. The Eq. (2)-(3) are used to generate the two random sequences. It is used to generate the chaotic sequences shown in Eq. (4). From the Eq.(2)-(7) , the encrypted matrix was derived as the encoding process discussed in section III-B.

As discussed in the section III-C, the decoding process done. By using the Eq.13, the l shares are combined as a 2D matrix. First the original keys were reconstructed using Eq. (14)-(16). The figure-(10) shows the reconstruction of keys.

Also the U, V and W matrices were retrieved. The figure.(11)- (12) Shows the reconstruction of U, V and W matrices.

The original image is decrypted by combining of all shared matrices. If the receiver has l _r_ image shares, the original image can retrieved otherwise a noise like image will appear. The figure-(13) shows the noise like image, when the receiver has less than l number of shares.
V. CONCLUSION

The Lossless secret image sharing using image encryption and sharing matrix is the most effective technique for secretly sharing image with high security level. Here Chaotic based random sequence is generated during the encrypted process and the substitution technique is used for encryption. At the end of sharing part the 1D encoded share obtain. In reconstruction part, if the receiver has \( l \geq l \) shares, then only the original image should retrieve. The computation cost is low. It is used to detect the fakeshare.

VI. REFERENCES
