Digital Image Sharing Using DCT in Lossless Visual Cryptography Scheme

Chaithanya.A*

*M Tech Computer Science and Engineering, Lourdes Matha College of Science and Technology, Thiruvananthapuram, India

chaithanyaasok@gmail.com

Abstract — Conventional visual secret sharing (VSS) schemes hide secret images in shares that are either printed on transparencies or are encoded and stored in a digital form. The shares can appear as noise-like pixels or as meaningful images; but it will arouse suspicion and increase interception risk during transmission of the shares. Hence, VSS schemes suffer from a transmission risk problem for the secret itself and for the participants who are involved in the VSS scheme. To address this problem, a method called Digital Image Sharing using DCT is proposed. This method is introduced in lossless visual cryptography scheme. Here the image is converted into an intermediate form using DCT after that image will be divided into 2 shares. The discrete cosine transform (DCT) is the technique for converting an image into elementary frequency components. Share embedding is used to protect the shares for reducing the transmission risk problem. The recovered secret image will be always lossless and color image.

Index Terms — DCT, LVC, NVSS, VSS

I. INTRODUCTION

Security has gained a lot of importance as information technology is widely used. Cryptography refers to the study of mathematical techniques and related aspects of Information security like data confidentiality, data integrity, and of data authentication. Visual cryptography was originally invented and pioneered by Moni Naor and Adi Shamir in 1994 at the Eurocrypt conference. Visual cryptography is a new type of cryptographic scheme, which can decode concealed images without any cryptographic computation”. As the name suggests, visual cryptography is related to the human visual system.

Visual cryptography is regularly used for image encryption. Encryption starts with the use of secret sharing concepts where the secret image is split into shares which are noise-like and secure. These images are then transmitted or distributed over an entrusted communication channel. Recognition of a secret message from overlapping shares and the secret image is decrypted without additional computations or cryptography knowledge. Visual cryptography schemes are characterized by two parameters: the expansion corresponding to the number of sub pixels contained in each share and the contrast, which measures the “difference” between black and white pixels in the reconstructed image.

A secret is something which is kept from the knowledge of any but the initiated or privileged. Secret sharing defines a method by which a secret can be distributed between a group of participants, whereby each participant is allocated a piece of the secret. This piece of the secret is known as a share. The secret can only be reconstructed when a sufficient number of shares are combined together. While these shares are separate, no information about the secret can be accessed. That is, the shares are completely useless while they are separated. Within a secret sharing scheme, the secret is divided into a number of shares and distributed among n persons. When any k or more of these persons (where k ≤ n) bring their shares together, the secret can be recovered. However, if k - 1 persons attempt to reconstruct the secret, they will fail.

Image sharing is a subset of secret sharing because it acts as a special approach to the general secret sharing problem. The secrets in this case are concealed images. Each secret is treated as a number; this allows a specific encoding scheme supplied for each source of the secrets. Without the problem of inverse conversions, the digits may not be interpreted correctly to represent the true meaning of the secret.

Image sharing defines a scheme which is identical to that of general secret sharing. In (k, n) image sharing, the image that carries the secret is split up into n pieces (known as shares) and the decryption is totally unsuccessful unless at least k pieces are collected and superimposed.

When the k shares are stacked together, the human eyes do the decryption. This allows anyone to use the system without any knowledge of cryptography and without performing any computations whatsoever. This is another advantage of visual cryptography over the other popular conditionally secure cryptography schemes. The mechanism is very secure and very easily implemented. An electronic secret can be shared directly; alternatively the secrets can be printed out onto transparencies and superimposed, revealing the secret.

II. LITERATURE SURVEY

The objective of the literature review is to find and explore the benefits of digital image sharing techniques and also to find the shortcomings in existing methods and techniques. The main goal of this literature review is to find the gaps in existing research and techniques and to find possible solutions to overcome these holes.

[1] Visual Secret Sharing Schemes hide a Secret image in shares that appear noise-like picture or noiseless picture. VSS schemes suffer from a transmission risk problem while sharing shares contains Secret Images. To address this problem, we proposed a natural-image-based VSS scheme (NVSS scheme) that shares secret images via various carrier media to protect
the secret and the participants during the transmission phase. This Process involves sharing a secret image over arbitrary selected natural images (called natural shares) and one noise-like share. The natural shares can be photos or hand-painted pictures in digital form or in printed form. The noise-like share is generated based on these natural shares and the secret image. The unaltered natural shares are diverse, thus greatly reducing the transmission risk problem. We also propose possible ways to hide the noise like share to reduce the transmission risk problem for the share. Experimental results indicate that the proposed approach is an excellent solution for solving the transmission risk problem for the VSS schemes.

