Extending the Visual Cryptography Algorithm Without Removing Cover Images

Dr.V.R.Anitha, M.Tech, Ph.d [1], Dilip kumar Kotthapalli [2]

[1] Professor of ECE, Department of Electronics and Communication Engineering, Sree Vidyanikethan Engineering College, TIRUPATI – 517 102, A. P., INDIA

[2] M.Tech student, Department of Electronics and Communication Engineering, Sree Vidyanikethan Engineering College, TIRUPATI – 517 102, A. P., INDIA

Abstract: Visual cryptography is a simple and powerful method which can provide high security for confidential information. This technique generate noise-like random pixels on share images to hide secret information which on overlay decrypt the information this technique is known as conventional visual secret sharing schemes. It suffers a management problem, because of which dealers cannot visually identify each share. This problem is solved by the extended visual cryptography scheme (EVCS), which adds a meaningful cover image in each share. But while removing the extra cover image it produces extra noise or degrades the hidden image quality. Hence we are Extending the visual cryptography algorithm without removing cover images where it reduces pixel expansion problem and shares match duration.

Keywords - Extended visual cryptography (EVC), pixel expansion problem, shares synchronization, general access structure

I. INTRODUCTION

We need very efficient security systems for preventing confidential information from being accessed by unauthorized persons. As computing power becoming more and more faster our older cryptographic systems becoming less secure because an attacker can attempt large number of random attack attempts in shorter time. Visual cryptography is a secret information sharing technique which shares the information in the form of images. Concept of visual cryptography is introduced by Moni Naor and Adi Shamir in 1994.

In this method each message is considered as an image of black and white pixels. This image is divided into n slides called transparency. Each pixel of the message appears in each transparency in a different modified version. For getting the original information from transparencies, all of them are stacked together with proper alignment. The simplest example of visual cryptography is a scheme in which we split the image into two different shares. The decryption of the image will be done by overlapping the shares. When we place both the shares one over another with proper alignment, we can interpret the original image.

Here occurs some management problems which not only affects the practicability of storage/transmission requirements for shares but also tends to pixel expansion problem. To the best of our knowledge, the existing Extended Visual Cryptography Schemes (EVCS) algorithms for GASs cannot avoid the pixel expansion problem. Therefore, we are motivated to find a solution to this problem.

Visual Cryptography (VC) aims to share a secret message between several shadow images (SI, sometimes named transparencies) in accordance with the initial scheme. That algorithm is known to be very effective because no information about the message transmitted what-so-ever leaks into any of the SI's. This differs from the technique known as watermarking.

In VC, all required SI's need to be present, and need to be overlaid for the message to appear. In a VC scheme, each SI is a random distribution of black-and-white subpixels. All subpixels are independent from each other and therefore one SI alone leaks strictly no information. To reveal the message a minimal number of SI's must be stacked together and duly registered

II. SYSTEM ASSUMPTIONS

Conventional VSS schemes generate noise-like random pixels on shares to hide secret images. In this manner, the secret can be perfectly concealed on the share images. However, these schemes suffer from a management problem dealers cannot identify each share visually. Hence, researchers have developed the extended visual cryptography scheme, which adds a cover image to share images.

The first phase of the algorithm, which uses optimization techniques for a given access structure,

constructs a set of noise-like shares that are pixel expansion free. The second phase of the algorithm directly adds a cover image on each share via a stamping algorithm. In this manner, the pixel expansion can be removed entirely. In visual cryptography, the message is encoded into a binary pattern. In each Share image, each message pixel is represented by a fixed-size binary pattern, named a share, which therefore consists of subpixels. In each share, two of the four subpixels, selected randomly, are black. The pixel expansion problem is a common disadvantage with most of the VSS schemes.

III. MODULES

The proposed work is divided into four modules as:

1. Gray Scale Conversion, 2. Image Encryption,
3.Adding cover images, 4. Image Decryption.

1. Grayscale Conversion

In photography and computing, a grayscale digital image is an image in which the value of each pixel is a single sample, that is, it carries only intensity information. Images of this sort, also known as black-and-white, are composed exclusively of shades of gray, varying from black at the weakest intensity to white at the strongest.

Conversion of a color image to grayscale is not unique; a common strategy is to match the luminance of the grayscale image to the luminance of the color image. In fact a gray color is one in which the red, green and blue components all have equal intensity in RGB space. The grayscale intensity is stored as an 8-bit integer giving 256 possible different shades of gray from black to white. Gray-level conversion is the process which converts the given original image to a 256 bits gray-level bitmap image.

