RESEARCH ARTICLE OPEN ACCESS

The Cryptographic Schemes for Secret Images

P. Anusha[1], C. Prasad Rao[2]
[1]M.Tech Student, CSE Department, Sri Aditya Engineering College, A.P, India
[2]Asst.professor, CSE Department, Sri Aditya Engineering College, A.P, India

Abstract
Visual cryptography is one of the techniques used to encrypt the images by dividing the original image into transparencies [1]. The transparencies can be sent to the intended person, and at the other end the transparencies received person can decrypt the transparencies using our tool, thus gets the original image. Our 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 our application here sender gets the two or more transparencies of the same image. Our application provides an option to the end user of encryption. The end user can divide the original image into number of different images. Using our 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 [source].

Keywords - Visual cryptography, transparencies, visual cryptographic schemes. *,etc*

I. INTRODUCTION

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[2]. 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 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 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 Fig. 1, where, generally speaking, a –VCS means any out of shares could recover the secret image. 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. VCS has many special applications, for example, transmitting military orders to soldiers who may have no cryptographic knowledge or computation devices in the battle field. Many other applications of VCS, other than its original (i.e., sharing secret image), have been found, for example, authentication and identification, watermarkingand transmitting passwords etc.

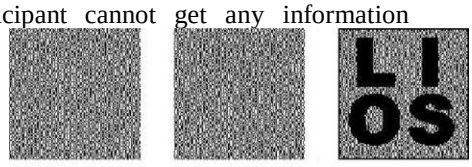


Fig. 1

Visual Secret Sharing Scheme :

The basic model of the visual cryptography consists of a several number of transparency sheets. On each transparency a ciphertext is printed which is indistinguishable from random noise. The hidden message is reconstructed by stacking a certain number of the transparencies and viewing them. The system can be used by anyone without any knowledge of cryptography and without performing any cryptographic computations. Naor and Shamir have developed the *Visual Se cret Sharing Scheme(VSSS)* to implement this model[Naor95]. In *k* out of *n* VSSS(which is also called (*k*, *n*) scheme), an binary image(picture or text) is transformed into *n* sheets of transparen- cies of random images. The original image be- comes visible when any *k* sheets of the *n* transparencies are put together, but any combination of less than *k* sheets cannot reveal the original binary image.

Examples of EVCS can be found in the experimental results of this paper, such as Fig. 2.

Fig. 2

EVCS can also be treated as a technique of steganography. One scenario of the applications of EVCS is to avoid the custom inspections, because the shares of EVCS are meaningful images, hence there are fewer chances for the shares to be suspected and detected.

II. LITERATURE SURVEY

Literature survey is the most important step in software development process. Before developing the tool it is necessary to determine the time factor, economy and company strength. Once these things are satisfied, then next step is to determine which operating system and language can be used for developing the tool. Once the programmers start building the tool the programmers need lot of external support. This support can be obtained from senior programmers, from book or from websites. Before building the system the above consideration are taken into account for developing the proposed system.

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 [3]. 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.

EVCS can also be treated as a technique of steganography. One scenario of the applications of EVCS is to avoid the custom inspections, because the shares of EVCS are meaningful images, hence there are fewer chances for the shares to be suspected and detected. There have been many EVCSs proposed in the literature. Furthermore, Zhou *et al.* [20] presented an EVCS by using half toning 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 half toning 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 [3]. Their third EVCS modified the half toned share images and imported extra black pixels to cover the visual information of the shares.

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

Multi-pixel encoding 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 withoutpixel expansion. The experimental results also show that it can achieve high efficiency for encoding and good quality for overlapped images.