[2] Extended visual cryptography scheme consider n-number of natural image and one secret image. Extended visual cryptography scheme generate a noise like shares with every share associate a cover image and in that cover image hides a secret image. The algorithm which has been proposed in this method is easy to maintain for both sender and receiver because they know that in which cover image is hidden. It is easy for receiver also to combine cover image and extract secret image. In this paper they propose general approach to clarify the pixel expansion problems, this approach only for binary secret images. There are two phases in this proposed approach. First phase based on a given access structure, in this phase using an optimization technique they construct meaningless shares. In second phase using stamping algorithm they add cover image in each shares. The experimental result display that problem of pixel expansion is solved by extended visual cryptography scheme for general access structure. In this cover images are added with each share so it tampers the security.

[3] Visual cryptography scheme is a cryptographic technique which allows visual information to be encrypted into several shares in such a way that the decryption can be performed by the human visual system, without the aid of computers. Random grid is a methodology to construct visual secret sharing (VSS) scheme without pixel expansion in which an RG scheme takes an input image and transforms it into multiple cipher-grids that provide no information on the original image and the resulting decrypted image retains the size of the original image. Intent of this paper is on comparative study of visual cryptography and Random grid cryptography on the basis of analysis and correctness of simple VC schemes and RG schemes, improving contrast of the reconstructed image using various algorithms and multiple-image encryption using rotating angles.

[4] In the work of Ran-Zan Wang and Shuo-Fang Hsu, proposed a method for implementing visual cryptography (VC) in which an additional tag is attached to each generated share. The proposed tagged visual cryptography (TVC) scheme works like a traditional VC scheme does, where the original image is encoded in shares in such a way that the secret can be revealed by superimposing any or more shares, but knowledge of less than shares gets no secret information. A notable characteristic of TVC is that an extra tag can be revealed by folding up each share, which provides users with supplementary information such as augmented message or distinguishable patterns to identify the shares. The tagging property can easily be applied to any reported VC scheme to endow the generated shares with more capabilities. A common characteristic of both traditional VC and extended VC schemes is that a single share carries no useful information to users. In this letter, a method to endow VC schemes with the ability of displaying tag patterns by folding up a single share is proposed. The tagging property enriches new functions to the target shares. For example, it can display fake message to establish a cheating mechanism to unauthorized inspectors, or the tag pattern can exhibit unique symbol associated with each sharing instance, and provide a user-friendly environment for users to distinguish among and manage to the numerous shares. The proposed method is simple and can easily be applied to any reported VC schemes.

[5] The secret sharing schemes in conventional visual cryptography are capable of sharing one secret image into a set of random transparencies (called shares) in the form of rectangles, which reveal the secret image to the human visual system when they are superimposed. Recently, visual secret sharing schemes involving multiple secrets have attracted much attention. By adopting rotations on one of the two encoded circle shares, more than two secrets could be shared. Yet, the encoding and decoding processes of circle shares need more sophisticated mechanisms than those of rectangular or square ones. In this paper, we explore the possibilities of visual multiple secret sharing using simply two rectangular or square shares. Specifically, in this paper define some operations onto a transparency based upon turning over or flipping around. Then propose visual cryptographic schemes that are able to encode two or four secrets into two rectangular shares and up to eight secrets into two square shares such that the secrets cannot be obtained from any single share, whereas they are revealed by stacking the two shares under various combinations of turning or flipping operations.

The proposed schemes, which solidly elaborate the relationship between the encoded shares and the shared secrets, broaden the research scope and enrich the flexibility and applicability of visual cryptography or image encryption theoretically and practically. Design innovative schemes for encrypting two, four and eight secret images into two shares in this paper. The encrypted shares are in the form of rectangle (for two and four secrets) or square (for eight ones), which are more efficient and effective as compared to the circle or ring shares, since the former shares are simpler to encode, and easier to align and manipulate (via simply turning over and flipping around to reveal the next secret) than the latter ones which are difficult to specify the starting position and the rotational angles for alignment, or result in distortions when using circle shares. The decoding process is simply done by our visual perception so that no computing device is needed. The pixel expansion in this scheme is 2x where x = 2, 4 and 8, that is the same as that in (the best so far in the literature which adopted circle shares). The light transmissions of the two encrypted shares are 1/(2x) and 1/2, and the contrast of the reconstructed results is 1/(2x). Specifically, they could shuffle corresponding pixels in two images, randomly to obtain two shares with an equal light transmission. Even though at most eight secrets are considered (with regard to the simple turning over and flipping around operations), the number of the shared secrets and the reconstructed light contrast are quite appealing in practical. This scheme enriches the potential applications of image encryption or visual secret sharing to a greater extent.
Applications such as interleaving the true secrets with the forgeries, the considerations of order-sensitive secrets (say, how to protect/transmit the order), the authentication via some secrets to detect tempering, and so on truly deserve further investigation. The authors hope to generalize the ideas to encrypt arbitrary x secrets, 2 ≤ x ≤ 8, into two shares in the near future.

