International Journal of Research In Advent Technology Vol.3 No.2, February 2015
E-ISSN: 2321-9637

Extended Visual Cryptography Scheme for Colour Images with No Pixel Expansion

Samiksha Chaudhary, Dhrumil Shah, Mayuri Sonawane, Mrunali Desai
samiksha.c@somaiya.edu , dharumil.s@somaiya.edu , m.sonawane@somaiya.edu , mdesai@somaiya.edu

Abstract- Visual Cryptography is a special encryption technique to hide information in images, which divide secret image into multiple shares. Each share holds some information when k out of n shares 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 problemsand can be used for color images.

Keywords: Extended visual cryptography, secret sharing scheme and general access structure.

1. INTRODUCTION

Visual Cryptography was introduced by Moni Naor and Adi Shamir at EUROCRYPT 1994[1,2] is a new cryptographic scheme where the cipher text is decoded by the human visual system (eyes). Hence, there is no need to perform any complex cryptographic computation for decryption. The idea is to hide a secret message (text, handwritten text, picture, etc…) in different images called shares or cover images. When the shares (transparencies) are stacked together in order to align the sub pixels, the secret message can be recovered. The simplest case is the 2 out of 2 scheme where the secret message is hidden in 2 shares, both needed for a successful decryption. W.G. Tzeng and C.M. Hu [3] introduced a new color secret sharing scheme based on Visual Cryptography schemes (VCS) where the traditional stacking operation of sub pixels and rows interrelations is modified. This new technique does not require transparencies stacking and hence, it is more convenient to use in real applications. Visual Cryptography is a special encryption technique to hide information in images in such a way that it can be decrypted by the human vision if the correct key image is used. In secret sharing mechanisms, the secret data is divided into several shares (images) anddistributed among participants. Shares are stacked together to recover the data. Visual cryptography (VC) attempts to recover a secret image via the human visual system by stacking two or more transparencies.

In VC approach [4], the secret image was partitioned into *n* shadow images (shares), and each participant would receive only one share. Once any *k* or more shares of a secret are stacked together, the secret image will be visually retrieved without the help of the computer. That is to say that the secret image will be invisible if the number of stacked sharesis less than *k*. This is known as (*k*, *n*)-threshold mechanism. Figure1 describesan example for visual cryptographyscheme suggested by Naor [2].There have been some otherEVCS schemes proposed, there is no EVCS forcolor images that supports the general k-out-of-nsecret sharing while having no pixelexpansion,that is, the pixel expansion rate being equal toone. The above mentioned drawback could be eliminated with the help of k-out-of-n EVCS forcolor images with-out pixel expansion. Aprobabilistic technique will help in achieving nopixel expansion. The scheme also allows a user to choose the number of color levels for eachprimary color (i.e. Red, Green and blue) that thereconstructed image and each share image couldhave. The reconstructed image refers to theimage obtained by imposing k or more shareimages. Thevarious references used are listed at the end of this paper.

2. BACKGROUND & MOTIVATION

Previously a multipixelencoding method which could recover the graylevelor colored images with better visualquality. Hou used halftone technique and colorcomposition decomposition to simulate the grayscale of an image, thus solved the problem ofNaor and Shamir's method which could only beapplied to black and white images. Later Thien and Lin improved Shamir'stheorem by using r pixels of a secret image asthe coefficients of a r-1 degree polynomial, and,consequently, reduced the share size to 1/r.Based on the conceptions, Chen and Lin also proposed a differentprogressive secret sharing scheme, using thetechniques of reordering the bit-planes anddiscrete cosine transformation of an

image,respectively. References provided perfect ways to share information and could even obtain the objective ofdisplaying the secret image progressively.Nevertheless, all these schemes neededcomputer to solve those complicated math inorder to decrypt the secret image other thansimply using the human eyes.The conventional VC is to producen shares from a secret image and to dispatchthem to n participants. We will get the secretinformation only when k or more shares are stacked together and nothing if less than k sharesare obtained, which is the conception of "All-or-Nothing." A new sharing concept called"progressive VC" came out which can improvethe clarity of a secret image step by step bystacking more and more shares.Jin-et-al proposed a multi-resolutionapproach to share secret image that can beapplied to VC. They expand pixels to 3×3 blockin which eight of them are used to represent thegray value of each pixel and the remaining oneis used to store the halftone value of the secretimage. In order to take advantage of visualeffects, Jin-et-al uses a "lookup table" toadjust the pixel value so that pixels with a largergray value in the secret image own more "1"s (1represents black) in its eight bit-planes. Theadjusted eight binary digits are handled byconventional VC; therefore, an obscure secretimage can be directly obtained from stackingshares. By utilizing computer equipment's toperform the XOR operations on the ninth bit, thehalftone secret image can be perfectlyreconstructed. However, Jin's work cannot disclose the secret image progressively. At most,we can say that they proposed a multi-resolutionscheme via different approaches to share a secretimage. Their method expanded every secretpixel to a 3×3 block, and by using the pixelexpansionscheme, their shares will be furtherexpanded to 6×6 times larger, which causes asevere waste of storage and transmission time.

