An Effective Approach for Enhancing Quality of Retrieved Secret Images

V.Annie Daisy¹, R.Saranya², V.Annie Jaisy³

¹, ², ³Computer Science and Engineering, Jeppiaar Engineering College, Chennai, Kanceepuram, India

Abstract
To implement a Visual Secret Sharing Scheme (VSSS) which encrypts multiple secret images into the same quantity of share images to increase the encryption capacity compared with the original VSSS. Error Diffusion Algorithm is used to enhance the contrast and quality of the decrypted or stacked image. It is achieved by using the Jarvis Error Filter.

Keywords: Visual Cryptography, Visual Secret Sharing Scheme, Error Diffusion, (2,2)scheme, Jarvis Error Filter.

1. Introduction
Even with the remarkable advance of computer technology, using a computer to decrypt secrets is infeasible in some situations. For example, consider the following problem: a security guard checks the badge of an employee or a secret agent recovers an urgent secret at some place where no electronic devices are available. In these situations the human visual system is one of the most convenient and reliable tools to do checking and secret recovery. From these it is known that in some cases we need a secret sharing scheme which does not need computer for decryption process.

Visual Cryptography (VC) is a method of devising a secret sharing scheme in which a secret image is encrypted into shares such that stacking a sufficient number of shares reveals the secret image. Here the secret is decoded directly by the human visual system. Shares are usually presented in transparencies. Each participant holds a transparency (share). Unlike conventional cryptographic methods, VC needs no complicated computation for recovering the secret. The act of decryption is to stack the shares and view the image that appears on the stacked shares simply. A visual secret sharing scheme is a type of secret sharing scheme with the special property that a secret image can be recovered visually by the human eye and does not require any calculations on a computer.

2. Proposed System
A 2 out of 2 visual secret sharing scheme is implemented which encrypts two secret images and these secret images are constructed as 2 shares such that the secret image can be retrieved only by using both the shares.

The visual secret sharing scheme for multiple secrets is intended to encrypt more than one secret image into the same quantity of share images to increase the encryption capacity compared with the original visual secret sharing scheme.

Shares are created using the concept of pixel expansion in visual cryptography. Pixel expansion is the number of subpixels that each pixel of the secret image is encoded into in each share.

Sub pixels obtained by pixel expansion are encoded in halftoned images taking meaningful visual information. A halftone image is made up of a series of dots rather than a continuous tone.

Error Diffusion is used to produce the halftoned image. Error diffusion is a type of halftoning in which the quantization residual is distributed to neighboring pixels that have not yet been processed. Jarvis Error Filter is used for error diffusion to diffuse quantization error over neighbouring continuous tone pixels. Visually pleasing halftoned image can be obtained. Reconstruction of the secret image is done by performing OR operation with the halftone shares for retrieving first secret and rotate the second share and stack inorder to retrieve the second secret image.

© Copyright reserved by IJETR
2.1 Visual Cryptography Using Error Diffusion

Visual Cryptography is an encryption technique where a secret image is cryptographically encoded into \( n \) meaningless share images. In visual secret sharing scheme \((k,n)\) the secret images can be visually revealed by stacking together any \( k \) or more transparencies of the shares and by inspecting less than \( k \) shares, one cannot retrieve the secret image.

There are totally four modules used in our project which is listed below. Each module has specific usage in the project and its description is given below followed by the list of modules.

2.1.1 Halftoning Grayscale Image

Halftoning process converts a continuous-tone image into a binary valued image. Error diffusion algorithm is used for half toning process. It uses the Jarvis Error Filter.

The scanned image is initially converted into grey-scale image. Then the image is thresholded. The threshold value is chosen automatically. Every image say, \( p(a, b) \) is composed of light and background pixels have intensity levels grouped into two dominant modes. One obvious way to extract the objects from the background is to select a threshold \( T \) that separates these modes. Then any point \((a, b)\) for which \( p(a, b) \geq T \) is called an object point; otherwise the point is called a background point. In other words, the threshold image \( t(a,b) \) is defined as:

\[
t(a,b) = \begin{cases} 
1 & \text{if } p(a,b) \geq T \\
0 & \text{if } p(a,b) < T 
\end{cases}
\]

2.1.2 Random Share Creation

The halftoned image consists of only binary values (0 or 1). Therefore the share generation of the secret image is easy and the retrieved image will not suffer from the change in values of the pixel. Therefore the share is generated for the two secret images.

A binary image pixel is divided into two sub-pixels out of which black or white is randomly chosen depending on the current pixel. If the image pixel is white, then choose one of the two rows for white (0 1 0 1 or 1 0 1 0), else if it is black, then choose between one of the two rows for black (0 1 1 0 or 1 0 0 1).

2.1.3 Embedding

The Host image in which the Secret shares are to be embedded are halftoned and complemented, therefore the shares are embedded into it and can be stacked without extracting the shares.

Secret pixels are encoded to the predetermined position in half toned image and complemented half toned image. Pixels from share 1 is distributed to half toned image and pixels from share 2 are distributed to complemented half toned image.

In this way the share generated for second secret image is also embedded in the halftoned image and complemented halftoned image.

2.1.4 Stacking

Reconstruction of the secret image is done by performing OR operation with the halftone shares. To retrieve the first secret OR operation is performed with halftone share. To retrieve the second secret the second embedded share is rotated and then OR operation is performed.

3. Tables, Figures and Equations

3.1 Architecture

![Architecture of proposed system](fig3.1)

- Halftoning
- Share Generation
- Embedding
- Stacking
The architecture of the proposed system is shown above and the process of the proposed system are explained in the modules section.

The activities that are carried in this process are illustrated using the diagram shown below.

3.2 (n,n) Scheme

(n,n)-Scheme: This scheme encrypts the secret image into n shares and obtains the secret image when all n of the shares are overlaid, but any n -1 of them will not produce any hint about the secret image. The user has to give the value of n, the number of participants. Here we use the (2,2) scheme where the 2 shares are generated for the secret image and overlaying that 2 shares the secret image is revealed.

3.2 Jarvis Error Filter

The Jarvis Error Filter is used for the Error Diffusion process where the errors that occur during the threshold process are distributed to the neighboring pixels. The errors are distributed to the 12 neighboring pixel as shown in the figure given below.
4. Conclusions

Visual cryptography is used along with the concept of halftoning where the continuous-tone image is first transformed into a binary image by using error diffusion and hence error filters, and then the visual secret sharing is applied. Error diffusion has low complexity and provides halftone shares with good image quality. The recovered secret image is not so clear but the shares are of better quality means better secret hiding and hence the quality of the secret image can be traded off for better secrecy. A reconstructed secret image, obtained by stacking qualified shares together, does not suffer from cross interference of share images.

References


[6] JIM CAI “A SHORT SURVEY ON VISUAL CRYPTOGRAPHY SCHEMES”