Steps of grayscale algorithm:

Step 1: Get dimension of the uploaded image
Step 2: Declare to variable X and Y representing x axis and y axis.
Step 3: Set initial position of X and Y to '0'
Step 4: increment the value of x and y by '1'
Step 5: get the pixel value of x and y
Step 6: check to which the pixel value is near-by to white or black
Step 7: change the value to black if it is near to black
Step 8: else change the value to the white if it is near to white
Step 9: repeat till all the pixels are converted.

2. Image Encryption

In cryptography, encryption is the process of encoding messages (or information) in such a way that hackers cannot read it, but that authorized parties can view that message. In an encryption scheme, the message or information is encrypted using an encryption algorithm, turning it to an unreadable cipher-text. This image is divided into n slides called transparency. Each pixel of the message appears in each transparency in a different modified version. For getting the original information from transparencies, all of them are stacked together with proper alignment.

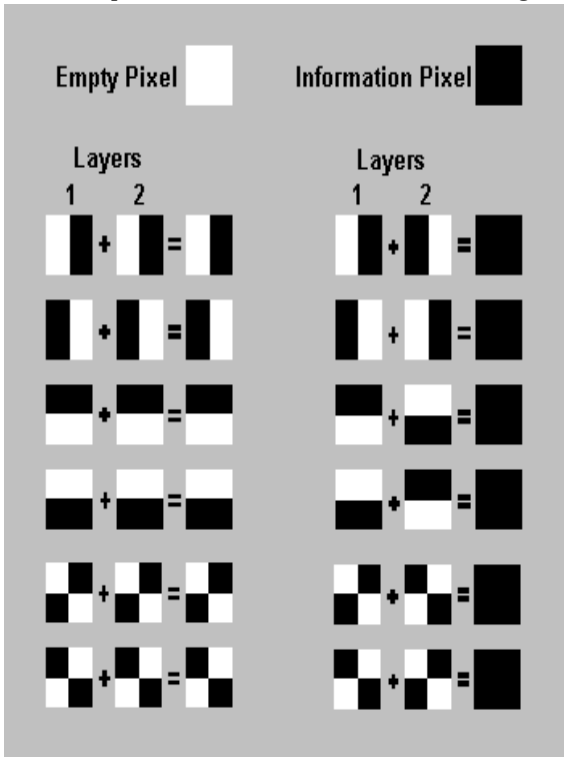


Fig1 : shares synchronization

Steps of encryption algorithm:

Step 1: Get width and height of the image
Step2: Horizontal block=image width/2
Step3: Vertical block =image height/2
Step 4: Number of block = horizontal block X vertical block
Step 5: For n=0 to no.of.block-1
For x=0 to n-1
For y=0 to n-1
Encrypt pixel using position (x, y)

3. Adding cover images

Conventional VSS schemes generate noise-like random pixels on shares to hide secret images. In this manner, the secret can be perfectly concealed on the share images. However, these schemes suffer from a management problem dealers cannot identify each share visually and also it suffers pixel expansion problems. Hence, researchers have developed the extended visual cryptography scheme, which adds a cover image to share images which reduces pixel expansion problem and also reduces shares matching duration.

4. Image Decryption

The decryption of the image will be done by overlapping the shares, without removing cover images, by means of that we can avoid pixel expansion problems. Where removing cover images results in change in the display quality of the recovered image. When we place both the shares one over another with proper alignment, we can interpret the original image.

IV. IMPLEMENTATION ISSUES

Each pixel of the images is divided into smaller blocks. There are always the same number white (transparent) and black blocks. If the pixel is divided into four equal parts, there are two white and two black blocks. The example images from above uses pixels that are divided into four parts.

In the table on the right we can see that a pixel, divided into four parts, can have six different states. If a pixel on layer 1 has a given state, the pixel on layer 2 may have one of two states: identical or inverted to the pixel of layer 1. If the pixel of layer 2 is identical to layer 1, the overlayed pixel will be half black and half white. Such overlayed pixel is called grey or empty. If the pixels of layer 1 and 2 are inverted or opposite, the overlayed version will be completely black. This is an information pixel.