B) Halftone Visual Cryptography:

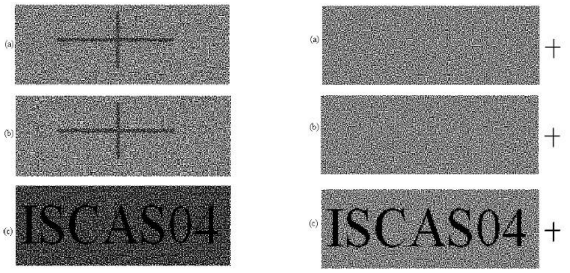
Visual cryptography encodes a secret binary image into shares of random binary patterns. If the shares are xeroxed onto transparencies, the secret image can be visually decoded by superimposing a qualified subset of transparencies, but no secret information can be obtained from the superposition of a forbidden subset. The binary patterns of the shares, however, have no visual meaning and hinder the objectives of visual cryptography. Extended visual cryptography [1] was proposed recently to construct meaningful binary images as shares using hypergraph colorings, but the visual quality is poor. In this paper, a novel technique named halftone visual cryptography is proposed to achieve visual cryptography via half toning. Based on the blue-noise dithering principles, the proposed method utilizes the void

and cluster algorithm [2] to encode a secret binary image into halftone shares (images) carrying significant visual information. The simulation shows that the visual quality of the obtained halftone share is observably better than that attained by any available visual cryptography method known to date.

C) Visual Cryptography for Print and Scan Applications:

Yan et al. [2] proposed a scheme in which they found a way of properly aligning the shares. The proper alignments of the shares are very important since only then the secret will be revealed. They came up with two methods:

Firstly, they put a mark beside the shares as shown in Figure 2 I and then the shares are overlapped according to the mark.



I II

Fig 3

I. Shares and reconstructed image using the first technique.
II. Shares and reconstructed image using the second technique.

Secondly, they put the mark in the shares using extended Visual Cryptography scheme. The example of this method is shown in Figure 2 II. The above two techniques work in the spatial domain. The drawback of these methods is that the alignment marks are visible to the unauthorized persons and can be thus easily removed by cropping (for the first method) and by localized image alteration (for the second method).

D) Joint Visual Cryptography and Watermarking:

In this paper, we discuss how to use watermarking technique for visual cryptography. 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, we proposed a joint Visual-cryptography and watermarking (JVW) algorithm that has the merits of both visual cryptography and watermarking.

E) An improved visual cryptography scheme for secret hiding: Authors: R.Youmaran, A. Adler, A.Miri

Visual Cryptography 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.

III. DIFFERENT MODULES:

- Interface design using applet frame work
- Visual cryptography implementation
- Encoding
- Decoding
- Creating transparencies
- Un-hiding image from transparency
- Testing and integration

MODULES DESCRIPTION:

The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover.

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

Encoding:

A high level view of the encoding algorithm is shown here:

1. Initialize the dictionary to contain all strings of length one.
2. Find the longest string W in the dictionary that matches the current input.
3. Emit the dictionary index for W to output and removeW from the input.
4. Add W followed by the next symbol in the input to the dictionary.
5. Go to Step 2.

A dictionary is initialized to contain the single-character strings corresponding to all the possible input characters (and nothingelse except the clear and stop codes if they're being used). The algorithm works by scanning through the input string for successively longer substrings until it finds one that is not in the dictionary. When such a string is found, the index for the string less the last character (i.e., the longest substring that *is* in the dictionary) is retrieved from the dictionary and sent to output, and the new string (including the last character) is added to the dictionary with the next available code. The last input character is then used as the next starting point to scan for substrings.

Decoding:

The decoding algorithm works by reading a value from the encoded input and outputting the corresponding string from the initialized dictionary. At the same time it obtains the next value from the input, and adds to the dictionary the concatenation of the string just output and the first character of the string obtained by decoding the next input value. The decoder then proceeds to the next input value (which was already read in as the "next value" in the previous pass) and repeats the process until there is no more input, at which point the final input value is decoded without any more additions to the dictionary.

