A Novel Approach in Visual Cryptography

Saptagiri[1],M Ravikumar[2],D Venkanna[3]

[1,2,3] ECE Dept, Sree Dattha Institute of Engineering & Science

ABSTRACT: At the present time, in commercial, military and medical fields, the protections of susceptible information are most important concern. To resolve the reliability problems for secret images, a visual cryptography scheme is a good choice. Visual cryptography is a very protected and exclusive method to protect secrets. Visual cryptography is an encryption technique which is used to hide information which is present in an image.Unlike raditional cryptographic schemes, it uses human eyes to recover the secret without any complex decryption algorithms and with out facility of computers. It is a secret sharing scheme which uses images distributed as shares such that, when the shares are superimposed, a hidden secret image is revealed .In this paper we represent we represtnes the novel tachnique to hide secret information pixel into cover image with providing more visual quality of cover images compare to other technique.
Keywords: Secret image sharing, cryptography ,visual quality of image,pixel expansion

I. INTRODUCTION

1994, Naor and Shamir [1] introduced a very interesting and simple cryptographic method called visual cryptography to protect secrets (Naor and Shamir, 1995). Basically, visual cryptography has two significant features. The first aspect is its perfect concealment, and the second feature is its decryption method which requires neither complex decryption algorithms nor the aid of computers. It uses only human visual system to identify the secret from the stacked image of some approved shares[2]. Therefore, visual cryptography is an incredibly approach to keep secrets while computers or other decryption devices are not available.

(2, 2) visual cryptography scheme can be used to discuss fundamental visual cryptography.Senders create two layers. Basically pixel expansion may be 2, 4, 8 etc[3]. we have taken pixel expansion 2. That means one pixel of our original image is replaced by 2 pixels in share image. If the pixel is white the sender takes any row from the last two rows of Figure 1.2 randomly and if the pixel is black, the sender takes any row from the first two rows of Figure 1.2 randomly. By overlapping the two shares as shown in the last row of figure 1.2 randomly.

Fig.1.1-Construction of (2,2) VCS Scheme

For example, in below for encryption bvm.bmp as taken as input secret image. Instead of sending secret image we send two encrypted images and for decryption we just superimpose two images, we will get result [3]. All thought we will not get clear image but we can visually visualize the content.
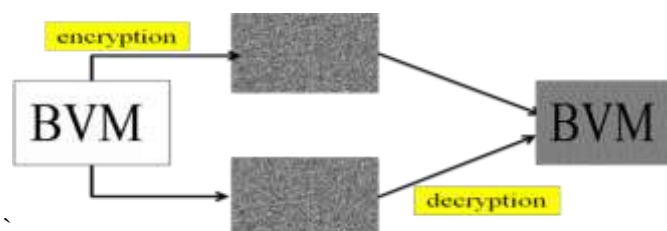

`
Fig 1.2 Example of (2,2) VCS scheme[3]

Visual cryptography is a method for fulfilling secret sharing activities in the environments with insufficient computing power [3]. Secure image sharing techniques overcome the traditional cryptographic approach, providing new solutions for the development of new and secure imaging applications.

The important parameters of this scheme are
a) Pixel expansion „m‟, which refers to the number of pixels in a share used to encrypt a pixel of the secret image. This implies loss of resolution in the reconstructed image[6].
b) Contrast „α‟, which is the relative difference between black and white pixels in the reconstructed image. This implies the quality of the reconstructed image[6].

The basic model of visual cryptography proposed by Naor and Shamir [1] accepts binary image „I‟ as secret image, which is divided into „n‟ number of shares. Each pixel of image „I‟ is represented by „m‟ sub pixels in each of the „n‟ shared images. The resulting structure of each shared image is described by Boolean matrix „S‟ Where S=[Sij] an [n x m] matrix Sij=1 if the jth sub pixel in the ith share is black Sij=0 if the jth sub pixel in the ith share is white When the shares are stacked together secret image can be seen but the size is increased by „m‟ times[6].
The grey level of each pixel in the reconstructed image is proportional to the hamming weight H(V) of the OR – ed Vector „V‟, where vector „V‟ is the stacked sub pixels for each original pixel[4].

