International Journal of Computer Trends and Technology (IJCTT) - volume4 Issue5–May 2013

Entrenched Visual Cryptography using Secret Sharing Scheme with public Key

Kode Phani Kumar[1], B.VeeraMallu[2]

[1]M.Tech, Department of CSE, K.L.University, Andhra Pradesh, India
[2]Assoc.professor, Department of CSE, K.L.University, Andhra Pradesh, India

***Abstract*: Visual cryptography scheme (VCS) is a cryptography technique which allow visual data i.e.: printed text, handwritten notes, and picture is encrypted in such a way that the decryption can be done by the human visual system, without the support of computers. In order to share undisclosed images, VCS used as a secret sharing schema. The idea is to convert the written stuff into a cipher text by using ElGamal Algorithm and then place that cipher text in to an image and encode this image into n shadow images. The decoding requires only selecting some splits of these n images, creation transparencies of them, and stacking them on top of other transparencies.**

***Keywords*: Visual cryptography scheme, secret sharing**

I.INTRODUCTION

With the rapid improvement of network technology, multimedia information can be sent over the internet easily. Various secret information such as military maps and Commercial identifications are transmitted over the Internet. While using secret images, security issues should be taken into consideration because hackers may utilize weak link over communication network to steal information that they want to deal with the security problems of secret images, a variety of image secret sharing schemes have been developed.

Visual cryptography is invented first in 1994 by Noar and Shamir. Visual cryptography is a cryptographic technique which allows visual data (e.g. printed text, handwritten notes and pictures) to be encrypted in such a way that the decryption can be done by the human visual system, without the help of computers. Visual cryptography scheme removes difficult computation problem in decryption process, and the secret images can be restored to former condition by stacking procedure. This property makes visual cryptography mainly useful for the low computation load necessity. The idea of the visual cryptography model proposed in is to split a secret data into two random shares (printed on transparencies) which individually reveals no information about the secret image other than the size of the secret image. The secret image can be reorganizing by stacking the two shares. The fundamental operation of this scheme is logical operation OR. In this paper, we call a Visual cryptography scheme 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 (*k* ,*n*)-VCS means any out of *n* shares could recover the secret image. In the scheme of Fig. 1, shares (a) and (b) are distributed to two participants secretly, and each member 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. In (2,2) secret sharing, any share by itself does not provide any information, but together they reveal the secret data.

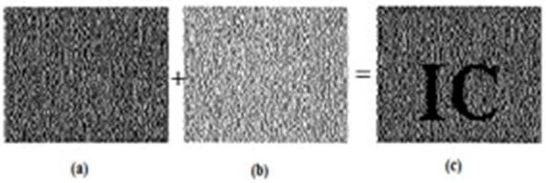

Fig.1: Example of traditional VCS.

VCS has many special applications, for example, transmit military orders to soldiers who may have no cryptographic knowledge or working out devices in the battle field. Extra applications of VCS, other than its original objective (i.e., sharing secret image), have been found, for example, verification and identification, watermarking and transmitting passwords etc.

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 equivalent VCS of an EVCS, a traditional VCS that have the same access structure with the EVCS. Usually, an EVCS takes a secret image and original share images as inputs, and outputs a share that suits the following three conditions:
1)Any qualified split 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 significant images.

II. RELATED WORK:

A.Elgamal encryption algorithm:

In cryptography, the ElGamal encryption system is an asymmetric encryption algorithm for public-key cryptography which is establish on the Diffie–Hellman key exchange. It was described by elgamal in 1984. ElGamal encryption is used in the free GNU Privacy Guard software, modern versions of PGP, and other cryptosystems. The Digital Signature Algorithm is a alternative of the ElGamal signature scheme, which should not be perplexed with ElGamal encryption.
One reason for the great momentum following up ElGamal's work is its enabling of the use of the widely believed reliable intractability for underlying the security of public-key cryptosystems: the CDH problem, which is widely believed to be as hard as the DL problem and the latter is
Considered to be a good alternative to the other widely accepted reliable intractability, the IF problem (the basis for the RSA and Rabin).
We now show that the system specified in is indeed a cryptosystem, i.e., Alice's
decryption procedure will actually return the same plaintext message that Bob has encrypted. Since

$C^x_1 \equiv (g^k)^x \equiv (g^x)^k \equiv j^k \equiv c_2/m \pmod p$,

the decryption calculation does indeed restore the plaintext *m*.The division in the decryption step needs to use the extended Euclid algorithm which is generally more costly than a multiplication. However Alice may avoid the division by computing.

