ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 2, pp: (1064-1071), Month: April - June 2015, Available at: www.researchpublish.com

Embedded Extended Visual Cryptography Schemes for Secret Image Using LZW Data Compression Algorithm

[1]Darshana R Wadde, [2]Prof.B.A.Patil

[1]Mtech Student, [1, 2] CSE Department, KLEMSSCET Belgaum, India

Abstract: **Visual cryptography scheme (VCS) is a kind of secret sharing scheme that focuses on sharing the secret images.The basic idea of visual cryptography scheme is to split secret image into number of random shares, here single share does not reveal any information about the secret image but by stacking two shares we can reconstruct the secret image. The underlying operation of the scheme is OR operation. Visual cryptography is one of technique used to encrypt the secret images by dividing the original image into transparencies. The transparencies can be sent to the intended person, and at the other end the transparencies received person can decrypt the transparencies using the tool, thus gets the original image. The proposed Visual cryptography provides the demonstration to the users to show how encryption and decryption can be done to the images. In this technology, the end user identifies an image, which is not the correct image. That is, while transmitting the image the sender will encrypt the image using the application here sender gets the two or more transparencies of the same image. The application provides an option to the end user of encryption. The end user can divide the original image into number of different images. Using the application we can send encrypted images that are in the format of GIF and PNG. The encrypted transparencies can be saved in the machine and can be sent to the intended person by other means.**

Keywords: **Image processing, visual Cryptography Scheme (VCS), GIF Encoding, Decoding.**

1. INTRODUCTION

Visual cryptography is the art of encrypting visual information such as handwritten text, images etc. The encryption takes place in such a way that no mathematical computations are required in order to decrypt the secret image. The original information to be encrypted is called as secret. Visual cryptography technology [1][4],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.

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 the users.

The basic principle of the visual cryptography scheme (VCS) was first introduced by Naor and Shamir. VCS is a kind of secret sharing scheme that focuses on sharing secret images. The idea of the visual cryptography model proposed in is to split a secret image into two random shares (printed on transparencies) which separately reveals no information about the secret image other than the size of the secret image. The secret image [9] can be reconstructed by stacking the two shares. The underlying operation of this scheme is logical operation OR. In this paper, we call a VCS with random shares the

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 2, pp: (1064-1071), Month: April - June 2015, Available at: www.researchpublish.com

traditional VCS or simply the VCS. In general, a traditional VCS takes a secret image as input, and outputs shares that satisfy two 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. An example of traditional (2,2)-VCS can be found in below Fig. 1.

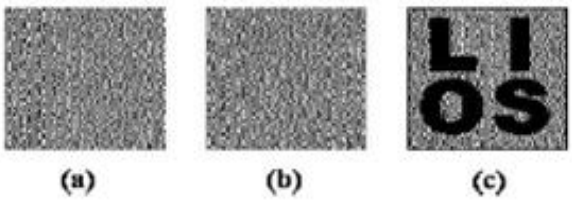


Fig 1: Basic traditional (2, 2) VCS

In the scheme of Fig. 1, shares (a) and (b) are distributed to two participants secretly, and each participant cannot get any information about the secret image, but after stacking shares (a) and (b), the secret image can be observed visually by the participants. Visual cryptography has many other modes they (2,3),(2,4),(2,5) which consist of more then two transparencies while encrypting the secret image VCS needs minimum of two shares, in single share positioning of pixel will be difficult.

2. RELATED WORK

2.1 Visual Cryptography for General Access Structure by Multi-pixel Encoding with Variable Block Size:

Multi-pixel encoding [11] is an emerging method in visual cryptography for that it can encode more than one pixel for each run. However, in fact its encoding efficiency is still low. This paper presents a novel multi-pixel encoding which can encode variable number of pixels for each run. The length of encoding at one run is equal to the number of the consecutive same pixels met during scanning the secret image. The proposed scheme can work well for general access structure and chromatic images without pixel expansion. The experimental results also show that it can achieve high efficiency for encoding and good quality for overlapped images.