In this way the decoder builds up a dictionary which is identical to that used by the encoder, and uses it to decode subsequent input values. Thus the full dictionary does not need be sent with the encoded data; just the initial dictionary containing the single-character strings is sufficient (and is typically defined beforehand within the encoder and decoder rather than being explicitly sent with the encoded data.)

Creating Transparencies:

This scheme provides theoretically perfect secrecy. An attacker who obtains either the transparency image or the screen image obtains no information at all about the encoded image since a black-white square on either image is equally likely to encode a clear or dark square in the original image.

Another valuable property of visual cryptography is that we can create the second layer after distributing the first layer to produce any image we want. Given a known transparency image, we can select a screen image by choosing the appropriate squares to produce the desired image. One of the most obvious limitations of using visual cryptography in the past was the problem of the decoded image containing an overall gray effect due to the leftover black sub pixel from encoding. This occurred because the decoded image is not an exact preproduction, but an expansion of the original, with extra black pixel. Black pixel in the original document remains black pixel in the decoded version, but White pixel becomes gray. This resulted in a lot of contrast to the entire image. The extra black sub pixel in the image causes the image to become distorted.

D - Secret information. K - Number of shares generated from D. share - piece of information.

Divide data D into n pieces in such a way that D is easily reconstruct able from any k pieces, but even complete knowledge of any k-1 pieces reveals no information about D. Stacking two pixels (each consists of four sub-pixels) can occur for example the following two cases: Secret sharing scheme is a method of sharing secret information among a group of participants. In a secret sharing scheme, each participant gets a piece of secret information, called a share. When the allowed coalitions of the participants pool their shares, they can recover the shared secret; on the other hand, any other subsets, namely non-allowed coalitions, cannot recover the secret image by pooling their shares. In the last decade, various secret sharing schemes were proposed, but most of them need a lot of computations to decode the shared secret information. The basic 2 out of 2 visual cryptography model consist of secret message encoded into two transparencies, one transparency representing the cipher text and the other acting as a secret key. Both transparencies appear to be random dot when inspected individually and provide no information about the original clear text. However, by carefully aligning the transparencies, theoriginal secret message is reproduced. The actual decoding is accomplished by the human visual system. The original is encrypted into 2 transparencies you need both transparencies to decode the message.

Un-hiding Image from Transparency:

The simplest form of visual cryptography separates an image into two layers so that either layer by itself conveys no information, but when the layers are combined the image is revealed. One layer can be printed on a transparency, and the other layer displayed on a monitor. When the transparency is placed on top of the monitor and aligned correctly, the image is revealed. For each image pixel, one of the two encoding options is randomly selected with equal probability. Then, the appropriate colorings of the transparency and screen squares are determined based on the color of the pixel in the 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.

IV. PROCESS SPECIFICATION

A) INPUT DESIGN:

The input design is the link between the information system and the user. It comprises the developing specification and procedures for data preparation and those steps are necessary to put transaction data in to a usable form for processing can be achieved by inspecting the computer to read data from a written or printed document or it can occur by having people keying the data directly into the system. The design of input focuses on controlling the amount of input required, controlling the errors, avoiding delay, avoiding extra steps and keeping the process simple. The input is designed in such a way so that it provides security and ease of use with retaining the privacy. Input Design considered the following things:

- What data should be given as input?
- How the data should be arranged or coded?
- The dialog to guide the operating personnel in providing input.
- Methods for preparing input validations and steps to follow when error occur.

B) OBJECTIVES:

1. Input Design is the process of converting a user-oriented description of the input into a computer-based system. This design is important to avoid errors in the data input process and show the correct direction to the management for getting correct information from the computerized system.
2. It is achieved by creating user-friendly screens for the data entry to handle large volume of data. The goal of designing input is to make data entry easier and to be free from errors. The data entry screen is designed in such a way that all the data manipulates can be performed. It also provides record viewing facilities.
3. When the data is entered it will check for its validity. Data can be entered with the help of screens. Appropriate messages are provided as when needed so that the user will not be in maize of instant. Thus the objective of input design is to create an input layout that is easy to follow.

