Transmission Risk Reduction using Diverse Media Digital Images Sharing

Anjali Maharudra Bhunje  
Department of Electronics and Communication Engineering  
VPCOE, Baramati, Maharashtra, India

Prof. Premanand K. Kadbe  
Department of Electronics and Communication Engineering  
VPCOE, Baramati, Maharashtra, India

Abstract - This paper gives idea about sharing the digital image without affecting its privacy. It proposes possible ways to hide the noise-like share and reduce transmission risk problem for sharing. To achieve this goal, Visual Secret Sharing scheme (VSS) is implemented to hide secret images that are either printed transparencies or are encoded and stored in digital form and shares are easy to detect by naked eyes/unauthorized user. Hence to avoid problems generated by VSS, (n, n)-NVSS (Natural Image based VSS) Scheme encryption/decryption algorithms to reduce the intercepted risk during the transmission phase is used. Regardless of the number of participants the value of n increases, the NVSS scheme uses only one noise share for sharing the secret image. It proposes a useful concept and method for using unaltered images as shares in a VSS scheme. A method to store the noise share as the QR code is used. The original motivation of NVSS scheme is to use printed images as sharing images and developing a method for storing the noise share.

Keywords – Visual secret sharing scheme, natural images, transmission risk, visual cryptography, shares.

I. INTRODUCTION

In day to day life information is increasingly important and gets more value when shared with others. Due to networking and communication media, it is used to share the important information like images, audio, video, pictures easily. Hackers tried to access unauthorized data. To solve this problem certain techniques are used. Today, in computer-aided environment sharing visual secrets images has becomes an important issue today. Secret images can be various types such as handwritten documents, photographs and others. Visual cryptography is a technique that encrypts a secret image into n shares with each participant holding one or more shares.

Visual Secret Sharing scheme (VSS) is implemented to hide secret images that are either printed transparencies or are encoded and stored in digital form [1]. Visual secret sharing is a technique used to deliver and transmit secret images. They satisfy the security requirement for protecting secret content, but they suffer from transmission risk problem because holding noise like shares will cause hacker’s suspicion and share may be intercepted. The shares can be defined as the noise-like pixels or display low quality images. VSS scheme use a unity carrier for sharing images.

To solve this problem, Natural image based Visual Secret Sharing (NVSS) is proposed. NVSS scheme uses diverse media for sharing digital images. The diverse media contains handwritten documents, photographs, digital images, printed images, painted pictures and so on. The NVSS scheme can share a digital secrete image over n-1 arbitrary natural images and one share. Instead of altering the content of natural images, the NVSS scheme extracts features from each natural share. These unaltered natural shares are greatly reducing the interception possibility of these shares. The noise-like share can be concealed by using data hiding techniques. It can also be increase security level during transmission phase. It proposes a useful concept and method for using unaltered images as shares in a VSS scheme.

In this paper, develop encryption/decryption algorithm for the (n,n)-NVSS scheme. The algorithms are applicable to digital and printed images. The NVSS scheme is user friendly. But also reduces transmission risk and enhances the security of participants and shares.
II. RELATED WORK

Naor and Shamir [1] proposed the concept of Visual cryptography (VC) which allows the encryption of secret information in the image form. Visual cryptography (VC) scheme is more secure and very easy to implement. By using the concept of secret sharing, a secret image was broken up into n share images. Each share printed on transparencies and then distributed to the n participants. Anyone who involved in the scheme for n-1 shares cannot revealed any information about the secret image. By stacking their n shares, the secret image can be revealed. It can be visually recognized by human visual system and cryptographic knowledge. The display quality of recovered images is poor.

Pei-Ling Chiu and Kai-Hui Lee proposed the A Simulated Annealing Algorithm for General Threshold Visual Cryptography Schemes in 2011. In this paper, the optimization techniques are used to solve the problem of constructing pixel-expansion-freed -VC schemes on binary secret images. The main objective of this model is to maximize the contrast of the recovered image. They are totally focused on blackness and security constraints. A simulated-annealing-based algorithm are used to solve this complicated and difficult optimization problem. Compared with Yang’s model, this model produces a 49.7% improvement in contrast for (3,10)-VCS. The contrast values of recovered images can be improved. The images become clearer. It can be easily recognized by the naked eye. Display quality can also be improved by adjusting the blackness level.

Kai-Hui Lee and Pei-Ling Chiu proposed the An Extended Visual Cryptography Algorithm for General Access Structures in 2012. In this paper pixel expansion problem can be solved using an Extended Visual Cryptography Algorithm for General Access Structures. Binary secret images are applicable in this model. Two phase encryption algorithm is used. In which first phase uses an optimization techniques to construct a pixel expansion free VCS for given access structure. In the second phase cover images are added on each share using stamping algorithm. The experimental result shows that, it has better performance in terms of display quality of the recovered images which includes contrast, maintenance of the same aspect ratio and perfect reconstruction of black secret pixels as that of the original image.

Zhi Zhou proposed Halftone Visual Cryptography in 2006. Halftone visual cryptography uses half toning technique in which shares are created. They used blue-noise dithering principles with void and cluster algorithm. In Halftone visual cryptography, a secret binary image is encoded into n different halftone shares. It maintains security and increases quality of the shares.