2.2 Joint Visual Cryptography and Watermarking:

In this paper, we discuss how to use watermarking technique for visual cryptography [5]. Both halftone watermarking and visual cryptography involve a hidden secret image. However, their concepts are different. For visual cryptography, a set of share binary images is used to protect the content of the hidden image. The hidden image can only be revealed when enough share images are obtained. For watermarking, the hidden image is usually embedded in a single halftone image while preserving the quality of the watermarked halftone image. In this paper, they proposed a joint visual-cryptography and watermarking (JVW) algorithm that has the merits of both visual cryptography and watermarking

2.3 Visual Cryptography for Print and Scan Applications:

Visual cryptography is not much in use in spite of possessing several advantages. One of the reasons for this is the difficulty of use in practice [5]. The shares of visual cryptography are printed on transparencies which need to be superimposed. However, it is not very easy to do precise superposition due to the fine resolution as well as printing noise. Furthermore, many visual cryptography applications need to print shares on paper in which case scanning of the share is necessary.

The print and scan process can introduce noise as well which can make the alignment difficult. In this paper, we consider the problem of precise alignment of printed and scanned visual cryptography shares. Due to the vulnerabilities in the spatial domain, we have developed a frequency domain alignment scheme. We employ the Walsh transform to embed marks in both of the shares so as to find the alignment position of these shares. Our experimental results show that the technique can be useful in print and scan applications.

2.4 An Improved Visual Cryptography Scheme For Secret Hiding:

Visual Cryptography [7] 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.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 2, pp: (1064-1071), Month: April - June 2015, Available at: www.researchpublish.com

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 and of computers [11]. There are various measureon 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.

2.5 Halftone Visual Cryptography:

Visual cryptography [1] 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 [10] 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.

3. EXITING SYSTEM

Visual cryptography scheme is a art of encrypting the secret images so that apart from sender and intended person no one can realize the original image. By generating the covering shares the embedding covering can be realized by following algorithm.

The embedding process:

Input: The corresponding VCS (c_0, c_1) with pixel expansion and the secret image.

Output: The *n* embedded shares e_0,e_1,....e_{n-1}.

Step1: Dividing the covering shares into blocks that contain ($t \geq m$) subpixels each.

Step2: Choose m embedding positions in each block in the n covering shares.

Step3: For each black (respectively, white) pixel in *I*, randomly choose a share matrix M $\in$ c1

Step4: Embed the *m* subpixel of each row of the share matrix M into the *m* embedding positions chosen in Step2.

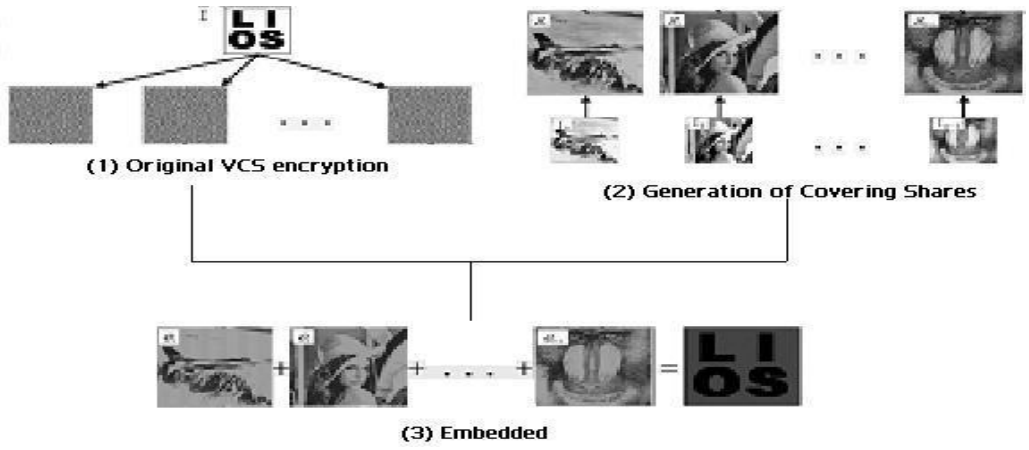


Fig 2: Embedding process

3.1 Limitation of the Existing System:

• The existing system does not provide a friendly environment to encrypt or decrypt the data (images).