3. PROBLEM STATEMENT

Extended visual cryptography visual cryptography scheme for color image without pixel expansion.

4. REVIEW OF LITERATURE

1. Visual Cryptography for General Access Structure by Multipixel encoding with Variable Block Size:

Multi-pixel encoding [3] 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 presents a novel multi-pixel encoding which can encode variable number of pixels for each run. The length of encoding atone 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. Encrypting Informative Color Image using Color Visual Cryptography:

In this paper [4] Color visual cryptography is implemented in such a way that encryption will require shares and decryption is done with the help of naked human eye i.e. visual cryptography. The decryption is done directly by the human visual system with no special cryptographic calculations. Color visual cryptography uses 2 out of two secret sharing schemes which generate two shares for every input image to be encrypted. The original image is reconstructed by printing the two output shares onto transparencies and superimposing them together. This is X-OR operation between the shares to reveal the original information. The algorithm first generates RED, GREEN, BLUE as well as the ALPHA components of each pixel of an input image and these three components are used to generate the shares using 2 out of 2 secret sharing scheme. This scheme is useful in many applications like in securing information but not useful for visually blind people.

3.Extended Visual Cryptography Scheme For Color ImagesWith No Pixel Expansion:

An extension of VCS called Extended Visual Cryptography Scheme (EVCS) was alsointroduced. In an EVCS [5], besides generating n shares for a secret image, these n shares also carry n meaningful and independently chosen images. To generate these shares, a user arbitrarily chooses n meaningful

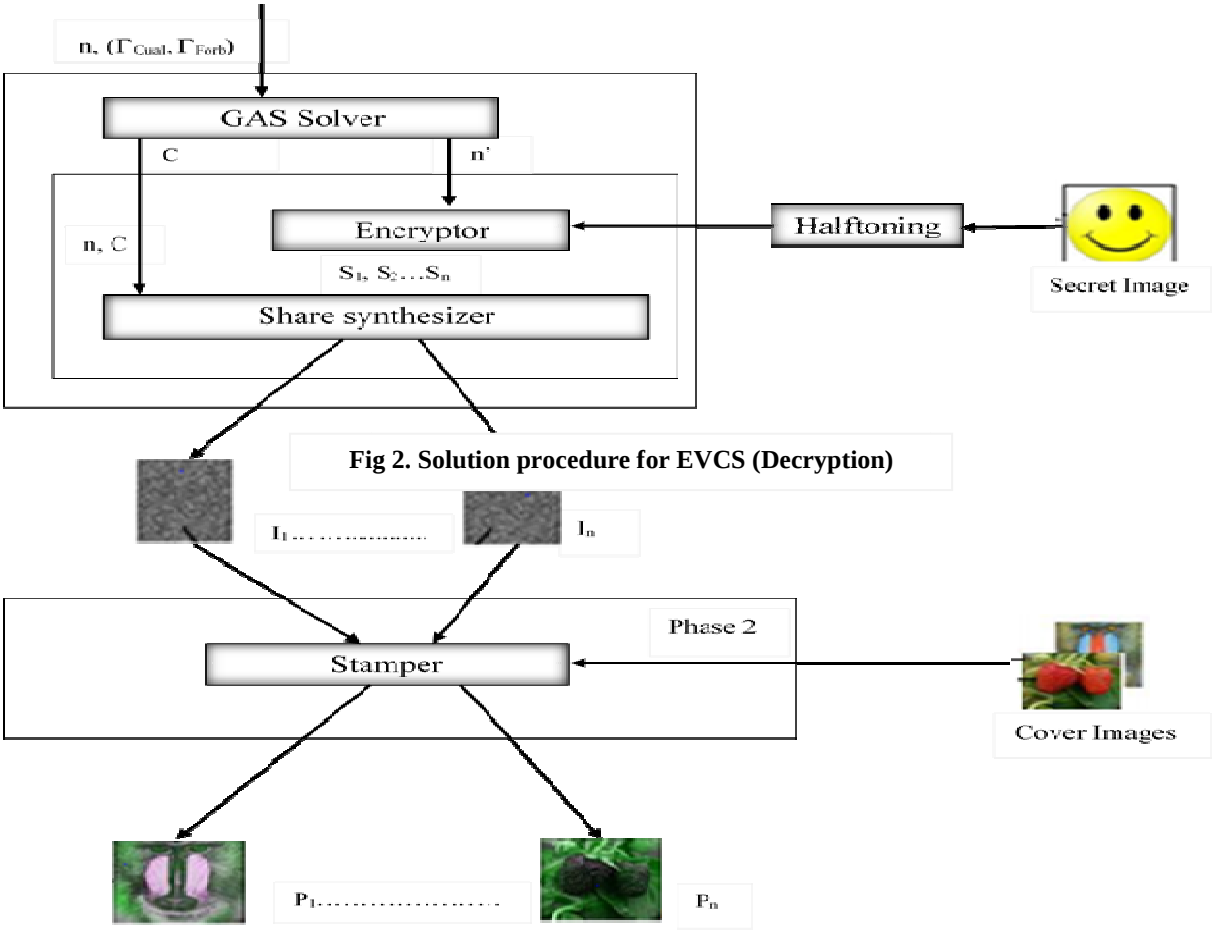
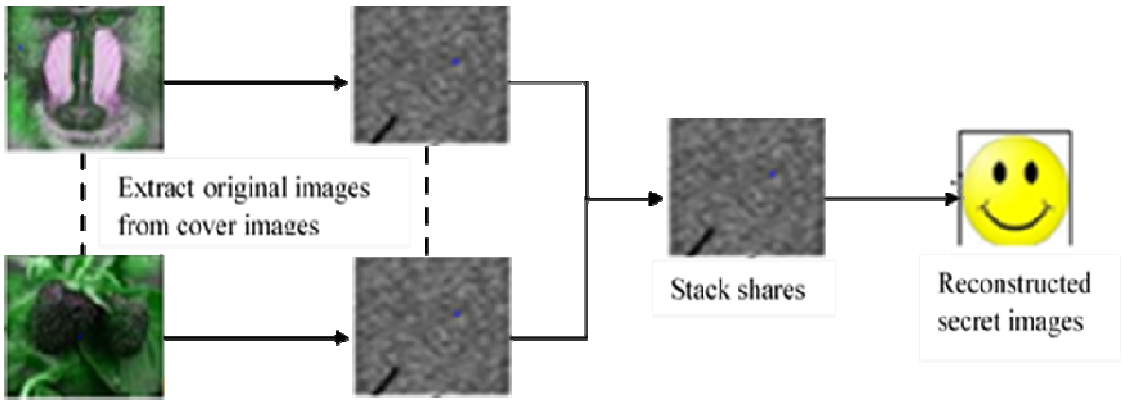