III. THE PROPOSED SCHEME

Naor and Shamir proved that the visual secret sharing scheme is very similar to the one-time pad encryption system. In a (2,2)-VSS scheme, the cipher text and secret random key can be denoted as two shares in the scheme. They are distributed to two participants who involve in the scheme. By applying the decryption operation, the two participants can decrypt the secret to the shares. They totally held by the participants [1].

In this paper, extract the secret key from a randomly chosen natural image in the (2,2)-NVSS scheme. In the (2,2)-NVSS scheme, the natural image and the generated share are distributed two participants. In the decryption process, the secret key can be extracted from the natural image. The secret key and generated share can recover the original image. The (n,n)-NVSS scheme assumes randomly n-1 natural shares and one generated share as media to share one digital true color secret image that has been 24-bit/pixel color depth. The main aim of this study is to reduce the transmission risk problem. In the NVSS scheme, natural shares can be of various types such as gray or color photographs of scenery, family activities, even flysheet, bookmarks, hand-painted pictures, web images or photographs. They are in digital or printed form. In the encryption process features are extracted from the natural shares. It cannot alter the natural shares. The natural shares can be delivered by participants who involved in the NVSS scheme. The natural shares are intercepted and it is not possible to verify that there is any hidden information in the image before reaching to the decryption process.

IV. IMPLEMENTATION

In this section the feature extraction module is described. Feature images are extracted from the natural shares. Simultaneously the printed and digital images are applicable to the feature extraction process. Then the image preparation and pixel-swapping modules are used.

A. Feature Extraction Module

Assume that size of natural share and secret images are w×h pixels. Before feature extraction start divide the natural share into a number of a × a pixel blocks.

- Block size is represented by a.
Natural shares denoted as N.
The shares and the secret image of the coordinates denoted by (x, y).
The left-top pixel of the coordinates defined by \((x_1, y_1)\).
The median is represented by M.
Feature matrix of N is F. The pixel value is black when the feature value is 0. The pixel value is white when the feature value is 1.

Feature extraction module consists of three processes such as binarization, stabilization and chaos process. The natural image are extracts first. The numbers of black and white pixels are balanced in second process. In this process, when \(h_{x,y} = 1\) is randomly selected and then set to 0. The process proved that the numbers of black and white pixels are equals. The total number unmatched black pixels calculated as:

\[
ps = \left( \frac{\sum_{x=1}^{a} h_{x,y} \cdot y \le y \le a} {a^2/2} \right) \quad (1)
\]

Some texture can be appears on the extracted feature images and the generated share. They can be used to eliminate by using chaos process. In each block randomly select \(p_c\) black and \(p_c\) white feature pixels and then the value of these pixels are alter. When \(h_{x,y} = 1\) the feature value of a pixel can be changed to 0 and When \(h_{x,y} = 0\) the feature value of a pixel can be changed to 1. \(p_c\) can be calculated as follows:

\[
p_c = a^2/2 \times P_n \quad (2)
\]

Where \(P_n\) be the probability to add noise.

\[B. \text{Algorithm: Feature Extraction}\]
Input N, a, Pn
Step 1: Divide N into blocks with a x a pixels
Step 2: Repeat steps 3-10 for each block
Step 3: Calculate median value of each block
Step 4: Calculate \(h_{x,y}\) as follows:
\[
h_{x,y} = 1, \quad f_{x,y} \ge M
\]
\[
0, \quad \text{Otherwise}
\]
Step 5: Calculate the number of unbalanced black pixels \(ps\)
Step 6: Randomly select \(ps\) pixels where \(h_{x,y} = 1\) and \(f_{x,y} = M\)
Step 7: Calculate \(p_c\) \(p_c = a^2/2 \times P_n\)
Step 8: When \(h_{x,y} = 1\) randomly select \(p_c\) candidate pixels
Step 9: When \(h_{x,y} = 0\) randomly select \(p_c\) candidate pixels
Step 10: Alter all values of \(h_{x,y}\) that were selected in step 8 and 9
Step 11: Output F.

\[V. \text{Experiment and Result}\]
We have implemented feature extraction algorithm on an image using MATLAB. First we have to take the original image figure (1) and then colour to grey scale image conversion figure (2).

The median value $M$ is 145.

$$
\begin{array}{cccc}
151 & 149 & 147 & 142 \\
150 & 148 & 144 & 139 \\
149 & 146 & 142 & 136 \\
147 & 143 & 138 & 133 \\
\end{array}
$$

Figure 3. 4 x 4 blocks of pixel values

$$
\begin{array}{cccc}
1 & 1 & 1 & 0 \\
1 & 1 & 0 & 0 \\
1 & 1 & 0 & 0 \\
1 & 0 & 0 & 0 \\
\end{array}
$$
If median value is less than the pixel value then the feature values at coordinates are set to 0. The feature values at other coordinates are set to 1.

The number of unbalanced black pixels $P_b = 0$. In each blocks the number of black and pixels are equal. The value of $P_c$ is 4. Then altered the coordinate with feature value 1 (0) to the 0 (1). In this way the clustering is reduced.

$$
\begin{array}{ccc}
0 & 1 & 1 & 0 \\
1 & 1 & 0 & 0 \\
0 & 0 & 1 & 1 \\
1 & 0 & 0 & 1 \\
\end{array}
$$

We have implemented feature extraction based algorithm in MATLAB. In feature extraction module, the feature images are extracted from the natural shares. The simulation result shows that in each block, the numbers of black and white pixels are equal.

REFERENCES