• The system supports with only one type of image format only. For example, if it is .jpg, then it supports only that same kind of image format only.

4. PROPOSED SYSTEM

Proposed system Visual cryptography provides a friendly environment to deal with images. Generally cryptography tools supports only one kind of image formats. The 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.

4.1 LZW Data Compression Algorithm:

Lempel–Ziv–Welch (LZW) is a universal lossless data compression algorithm created by Abraham Lempel, Jacob Ziv, and Terry Welch. It was published by Welch in 1984 as an improved implementation of the LZW algorithm published by Lempel and Ziv[13] in 1978. The algorithm is simple to implement, and has the potential for very high throughput in hardware implementations.

4.2 Process of LZW 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 greyscale 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.

4.3 Uses:

LZW [13] 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. Several other popular compression utilities also used LZW, or closely related methods.

LZW became very widely used when it became part of the GIF TIFF PDF image format in 1987. It may also (optionally) be used in and files. (Although LZW is available Adobe Acrobat DEFLATE in software, Acrobat by default uses for most text and color-table-based image data in PDF files.)

4.4 Advantages of Proposed System:

• The Embedded Visual Cryptography Schemes for Secret images tool is easy to use.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 2, pp: (1064-1071), Month: April - June 2015, Available at: www.researchpublish.com

• The image are compressed and send the receiver in order to decrease the size and for fast transmitting the data (image)

• It support .gif and .png formats only.

5. MODULE

- Interface design using Applet frame work
- Visual cryptography implementation
- Testing and integration

5.1 MODULES DESCRIPTION:

Interface design using Applet frame work:

In this module, we design user interface design using applet frame work. The user interface should be very easy and understandable to every user. So that any one can access using our system . It must be supportable using various GUIs. The user interface also consist of help file. The help file assists on every concepts of the embedded visual cryptography. Help file should clearly depict the details of the project developed in simple language using various screen shoots.

Visual cryptography Implementation:

This module is the core for the project, where we implement the Visual Cryptography. 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 strings replace 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 least 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.

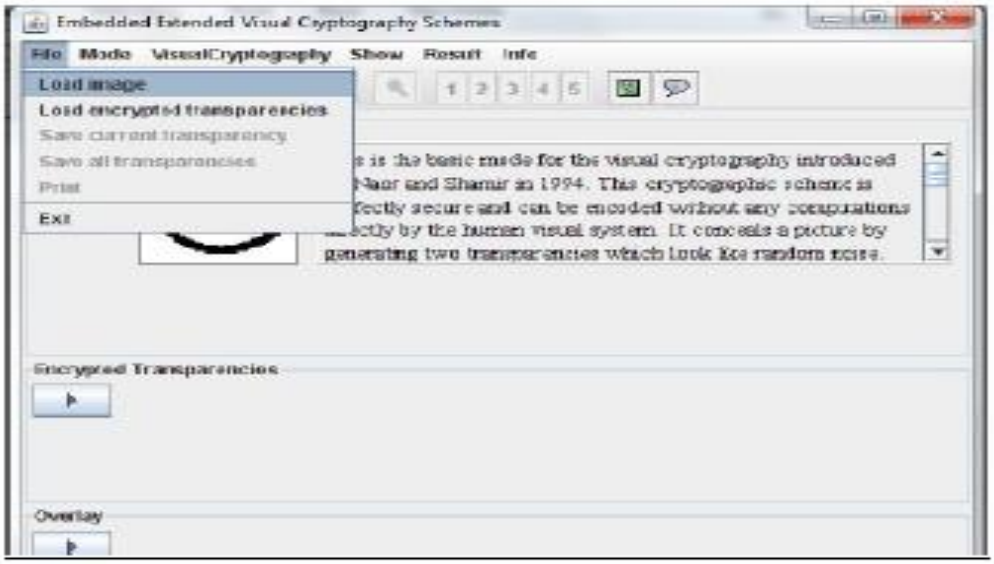
Testing and integration:

This is the final module, which consists of integration of Visual cryptography implementation module into interface design using applet viewer. Then we need to test with various images and formation of transparencies. The transparencies should be able to save and load into the user interface.