Fig 2. Solution procedure for EVCS (Decryption)

Fig 1. Solution procedure for EVCS (Encryption)

images which have the same size as the secret image. Then the user splits the secret image and embed the



share information into the n meaningful images in such a waythat given any k−1 or less shares, no information about the secret image can be obtained, while given any k or more shares, the secret image will be revealed when the shares are superimposed.The scheme is the first EVCS for color images with n pixel expansion. For a color secret image,suppose that n meaningful images have already been chosen. These images are color images chosen arbitrarily and will be used for generating n share images. Also, the choosing processing is totally

independent as long as the image size is the same as that of the secret image.
Since this scheme does not have any pixel expansion and scheme consists of the following steps:
1. Histogram Generation;
2. Color Quality Determination;
3. Grouping;
4. Share Creation.

5. PROPOSED SYSTEM

The main purpose of this is to avoid pixel expansion which occurred in previous researches, and provide higher security to image using the secrete General Access Structure (GAS) solver algorithm which first accept the image from user.

Step 1**:** Accept the image from user

Step 2: Convert into RGB image

Step 3: Histogram Generation

Step 4: Color Quality Determination

Step 5: Grouping

Step 6: Share Creation

Step 7: Transmission of share by cover images

Step 8: Decrypt

Step 9: Stack both share together

Step 10: Original image

6. CONCLUSION

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. It provides a safe and secure transmission as it involves multiple manipulations for encryption and decryption can be done at ease just with the naked eyes. This System provides a friendly environment to deal with color images which is not possible in VCS.
This application is aimed to support .gif and .png (portable network graphics) formatted images and the application would be developed using MATLAB, hence would provide a friendly environment tousers.

REFERENCES

[1] Adi Shamir, Massachusetts Institute ofTechnology “How to Share a Secret”,Communications of the ACM, Volume Number11, November 1979.
[2] Moni Naor, Adi Shamir: VisualCryptography. EUROCRYPT 1994: 1-12.
[3] Chavan, P.V.; Mangrulkar, R.S. “Encrypting Informative Color Image using Color Visual Cryptography” Emerging Trends in Engineering and Technology [ICETET] 3rd international conference,DOI:10.1109/ICETET.2010.94.
[4] M. Naor and A. Shamir, “Visual cryptography,” in Proc. Adv.Cryptol.:EUROCRYPT, vol. 950. 1995, pp. 1–12.
[5]Bert W.Leung, Felix Y.Ng, and DuncanS.Wong 2007.On the security of a Visualcryptography Scheme for Color Images (RGCRef. No. CityU 122107.
[6] Kai- Hui Lee and Pei-Ling Chiu, “Extended Visual Cryptography Algorithm for General Access Structure”, IEEE transaction on information forensics and security, vol 7 No.1, February 2012 pp.219-