An Extended Approach on Visual Cryptography Based on Various Schemes

M. Ramadhevi[1]
M.E. (Final Year - CSE)
Annapoorna Engineering College
Salem, TamilNadu, India

K. Thangadurai[2]
Asst.Professor (CSE)
Annapoorna Engineering College
Salem, TamilNadu, India

***Abstract*— A visual cryptography scheme (VCS) is a kind of secret sharing scheme which allows the encoding of a secret image into shares distributed to participants. The beauty of such a scheme is that a set of qualified participants is able to recover the secret image without any cryptographic knowledge and computation devices. An extended visual cryptography scheme (EVCS) is a kind of VCS which consists of meaningful shares (compared to the random shares of traditional VCS). In this paper, we propose a construction of EVCS which is realized by embedding random shares into meaningful covering shares, and we call it the embedded EVCS. Experimental results compare some of the well-known EVCSs proposed in recent years systematically, and show that the proposed embedded EVCS has competitive visual quality compared with many of the well-known EVCSs in the literature. In addition, it has many specific advantages against these well-known EVCSs, respectively.**

Keywords*— Embedded extended visual cryptography scheme (embedded EVCS), secret sharing.

I. INTRODUCTION

Visual cryptography technology [1], the end user identifies an image, which is going to act as the carrier of data. The data file is also selected and then to achieve greater speed of transmission the data file and image file are compressed and sent. Prior to this the data is embedded into the image and then sent. The image if hacked or interpreted by a third party user will open up in any image previewed but not displaying the data. This protects the data from being invisible and hence is secure during transmission. The user in the receiving end uses another piece of code to retrieve the data from the image. The scope of the System provides a friendly environment to deal with images. Generally tools supports only one kind of image formats. This application supports .gif and .png (portable network graphics) formatted images and the application has been developed using swing and applet technologies, hence provides a friendly environment to users.

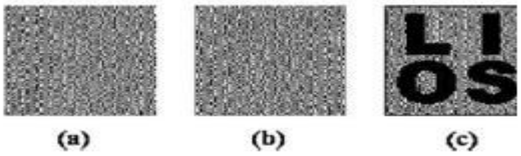


Fig.1. Example of traditional (2,2) VCS with image size 128 X 128.

II. TECHNIQUES USED IN EXTENDED VISUAL CRYPTOGRAPHY

A. Halftoning technique

Visual cryptography [2] encodes a secret binary image (SI) into shares of random binary patterns. If the shares are xeroxed onto transparencies, the secret image can be visually decoded by superimposing a qualified subset of transparencies, but no secret information can be obtained from the superposition of a forbidden subset. The binary patterns of the shares, however, have no visual meaning and hinder the objectives of visual cryptography. Extended visual cryptography was proposed recently to construct meaningful binary images as shares using hypergraph colourings, but the visual quality is poor. In this paper, a novel technique named halftone visual cryptography is proposed to achieve visual cryptography via halftoning. Based on the blue-noise dithering principles, the proposed method utilizes the void and cluster algorithm to encode a secret binary image into halftone shares (images) carrying significant visual information. The simulation shows that the visual qualities of the obtained halftone shares are observably better than that attained by any available visual cryptography method known to date

B. Secret Sharing Scheme

Visual Cryptography [2] is based on cryptography where *n* images are encoded in a way that only the human visual system can decrypt the hidden message without any cryptographic computations when all shares are stacked together. This paper presents an improved algorithm based on Chang’s and Yu visual cryptography scheme for hiding a colored image into multiple colored cover images. This scheme achieves lossless recovery and reduces the noise in the cover images without adding any computational complexity.

The Visual cryptography scheme is a cryptographic technique which allows visual information (e.g. printed text, handwritten notes, and picture) to be encrypted in such a way that the decryption can be performed by the human visual system, without the aid of computers. There are various measures on which performance of visual cryptography scheme depends, such as pixel expansion, contrast, security, accuracy, computational complexity, share generated is meaningful or meaningless, type of secret images (either binary or colour) and number of secret images (either single or multiple) encrypted by the scheme. The study of VCS is on the performance.

III. RELATED WORK

The associated secret sharing problem and its physical properties such as contrast, pixel expansion, and color were extensively studied by researchers worldwide. For example, Naor *et al* and Blundo *et al.* showed constructions of threshold VCS with perfect reconstruction of the black pixels. Ateniese *et al.* gave constructions of VCS for the general access structure. Krishna *et al.*, Luo *et al.*, Hou *et al.*, and Liu *et al.* considered color VCSs. Shyu *et al.* proposed a scheme which can share multiple secret images [13]. Furthermore, Eisen *et al.* proposed a construction of threshold VCS for specified whiteness levels of the recovered pixels.

