INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

An Extended Color Visual Cryptography Algorithm for General Access Structures

Juby Justin[1] and Giss George[2]

[1]M.Tech Student (CSE),
Viswajyothi College of Engineering and Technology,
Muvattupuzha, Kerala, India
jubyjustin@gmail.com

[2]Assistant Professor- CSE
Viswajyothi College of Engineering and Technology,
Muvattupuzha, Kerala, India
gissgeo@gmail.com

Abstract – *Visual Cryptography Scheme (VCS) is a type of secret sharing scheme which allows the encoding of a secret image into n shares that distributed to n participants. Each share constitutes some information and when k shares out of n stack together the secret will reveal. However; less than k shares are not work. The advantage of the visual secret sharing scheme is its decryption process i.e. to decrypt the secret using Human Visual System without any computation. Traditional Visual Cryptography suffers from share identification problem. This problem can be solved by extended visual cryptography (EVCS), which adds a meaningful cover image in each share. But most EVCS for general access structures suffer from pixel expansion problem. This paper proposes a general approach to solve above mentioned problems. This approach can be used for color secret images.*

Key Terms – *Extended Visual Cryptography Scheme (EVCS), Pixel expansion, General access structures*

1. INTRODUCTION

Visual Cryptography is a special type of encryption technique to hide information in images and decryption can be performed by the human vision if the correct key images are used. This technique was introduced by Naor and Shamir [2] in the year 1994. In Visual Cryptography scheme the secret image is divided into different random shares look like noise. It is impossible to retrieve the secret information from one of the images. Sufficient number of transparent images is required to reveal the information. The easiest way to implement Visual Cryptography is to print the two layers onto a transparent sheet.

In this technique text or picture should be fed as a digital image in the system as the input and the system generates 'n' (2<n) numbers of different images (called shares), look like images of random noise. Among 'n' number of shares user has to stack 'k' number of shares, where 2<k<n, to reveal the secret image. The major feature of this scheme is that the secret image can be decrypted simply by the human visual system without having to resort to any complex computation. Naor and Shamir's scheme[2] could hide the secret image in *n* distinct images called shares. The secret image could then be revealed by simply stacking together as many as *k* of the shares. Each of the shares looked like a collection of random pixels and of course appeared meaningless by itself. Naturally, any single share, before being stacked up with the others, reveals nothing about the secret image. Figure 1 describes an example for visual cryptography scheme suggested by Naor [2].

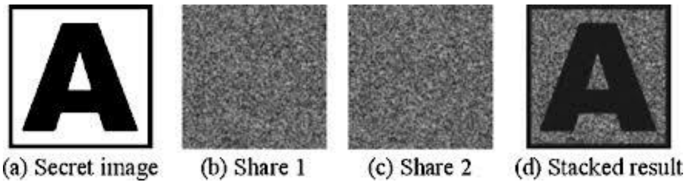

Figure.1.Example for visual cryptography scheme

Ateniese [3] proposed the basic concepts of general access structure (GAS) and developed a VC based solution for some GAS. By using the GAS, dealers can define reasonable combinations of shares as decryption conditions rather than specifying the number of shares. (k,n) –VSS scheme is a special case of GAS. Traditional Visual Cryptographic Scheme suffers from share management problem-dealers cannot identify each share visually. An Extended Visual Cryptography scheme

(EVCS), which embeds a cover image to each share to solve the share management problem.

The pixel expansion problem is a one of common disadvantage of most VSS scheme. In traditional VC-based approach, each pixels within the secret image is encrypted in a block consisting of *m* sub pixels in each share images. The pixel expansion problem affects the practicability of storage and decreases the contrast of the recovered image. The existing EVCS algorithms for GAS are suffering from pixel expansion problem. The proposed scheme is EVCS for GAS applicable for color secret/ cover images. The proposed scheme is a two phase algorithm, in which the first phase uses an optimization technique for construct a pixel expansion free shares for the GAS. The second phase of the algorithm adds a cover images to noise like shares using a stamping algorithm.

The remainder of this paper is organized as follows: Section 2 presents the related works. Section 3 introduces the proposed encryption algorithm. Section 4 presents the proposed decryption algorithm and Section 5 concludes this paper.

2. RELATED WORKS

In the year 1994, Naor and Shamir [2] introduced the concept of visual cryptography to encode a binary image into two shares, share$_1$ and share$_2$.The decryption can performed using human Visual System (HVS). In a *(k,n)*-threshold Visual Cryptography Scheme (VCS), one binary secret image was encoded into *n* random noise like shares. These *n* shares are distributed to a set of *n* participants. When *k* or more shares stacked together, the secret image is revealed. In the year 1996, Ateniese first proposed VCS for General Access Structure (GAS) [3].In Visual cryptography scheme for GAS, each participant in *P* receives one share. Certain subsets of participants, called qualified sets Γ_{Qual}, can recover the secret image, but other subsets of participants, called forbidden sets Γ_{Forb}, have no information on the secret image. As other traditional VCS Ateniese's VCS approach for GAS also suffers from pixel expansion and this scheme is only applicable for binary images.