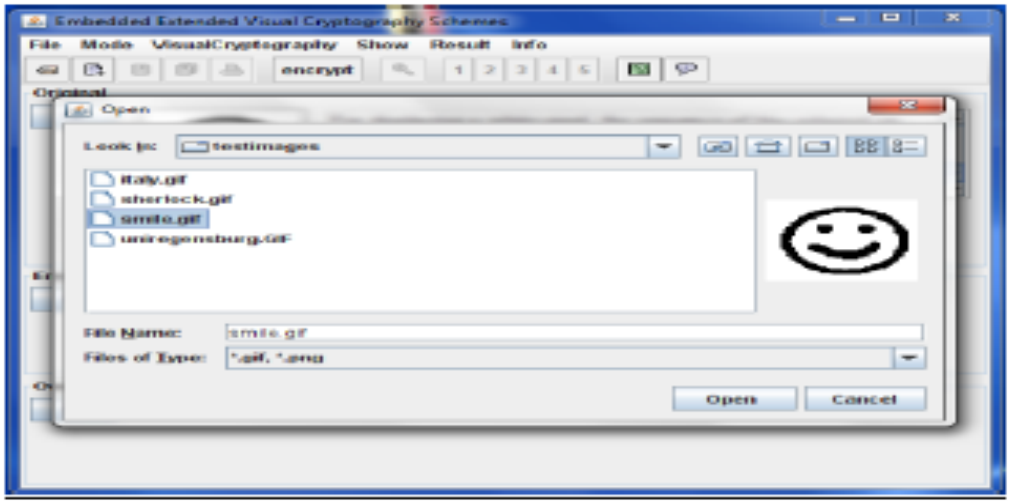
6. RESULTS ANALYSIS

6(a): shows the input of the image

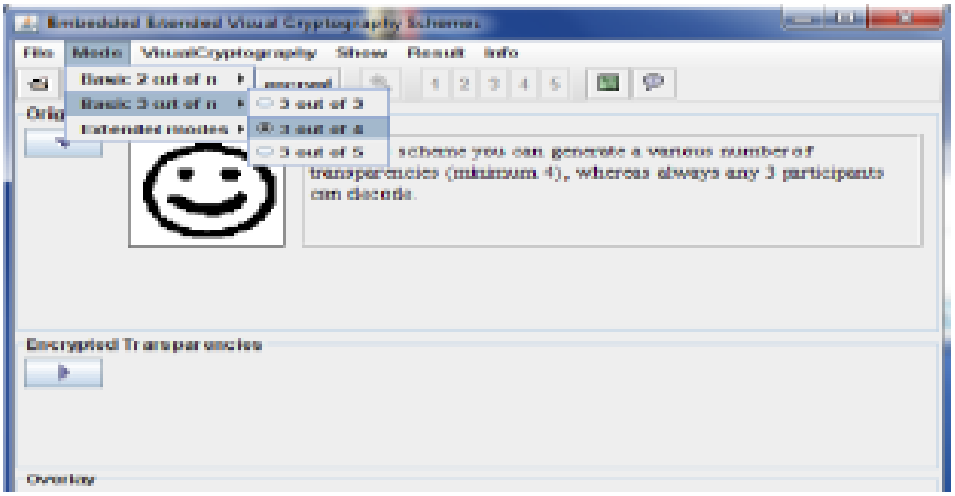
ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 2, pp: (1064-1071), Month: April - June 2015, Available at: www.researchpublish.com