We can now create the two layers. One transparent image, layer 1, has pixels which all have a random state, one of the six possible states. Layer 2 is identical to layer 1, except for the pixels that should be black (contain information) when overlayed. These pixels have a state that is opposite to the same pixel in layer 1. If both images are overlayed, the areas with identical states will look gray, and the areas with opposite states will be black.

If Visual Cryptography is used for secure communications, the sender will distribute one or more random layers 1 in advance to the receiver. If the sender has a message, he creates a layer 2 for a particular distributed layer 1 and sends it to the receiver. The receiver aligns the two layers and the secret information is revealed, this without the need for an encryption device, a computer or performing calculations by hand. The system is unbreakable, as long as both layers don't fall in the wrong hands. When one of both layers is intercepted it's impossible to retrieve the encrypted information.

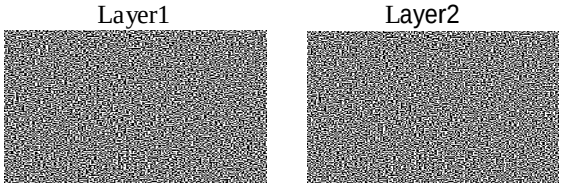
V. EXPERIMENTAL RESULTS

In this section, we first evaluate the performance of the proposed optimization model by comparing with the previous VC results for GASs. Then, we assess the performance of the proposed encryption algorithm for EVCS in terms of the pixel expansion problems and shares synchronization time. Finally, we demonstrate the results of our implementation of EVCS by examples.

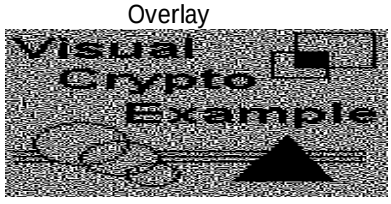
Visual Cryptography is a special encryption technique to hide information in images in such a way that it can be decrypted by the human vision if the correct key image is used. Visual Cryptography uses two transparent images. One image contains random pixels and the other image contains the secret information. It is impossible to retrieve the secret information from one of the images. Both transparent images or layers are required to reveal the information. The easiest way to implement Visual Cryptography is to print the two layers onto a transparent sheet.

When the random image contains truely random pixels it can be seen as a one-time pad system and will offer unbreakable encryption. In the overlay animation you can observe the two layers sliding over each other until they are correctly aligned and the hidden information appears.

Layer1 Layer2



Overlay



VI. CONCLUSION

The major contributions of our work is the first solution that addresses the pixel expansion problem of the EVCS for general access structures. So we add cover images to solve pixel expansion problems. Where removing cover images results in repeating the pixel expansion problems and also extends the shares synchronization time. So we are extending visual cryptography without removing cover images. where it reduces pixel expansion problem and shares match duration.

REFERENCES

[1] M. Naor and A.Shamir, "Visual cryptography," in Proc. Advances in Cryptology (Eurprocrypt'94), 1994, pp. 1–12.

[2] E.R.Verheul and H. C. A. v.Tilborg, "Constructions and properties of k-out-of-n visual secret sharing schemes," Designs Codes Crypto., vol. 11, pp. 179–196, 1997.

[3] H. Koga, "A general formula of the (t,n)-threshold visual secret sharing scheme," in Proc. Advances in Cryptology (Asiacrypt), 2002, pp. 328–345.

[4] Gamil R.S. Qaid and Sanjay N. Talbar,''Encryption and Decryption of Digital Image Using Color signal" IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 2, No 2, March 2012

[5] C. Blundo, S. Cimato, and A. D. Santis, "Visual cryptography schemes with optimal pixel expansion," *Theor. Comput. Sci.*, vol. 369, pp.169–182, 2006.

[6] D. Wang, L. Zhang, N. Ma, and X. Li, "Two secret sharing schemes based on boolean operations," *Pattern Recognit.*, vol. 40, pp. 2776–2785, 2007.

[7] G. Ateniese, C. Blundo, A. D. Santis, and D. R. Stinson, "Visual cryptography for general access structures," *Inform. Comput.*, vol. 129, pp. 86–106, 1996.

[8] C. S. Hsu, S. F. Tu, and Y. C. Hou, "An optimization model for visual cryptography schemes with unexpanded shares," *Found. Intelligent Syst., LNAI*, vol. 4203, pp. 58–67, 2006.

[9] G. Ateniese, C. Blundo, A. D. Santis, and D. R. Stinson, "Extended capabilities for visual cryptography," *Theor. Comput. Sci.*, vol. 250, pp. 143–161, 2001.