In the year 2010, Liu [4] proposed a step construction to construct a VCS for GASs by performing (2, 2) VCS recursively. This scheme is applicable only for binary secret images. The main concept of Liu's approach is that the participant can take multiple share images for sharing a single secret image. In 2012 Lee [1] proposed an extended VC algorithm for general access structures, that is free from pixel expansion problem and shares for GAS are meaningful. But Lee's concept is only applicable for binary secret and cover images.

3. PROPOSED ENCRYPTION ALGORITHM

This section, describes a two phase encryption algorithm of color EVCS for GASs. The solution procedures for color EVCS are shown in Figure 2. The first phase generates intermediate shares $(I_1, I_2 \ldots . I_n)$ based on the access structures. In the second phase cover images are embedded into the I-shares. Each module in proposed system will be described in the following sections.

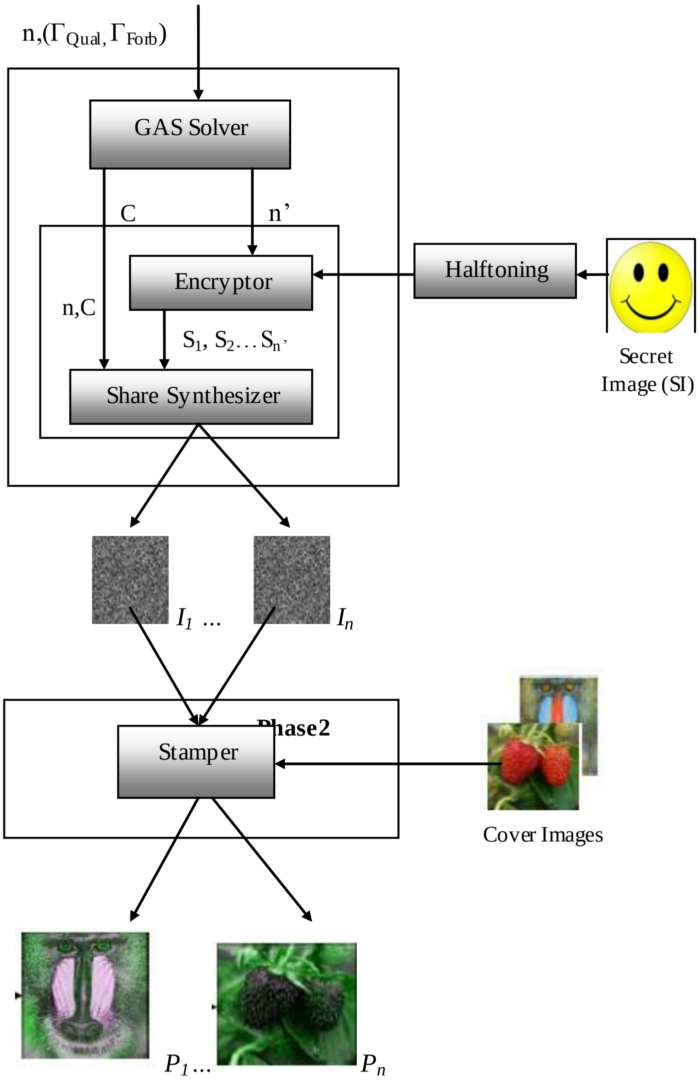

Figure 2 Solution procedure for Color EVCS

3.1 Phase I: Generating I- Shares: This phase constructs a pixel expansion free VCS for a given access structures $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}})$. The main idea behind this approach is as follows: In this scheme *n'* different keys are used to protect a secret and distribute these *n'* keys to n participants. Each participant is allowed to hold at least one key. If someone wants to access a secret, he/she has to collect *n'* different keys from a set of participants. If any one of the key is missed, the secret will remain protected.

In this scheme color image is used as secret image. In this method construction of (*n',n'*) VCS is adopted as encrypt or in Figure 2. The I-shares of access structures of VCS are synthesized from the basis shares produced by the encrypt or. Construction set C is the relation between the basis shares and I- shares. Before encrypting the secret image some preprocessing operations are performed. A GAS solver is used to find the number of basis shares *n'* and corresponding construction set C for the access structure of VCS.

3.1.1 GAS Solver:

For a set of participants $P= \{i_1,i_2,....i_n\}$ and access structure ($\Gamma_{Qua}, \Gamma_{Forb}$) the GAS solver is used to finding a construction set C with minimal *n'*. In this scheme a GAS solver is developed based on the simulated annealing (SA) approach to solve the proposed mathematic optimization formulation for the GAS problem. Our solution approach adopts an iterative improvement framework. The iteration is based on the decision variable *n*'. The proposed iterative improvement framework is listed in Algorithm 1[1]. The pseudo code for the proposed SA-based algorithm,*GAS_SA()* is in Ref [1].