III. PROPOSED STRUCTURE

A lossless tagged visual cryptography scheme is one of the most efficient multi-secret visual cryptograph schemes. Lossless visual cryptography (LVC) is capable of reconstructing the image with good quality. The encoding processes of Digital image sharing using NVSS and other VC schemes bring distortion to shares, which definitely lowers the visual quality of the decoded secret image. To overcome this lower quality problem new method is proposed, an extended visual cryptography scheme, named as secure digital image sharing using DCT in lossless visual cryptography scheme. Specifically, lossless means that the proposed scheme encodes the image without affecting the rebuilt secret image, i.e., the decoded secret image of this scheme has the same visual quality with that of the conventional VC scheme. In this thesis work the lossless visual cryptography is applied in of intermediate DCT images.

Image Preprocessing: In this module first select image from different source, then the image will be categorized. The data will be image or text, the text data converted into image format and then processed. The width and height of image is checked and resize the image if the size of image exceeds the system required image size.

DCT calculation: In this module the image is broken into 8 x 8 blocks of pixels. Working from left to right ,top to bottom, DCT is applied to each block. A discrete cosine transform (DCT) expresses a finite sequence of data points in terms of a sum of cosine functions oscillating at different frequencies.

\[ D(i,j) = \frac{1}{\sqrt{2N}} C(i)C(j) \sum_{x=0}^{2} \sum_{y=0}^{2} p(x,y) \cos \left( \frac{(2x + 1)\pi i}{2N} \right) \cos \left( \frac{(2y + 1)\pi j}{2N} \right) \]

\[ C(u) = \begin{cases} \frac{1}{\sqrt{2}} & u = 0 \\ 1 & u > 0 \end{cases} \]

p(x,y) is the x,y th element of the transformed image from the pixel values of the original image matrix.

For the standard 8x8 block that JPEG compression uses, N equals 8 and x and y range from 0 to 7. Therefore D(i, j) would be as in given below.

\[ D(i,j) = \frac{1}{4} C(i)C(j) \sum_{x=0}^{2} \sum_{y=0}^{2} p(x,y) \cos \left( \frac{(2x + 1)\pi i}{16} \right) \cos \left( \frac{(2y + 1)\pi j}{16} \right) \]

Share Management: In this proposed scheme the secret image is divided into shares, the original image is divided into different shares such that each pixel in the original image is replaced with a non-overlapping block of two sub pixels. Anyone who holds only one share will not be able to reveal any information about the secret.

Kafri and Keren proposed an algorithm which takes an input image of size height x width. It then initializes two cipher-grid images R1 and R2 with the same dimensions as the input image. The algorithm randomizes the contents of R1, producing an image of random pixels. R2 is next generated based on the input image and R1. This process occurs by scanning each pixel of the input image. If a pixel at location [x, y] in the input image is found to be same as, the pixel at R1 [x, y] then pixel at R2[x,y] will also same. If, instead, the pixel at [x, y] in the input image is not same as R1, then the pixel R2 [x, y] is set to be the complement of R1 [x, y].

Share Encryption/Decryption: The most proposed approach for the image encryption/decryption is RC4 stream cipher. The reason, RC4 stream cipher is speedy encrypt image, less resources used, less time and implementation complexity. Basically RC4 algorithm is the two stages process, KSA (Key scheduling Algorithm) and PRGA (Pseudo Random Generator algorithm). In the first stages of RC4 Stream Cipher algorithm on the bases of variable sized key from 1 to 256 a State Vector (State Table) of fixed length 256 bytes is generated, after on the base of State Table, we generate the key stream that XOR with plaintext and cipher text during encryption and decryption. During encryption the key stream is XOR with the plaintext and during decryption the cipher text XOR with key stream then convert into the plaintext.
**Share Embedding:** The method used for share embedding is LSB, it is the lowest bit in a sequence of binary number. Say, if bits of binary number are 10101001, the least significant bit is far right. The LSB based embedding is used to insert the secret data into the least significant bits of the pixel values in a cover image.