The term of extended visual cryptography scheme (EVCS) was first introduced by Naor *et al.* in, where a simple example of (2,2)-EVCS was presented. In this paper, when we refer to a corresponding VCS of an EVCS, we mean a traditional VCS that have the same access structure with the EVCS. Generally, an EVCS takes a secret image and original share images as inputs, and outputs shares that satisfy the following three conditions: 1) any qualified subset of shares can recover the secret image; 2) any forbidden subset of shares cannot obtain any information of the secret image other than the size of the secret image; 3) all the shares are meaningful images.

There have been many EVCSs proposed in the literature. Furthermore, Zhou *et al.* [20] presented an EVCS by using halftoning techniques, and hence can treat gray-scale input share images. Their methods made use of the complementary images to cover the visual information of the share images. Recently, Wang *et al.* proposed three EVCSs by using an error diffusion halftoning technique to obtain nice looking shares. Their first EVCS also made use of complementary shares to cover the visual information of the shares as the way proposed in. Their second EVCS imported auxiliary black pixels to cover the visual information of the shares. In such a way, each qualified participants did not necessarily require a pair of complementary share images. Their third EVCS modified the halftoned share images and imported extra black pixels to cover the visual information of the shares.

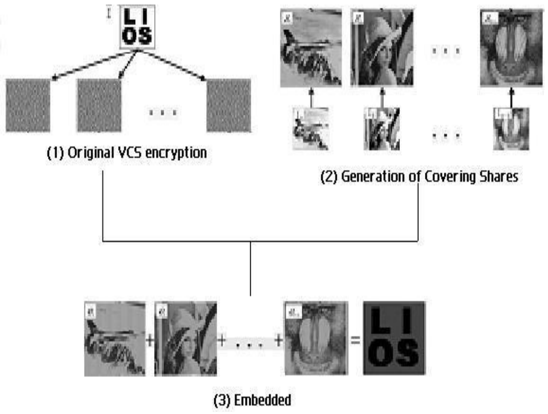
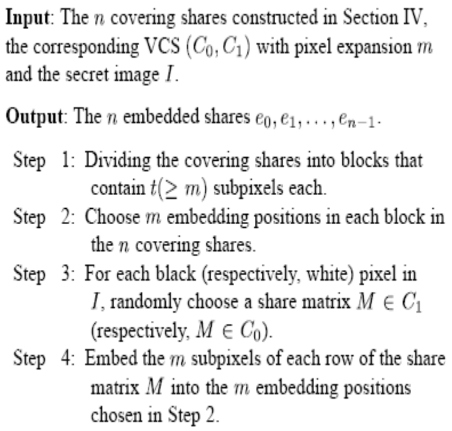

I
LI
OS
(1) Original VCS encryption
(2) Generation of Covering Shares
(3) Embedded
LI
OS

Fig.2. Embedded Sharing Scheme

A. Embedded Sharing Algorithm

For embedding the following process takes place.



```
Input: The $n$ covering shares constructed in Section IV, the corresponding VCS $(C_0, C_1)$ with pixel expansion $m$ and the secret image $I$.

Output: The $n$ embedded shares $e_0, e_1, \ldots, e_{n-1}$.

Step 1: Dividing the covering shares into blocks that
        contain $t(\geq m)$ subpixels each.
Step 2: Choose $m$ embedding positions in each block in
        the $n$ covering shares.
Step 3: For each black (respectively, white) pixel in
        $I$, randomly choose a share matrix $M \in C_1$
        (respectively, $M \in C_0$).
Step 4: Embed the $m$ subpixels of each row of the share
        matrix $M$ into the $m$ embedding positions
        chosen in Step 2.
```

Fig.3. Embedding Process Algorithm

IV. LZW COMPRESSION ALGORITHM

We used LZW Data Compression algorithm. The LZW data compression algorithm is applied for the gray scale image here. As a pre-processing step, a dictionary is prepared for the gray scale image. In this dictionary, the string replaces characters with single quotes. Calculations are done using dynamic Huffman coding. In compression of greyscale image select the information pixels. Then generate halftone shares using error diffusion method. At last filter process is applied for the output gray scale images.

A. Algorithm

The proposed systems use the LZW (Lempel-Ziv-Welch) Algorithm. The method used to implement in the following process.

1. Select the gray scale image.
2. Apply the LZW compression technique for the gray scale image.
3. Preparing the dictionary for the gray scale images.
4. In dictionary replaces strings of characters with Single codes.
5. Calculations are done by dynamic Huffman coding.
6. In compression of grey-scale image select the secret Information pixels.
7. Then generation halftone shares using error diffusion Method.
8. Filter process is applied for the output gray scale images.

Filters are used to improve the quality of reconstructed image to minimize the noises for sharpening the input secret image.