Algorithm1: SA- based algorithm for GAS solver

```
Procedure GAS_solver($n$, $n'_{max}$, $\Gamma_{Qua}$, $\Gamma_{Forb}$)

1.  $n' \leftarrow$ n
2.  Call GAS_SA($n$, $n'_{max}$, $\Gamma_{Qua}$, $\Gamma_{Forb}$, $C_{best}$, $Z_{best}$)
3.  If Zbest ≥ 1 then //No solution in last turn
4.  $n' \leftarrow n'+1$
5.    If $n' = n'_{max}$ then stop and Output " No Solution found"
6.    If n'<n then goto step 11
    else
7.    C← $C_{best}$// Found a solution in last turn
8.    If $n'$ < n then goto step 11
9.  $n' \leftarrow n'$-1 // Improvement
10. End If
11. Goto step 2
12. Output $n'$ , C
```

3.1.2*Halftoning:*

The proposed system uses color image as secret image. So some half toning techniques are applied before encryption. In this stage the color secret image is separated into three planes R, G, B. Then halftone operation is performed in each plane separately. Half toned R, G, B planes are given to the encryptor. In half toning the greyscale image is converted into binary images. In color image each plane is a greyscale image. So after halftone operation three binary images are obtained.

3.1.3 Share Constructor:

The share constructor consists of two modules in Figure 2: the encryptor and share synthesizer. The encryptor adopts Yang's construction for the (*n',n'*) – ProbVSSscheme [5]. In the share constructor, the first module (encryptor) generates the basis shares by employing Yang's ProbVSS scheme. Then the share synthesizer produces intermediate shares (I- shares) by stacking the basis shares upon the construction set C. The procedure for the share constructor is described in Ref [1]. The share constructor phase is applied on three planes.

3.2 *Phase II: Stamping Cover Images*

The most VCS produce the random noise like shares as output. The hackers are more interested in this type of random shares and these shares are difficult to recognize by the participants. To recover from these difficulties the proposed scheme uses meaningful shares. By using the stamping algorithm in Ref [1] the shares are meaningful if the secret is binary. But in the case of color secret image the shares a partially meaningful due to high amount of random pixels. So in the proposed system a digital watermarking technique [6] is used for stamping a cover image to the random share without any pixel expansion.

The cover images are color images that are represented by 24 bits (8 bits in each plane). The random looking shares are represented by 8 bits. The proposed scheme digitally watermarks these 8 bits of a pixel into the 24 bit pixel of the cover image. This can be done by replacing the b Least Significant Bits (LSB) of each plane of the cover image. The proposed digital watermarking technique used for stamping is listed in Algorithm 2 [6].

Algorithm2: Proposed Stamping algorithm

```
Procedure Stamping (Shares, Covers)

1.  Repeat for all shares
2.  Repeat for each pixel of share
        i)  Generate an array S[0…8] that contain the
        bits of a pixel value
    ii) Decompose the color cover into three components Red, Green, Blue and store bits of each component into three arrays R[0…8], G[0…8] and B[0…8] respectively.
    iii) Find that which channel contain more information, i.e which color has less effect in the cover image.
    iv) Replace the 2 least significant bits of the rest two channel with the share pixel value and 4 least significant bits of the channel that have less effect.
3. Stop
```

4. PROPOSED DECRYPTION ALGORITHM

The advantage of traditional VCS is no computation is required for decryption. Stacking of sufficient number of shares will reveals the secret image. In the proposed scheme a cover image is stamped into the shares. So before stacking the shares the original shares are extracted from the cover images. The extracting of original shares is to retrieve the 8 bit from the three planes of the cover images. Extract the same number of bits as embedded in the watermarking phase. The extracted shares are broken into three planes. The *8* bit planes of each shares is generated. Then, all the binary shares at the same bit plane are stacked. Stack operation can be implemented by performing the OR operation to reveal the secret image.

5. CONCLUSION

This paper proposes a two phased encryption for the Color EVCS for general access structures. The proposed scheme will solve the pixel expansion and share identification problem. The quality of the recovered image is high when compare with other VCS. In the proposed encryption algorithm, there is no need of sophisticated code for EVCS. Each phase in the encryption is less coherent, so it can be individually designed and also easily replaced separately. The advantage of the proposed scheme is the encryption phase is not only applicable to extended VCS but also to traditional VCS to construct shares without any pixel expansion. The proposed stamping algorithm can be applied on all existing VCS to modify them as EVCS without redesign the codebook.

REFERENCES

[1] Kai Hui Lee ,Pei Ling Chiu ”An extended visual cryptography for general access structure” *IEEE Trans on Information Forensics and Security,* Vol 7 ,No 1, Feb 2012

[2] M. Naor and A. Shamir, “Visual cryptography,” in *Proc. Advances in Cryptology (Eurprocrypt’94)*, 1994, pp. 1–12.

[3] 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.

[4] F. Liu, C. Wu, and X. Lin, “Step construction of visual cryptography schemes,” *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 1, pp. 27–38, Mar. 2010.

[5] C. N. Yang, “New visual secret sharing schemes using probabilistic method,” *Pattern Recognit. Lett.*, vol. 25, pp. 481–494, 2004.

[6] Aarti , Harsh K Verma, Pushpendra K Rajput, “ Ideal Contrast Secret Sharing Scheme through Meaningful Shares with Enveloping Digital Watermarking using Bit Plane based *(k,n)*-VCS” International Journal of Computer Applications vol. 46, No.9, pp 36-41 , May 2012