**For Encryption:**
Step 1. Read the cover image in which the secret data to be hidden.
Step 2. Read the secret data and convert in binary form.
Step 3. Compute the LSB of each pixels of cover image.
Step 4. Replace least significant bit (LSB) of cover image with each bit of secret data/image one by one.
Step 5. Write stego image

**For Decryption:**
Step 1. Read the stego image.
Step 2. Compute LSB of each pixel from the stego image.
Step 3. Retrieve bits and convert each 8 bit into corresponding character

**Inverse DCT calculation:** In this module the reverse calculation of DCT is applied to reconstruct the secret image. Here the size of image is compared to be large than the orginal secret image but quality is very high. The equation used for calculating inverse DCT is given below.

\[ P(x,y) = \frac{1}{4} \sum_{i=0}^{7} \sum_{j=0}^{7} C(i,j)F[i,j] \cos \left( \frac{(2x + 1)i\pi}{16} \right) \cos \left( \frac{(2y + 1)j\pi}{16} \right) \]

\[ C(u) = \begin{cases} \frac{1}{\sqrt{2}} & \text{if } u = 0 \\ 1 & \text{if } u > 0 \end{cases} \]

**IV. COMPARATIVE ANALYSIS**

The proposed lossless visual cryptography scheme reconstructed image has high image quality (same as original secret image). However, other cryptography systems in general produce images that are susceptible to distortion and degradation of quality. Therefore, substantial lossless method is achieved at the expense of quality. On the other hand, in order to evaluate and compare the performance of different visual cryptography methods, it is necessary to judge the visual quality of the decrypted images, for that PSNR values are calculated for measuring the quality of image.

**Lossless method PSNR Calculation**

<table>
<thead>
<tr>
<th>Secret image</th>
<th>Secret image size</th>
<th>Obtained image size</th>
<th>PSNR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flowers.jpg</td>
<td>59778 bytes</td>
<td>59778 bytes</td>
<td>INF</td>
</tr>
<tr>
<td>Tree.jpg</td>
<td>58127 bytes</td>
<td>58127 bytes</td>
<td>INF</td>
</tr>
<tr>
<td>Birds.jpg</td>
<td>62654 bytes</td>
<td>62654 bytes</td>
<td>INF</td>
</tr>
<tr>
<td>Vegetables.jpg</td>
<td>57164 bytes</td>
<td>57164 bytes</td>
<td>INF</td>
</tr>
</tbody>
</table>

Table 1: PSNR calculation of lossless VC method

**Digital image sharing using NVSS method**

<table>
<thead>
<tr>
<th>Secret image</th>
<th>Secret image size</th>
<th>Obtained image size</th>
<th>PSNR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flowers.jpg</td>
<td>59778 bytes</td>
<td>3045 bytes</td>
<td>15db</td>
</tr>
<tr>
<td>Tree.jpg</td>
<td>58127 bytes</td>
<td>1884 bytes</td>
<td>12db</td>
</tr>
<tr>
<td>Birds.jpg</td>
<td>62654 bytes</td>
<td>4172 bytes</td>
<td>17db</td>
</tr>
<tr>
<td>Vegetables.jpg</td>
<td>57164 bytes</td>
<td>4527 bytes</td>
<td>18db</td>
</tr>
</tbody>
</table>

Table 2: PSNR calculation of digital image sharing using NVSS method

**Graph 1:** Comparison based on quality of proposed method and previous method

The graph shows the comparison between the quality of output images of both the proposed method and the previous method. From the graph we can see that the PSNR values are above 30db for the Lossless VC method which means that there is no loss of data but in previous method all the values are below 30 db so it was lossy. So the quality of images in Lossless VC is more.

**V. CONCLUSION**

Security has gained a lot of importance as information technology is widely used. Visual cryptography (VC) is a process where a secret image is encrypted into shares which refuse to divulge information about the original secret image.
The secret image can be recovered simply by stacking the shares together. In conventional VC at the decoding time the quality of original image will be reduced. The proposed work reduces the transmission risk problem and also the quality of image is retained.

The proposed work has been divided into six modules. The carrier image and secret image is selected and preprocessing. Resized secret image converted into intermediate image using DCT. The DCT image will be divided into shares. The share will be embedded to the carrier image using LSB. The embedded image is send to the receiver end. Secret image and carrier image extracted from the embedded image.

REFERENCES