B. Applications

LZW compression became the first widely used universal data compression method on computers. A large English text file can typically be compressed via LZW to about half its original size. LZW was used in the public-domain program compress, which became a more or less standard utility in UNIX gzip DEFLATE compress uncompress_systems circa 1986. It has since disappeared from many distributions, both because it infringed the LZW patent and because produced better compression ratios using the LZ77-based algorithm, but as of 2008 at least FreeBSD includes both and as a part of the distribution.

V. ARCHITECTURE DIAGRAM

The following embedded visual cryptography is implemented in the Java Swing Framework.

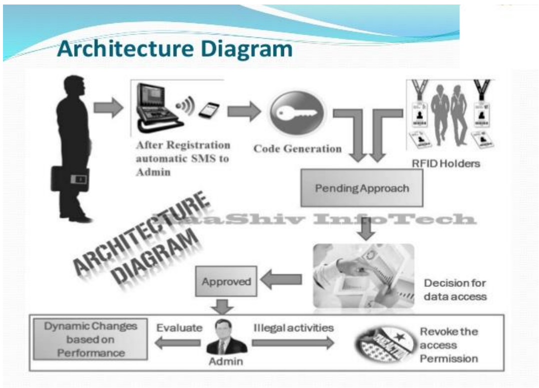


Fig.4. Network Implementation

VI. UML DIAGRAMS

A. Activity Diagram

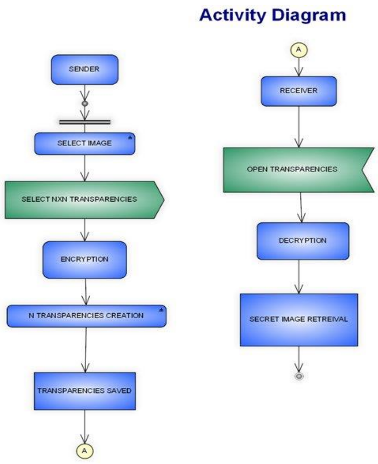


Fig.5. Activity Diagram

B. Dataflow diagrams

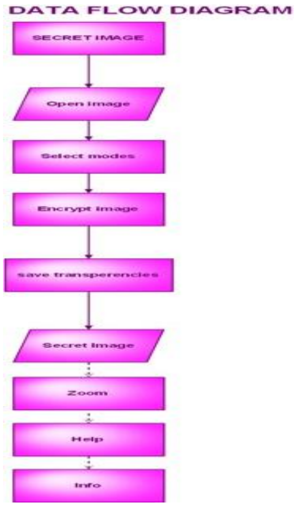


Fig.6. Data flow diagram

C. Sequence Diagram

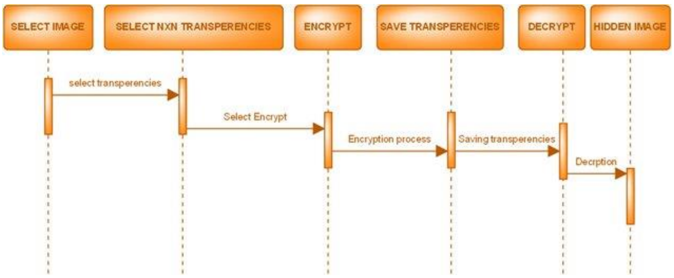


Fig.7. Sequence Diagram

VII. CONCLUSION

The Embedded visual cryptography scheme tool is simple and easy to use. Various visual cryptography schemes are studied and their performance is evaluated on four criteria: number of secret images, pixel expansion, image format and type of share generated. Security is the primary concern of today's communication world, is successfully implemented using the IDEA algorithm. It provides a safe and secure transmission as it involves multiple manipulations for encryption and so is it with decryption. This System provides a friendly environment to deal with images. Generally tools supports only one kind of image formats.

VIII. FUTURE WORK

In this paper, we propose a construction of EVCS which is realized by embedding random shares into meaningful covering shares, and we call it the embedded EVCS. Experimental results compare some of the well-known EVCSs proposed in recent years systematically, and show that the proposed embedded EVCS has competitive visual quality compared with many of the well-known EVCSs in the literature. In addition, it has many specific advantages against these well-known EVCSs, respectively.

IX. REFERENCES

[1] Feng Liu and chuankun.(2011), "Embedded Extended Visual Cryptography Schemes," IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, vol. 67, no. 2. (*references*)

[2] Shamir A. "How to share a secret",Commun ACM, vol. 22. No.11, pp.612-613.

[3] M.Naor and A.Shamir, "Visual Cryptography," in Proc.EUROCRYPT'94, Berlin Germany, vol. 950, pp. 1-12, Springer-verlag, LNCS.

[4] G. Ateniese, C. Blundo, A.De Santis and D.R. Stinson, "Visual Cryptography for general access structures," Inf.Computat.,vol. 129, pp. 86-106, 1996.

[5] http://java.sun.com.

[6] http://www.sourcefordge.com.

[7] http://www.java2s.com.