$m \leftarrow c_2 c_1^{-x} \pmod p$
One may verify that this decryption method works, but notice that –*x* here means *p* – 1 – *x*.

Algorithm 1: The Elgamal cryptography
Key steps
To set up a user's key material, user 1 perform the following steps:
1. Choose a random prime number p,
2. Compute a random multiplicative generator element g of F^*_p ;
3. Pick a random number x€u Z_{p-1} ;
4. Compute her public key by
$Y \leftarrow g^x \pmod p$;
5. Publicize (p,g,y) as her public key ,and keep x as her private key.

Encryption:
To send a confidential message m<p to user1, the sender picks K €u Z_{p-1} and computes cipher text pair (c1, c2) as follows:
$C1 \leftarrow g^k \pmod p$,
$C2 \leftarrow y^k m \pmod p$,

Decryption:
To decrypt cipher text (c1,c2) user1 computes
$m \leftarrow c_2/c^x{}_1 \pmod p$

III. HALFTONING TECHNIQUE:

One of the main drawbacks of the VCS's proposed is that, they cannot deal with the gray-scale image. So to deal with the gray-scale images, we proposed haiftone technique for VCS; on the other hand, it has large pixel expansion C X M , where C is the number of the gray-levels and M is the pixel expansion of the corresponding black and white VCS. In order to deal with the gray-scale image, the halftoning technique was introduced into the visual cryptography. The halftoning technique is used to alter the gray-scale image in to the binary image. This technique has been widely used in printing applications which has been proved to be very efficient. Once we have the binary image, the VCS anticipated can be applied directly. However, the simultaneous loss in quality is unavoidable in this case.

The patterning dithering makes use of a certain percentage of black and white pixels, often called as patterns, to achieve a sense of gray scale in the overall point of view. The pattern consists of black and white pixels, where a different percentage of the black pixels stand for the different gray nesses. The halftoning process is to map the gray-scale pixels from the original image into the patterns with certain percentage of black pixels. The halftoned image is a binary image. However, in order to store up the binary images one needs a large amount of memory.

The halftoning process is formally described in Algorithm 1. Generally, for an input image of size P X Q , the halftoning process runs on each pixel in I as follows. In Algorithm 1, the halftoning process causes the mn pixel expansion on the input image. We call it the halftone pixel expansion. In the rest of the paper, we denote as the halftone pixel expansion.

Algorithm 2: The halftoning process for each pixel in *I*:

Input: The m X n dithering matrix K and a pixel with gray-level g in input image I.

Output: The halftoned pattern at the position of the pixel

```
For x=0 to m-1 do
For y=0 to n-1do
If g<=Kij then print a black pixel at position (x, y);
Else print a white pixel at position (x ,y);
```

By using this halftone technique we will separate black and white pixels from a particular position of an image which has to be encrypted.

IV. ENTRENCHING VCS INTO THE COVERING SHARES:

The merging process can be realized by the following algorithm after generating the covering shares.

Algorithm 3: The Entrenching process:

Input: The covering shares constructed, the corresponding VCS with pixel expansion and the secret image I.

Output: The n embedded shares k0, k1,k2,…..,kn-1.

Step 1: First dividing the covering shares into blocks which contain t sub pixels each.

Step 2: Choose m merging positions in each block in the n covering shares.

Step 3: For each black and white pixel in I, randomly choose a share matrix.

Step 4: Embed the m sub pixels of each row of the share matrix M into the m embedding positions chosen in Step 2.

In the above Algorithm 2 of step 4, “embed” is represented as the pixels in the embedding positions are replaced by the sub pixels of the share matrix. The sub pixels in the covering shares will protect the information about the original shared image. Here by we will merge the covering shares which are generated with the original share images.

V. CONCLUSION:

The shares of the proposed scheme are meaningful images, and the stack of a qualified subset of shares will recover the secret image visually without the aid of computers. Visual cryptography schema can deal with gray-scale input images, has smaller pixel expansion, is completely secure, does not require paired share images, one applicant only needs to carry one share, and can be applied for common access structure.

REFERENCES:

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

[2]. M.Naor and A.Shamir, “Visual cryptography,” in *Proc. EUROCRYPT’ 94*, Berlin, Germany, 1995, vol. 950, pp. 1–12, Springer-Verlag, LNCS.

[3]. Z. Zhou, G. R. Arce, and G. Di Crescenzo, “Halftone visual cryptography,” in *Proc. 2003 Int. Conf. Image Processing*, 2003, vol. 1, pp.I-521–I-524.

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

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