6(b): shows the Loads the image on to the screen

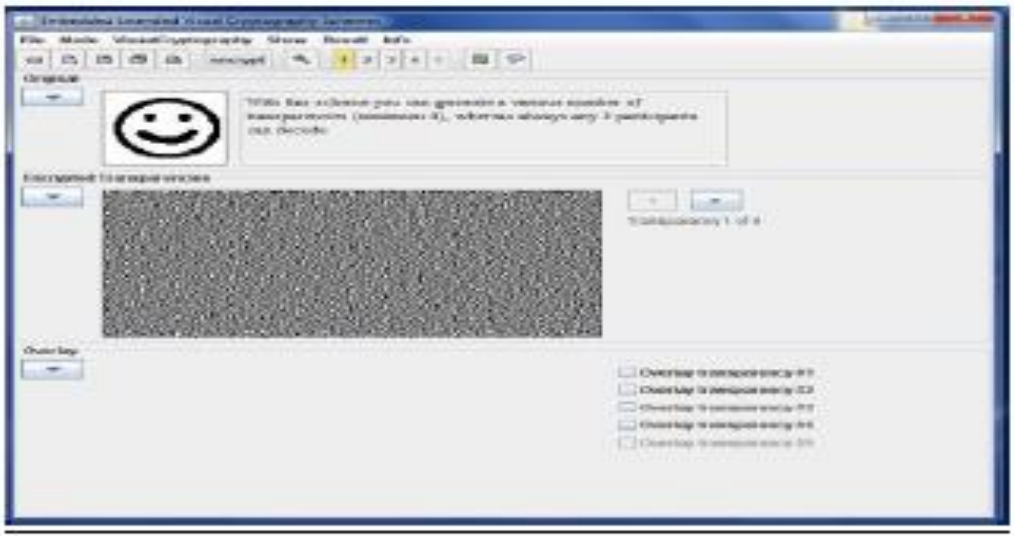


6(c) example of test image on to the screen



6(d) selects type of mode

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 2, pp: (1064-1071), Month: April - June 2015, Available at: www.researchpublish.com



6(e) shows the encrypted image loads on the screen

6(f) After Integration final image

7. CONCLUSIONS

The Embedded visual cryptography scheme tool is simple and easy to use. 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. 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. 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.

REFERENCES

[1] Shamir, "How to share a secret," Commun. ACM, vol. 22, no. 11, pp. 612–613, 1979.

[2] G. R. Blakley, "Safeguarding cryptographic keys," in Proc. National Computer Conf., 1979, vol. 48, pp. 313–317.

[3] M. Naor and A. Shamir, "Visual cryptography," in Proc. EUROCRYPT' 94, Berlin, Germany, 1995, vol. 950, pp. 1–12, Springer-Verlag, LNCS.

[4] M. Naor and B. Pinkas, "Visual authentication and identification," in Proc. CRYPTO'97, 1997, vol. 1294, pp. 322–336, Springer-Verlag LNCS.

[5] T. H. Chen and D. S. Tsai, "Owner-customer right protection mechanism using a watermarking scheme and a watermarking protocol," Pattern Recognit., vol. 39, pp. 1530– 1541, 2006.

[6] P. Tuyls, T. Kevenaar, G. J. Schrijen, T. Staring, and M. Van Dijk, "Security displays are enabling secure communications," in Proc. First Int. Conf. Pervasiv

[7] C. Blundo, A. De Bonis, and A. De Santis, "Improved schemes for visual cryptography," Designs, Codes and Cryptography, vol. 24, pp. 255–278, 2001.

[8] 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.

[9] N. K. Prakash and S. Govindaraju, "Visual secret sharing schemes for colour images using half toning," in Proc. Int. Conf. Computational Intelligence and Multimedia Applications (ICCIMA 2007), 2007, vol. 3, pp. 174–178.

[10] http://en.wikipedia.org/wiki/Lempl-Ziv-Welch.

[11] http://www.sourcefordgde.com.

[12] http://www.ieice.org/eng/shiori/mokuji.html.