C) OUTPUT DESIGN:

A quality output is one, which meets the requirements of the end user and presents the information clearly. In any system results of processing are communicated to the users and to other system through outputs. In output design it is determined how the information is to be displaced for immediate need and also the hard copy output. It is the most important and direct source information to the user. Efficient and intelligent output design improves the system's relationship to help user decision making. The system of 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.

It provides a safe and secure transmission as it involves multiple manipulations for encryption and so is it with decryption.

1. Designing computer output should proceed in an organized, well thought out manner; the right output must be developed while ensuring that each output element is designed so that people will find the system can use easily and effectively. When analysis design computer output, they should Identify the specific output that is needed to meet the requirements.
2. Select methods for presenting information.
3. Create document, report, or other formats that contain information produced by the system.

The output form of an information system should accomplish one or more of the following objectives.

- Convey information about past activities, current status or projections of the
- Future.
- Signal important events, opportunities, problems, or warnings.
- Trigger an action.
- Confirm an action.

V. TECHNIQUES AND ALGORITHM USED

In this technology, 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.

ALGORITHM:

Input: The c x d dithering matrix D and a pixel with gray- level g in input image I.

Output: The half toned pattern at the position of the pixel.

For i=0 to c-1 do

For j=0 to d-1 to do

If g<=Dij then print a black pixel at position (i, j);

Else print a white pixel at position (i, j);

For embedding

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.

VI. LIMITATIONS & FUTURE ENHANCEMENTS

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 EVC's, respectively.

VII. CONCLUSION

In this paper, we proposed a construction of EVCS which was realized by embedding the random shares into the meaningful covering shares. The shares of the proposed scheme are meaningful images, and the stacking of a qualified subset of shares will recover the secret image visually. We show two methods to generate the covering shares, and proved the optimality on the black ratio of the threshold covering subsets. We also proposed a method to improve the visual quality of the share images. According to comparisons with many of the well-known EVCS in the literature the proposed embedded EVCS has many specific advantages against different well- known schemes, such as the fact that it can deal with gray- scale input images, has smaller pixel expansion, is always unconditionally secure, does not require complementary share images, one participant only needs to carry one share, and can be applied for general access structure. Furthermore, our construction is flexible in the sense that there exist two trade- offs between the share pixel expansion and the visual quality of the shares and between the secret image pixel expansion and the visual quality of the shares.

REFERENCE & BIBLIOGRAPHY

[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 enablingsecure communications*,"in *Proc. First Int. Conf. Pervasive Computing, Boppard Germany, Springer-Verlag Berlin LNCS* 2004, vol. 2802, pp. 271–284.

[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 color images using halftoning*," in *Proc. Int. Conf. Computational Intelligence and Multimedia Applications (ICCIMA 2007)*, 2007, vol. 3, pp. 174–178.

[10] H. Luo, F.X.Yu, J. S. Pan, and Z. M. Lu, "*Robust and progressive color image visual secret sharing cooperated with data hiding*," in *Proc. 2008 Eighth Int. Conf. Intelligent Systems Design and Applications*, 2008, vol. 3, pp. 431–436.

SITES REFERRED
http://java.sun.com
http://www.sourcefordgde.com
http://www.networkcomputing.com/
http://www.roseindia.com/
http://www.java2s.com/

BIOGRAPHIES

P. Anusha is Pursuing M.Tech in Computer Science from Sri Aditya Engineering College, Surampalem, A.P. Her area of interest includes Cryptography, Data Base Management Systems, Data warehousing and Data Mining and Web Technologies.

C. Prasad rao, Asst. Prof. Computer Science and Engineering at Sri Aditya Engineering College, Surampalem, E.G.Dt. His area of interest includes Cryptography, Data Base Management Systems, Data warehousing and Data Mining and Web Technologies.