II.HALFTONE VISUAL CRYPTOGRAPHY:
Zhi Zhou, Gonzalo R. Arce, and Giovanni Di Crescenzo [4] proposed halftone visual cryptography. Halftone VC is built upon the basis matrices and collections available in conventional VC. In particular, in halftone VC a secret binary pixel p is encoded into an array of Q1 x Q2 subpixels referred to as a *halftone cell*, in each of n the shares[4]. The pixel expansion in halftone VC is thus Q1Q2. Generally, a square halftone cell obtained when,Q1=Q2 leads to undistorted reconstructed images and .By using halftone cells with an appropriate size, visually pleasing halftone shares can be obtained [4].
As shown in below figure 2.1 , we can make three phase of this.In phase one we are converting our secret image into share of image by appling VC technique.In second phase we take one cover image which is grayscale image ,convert into binary image by appling Error Diffusion method[5]. In third Phase we are hiding our secret share image pixel into cover image.
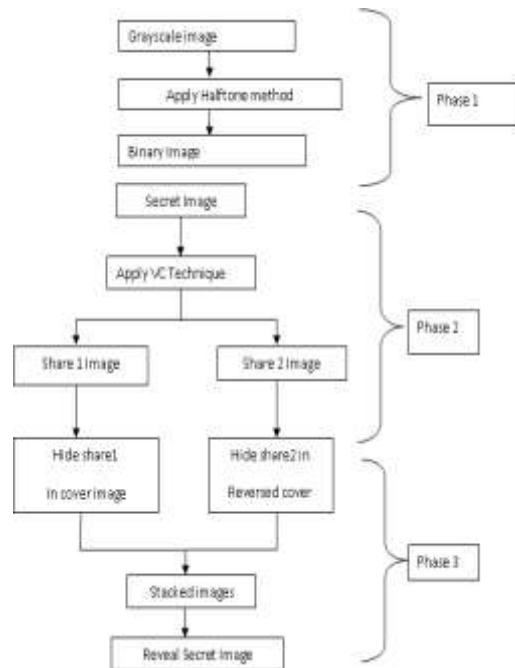

Fig 2.1 flow of halftone visual cryptography

III.PROPOSED TECHNIQUE
In the Basic technique when we are going to hide secret pixel into hafttone cell then, there are 2 pixel of the every halftone cell of cover image are change[5]. The reason is that we replacing cover image

pixel with secret share image pixel .So the quality of secret cover image is distordes, to overcome this problem we are use a novel technique. Table 3 Overview of new technique.

Table 3 overview of proposed technique

As shown in above table 3, suppose we want to hide secret pixels as shown in first row into 4 halftonn cell size of cover image.Here we are hiding our secret share pixels in to 1 and 3 number location of every halftone cell of cover image. As a result in every halftone cell pixels number 1 and 3 willl be replaced.to overcome this, we are findind secret image pixel pair in halftone cell and mark that pair location as a secret share image pixels locations. As a result, we are hiding share images pixels into cover image pixels with out distoring cover image pixels.so quality of cover image pixel will be increased.

IV.RESULT

As shown in below table 4, we have taken different bmp images which are our cover images then on cover images ,we are hiding secret share images with basic method and our new method. As we can see proposed technique results provide better visual quality.

Table 4 comparison Basic method and proposed method

IV.COMPARISION

Peak-Signal-to-Noise Ratio, which is the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. PSNR expressed in terms of logarithmic decibel scale which is an approximation to human perception of reconstruction quality. Higher PSNR generally indicates that the reconstruction is of higher quality.Here, in table 5, we are finding PSNR between original image and after hiding secret image into cover image. We compare PSNR between our method and basic method. As we can see our porposed method gives better PSNR.
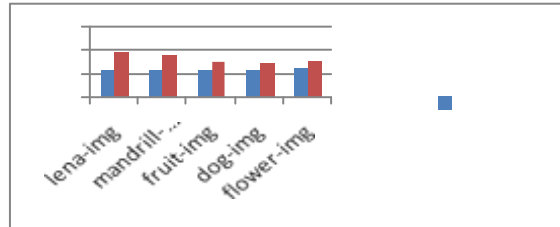
\

Table 5: comparison between basic method and our porosed method

V. CONCLUSION

In this paper introduction of visual cryptography is provided. This paper does gives antoher technique to hiding secret share images into cover image in halftone visual cryptography.As result says that by appling our proposed technique we can get better visual quality of cover images.

REFERENCES

[1]. Moni Naor and Adi Shamir, "Visual Cryptography", advances in cryptology– Euro crypt, pp 1-12, 1995.
[2]. J. B. Feng, H. C. Wu, C. S. Tsai, Y. F. Chang, and Y. P. Chu. "Visual secret sharing for multiple secrets". Pattern Recognition, 41:3572{3581,2008.
[3]. Prashant B swadas, Samip Patel,Dhruti Darji","A comparatively study of visual cryptography .,
[4]. IJRET vol-3
[5]. Z. Zhou, G. R. Arce, and G. D.Crescenzo, "Halftone visual cryptography,"IEEE Trans. Image Process.,vol. 18, no. 8, pp. 2441–2453,Aug. 2006.
[6]. Z. M. Wang, G. R. Arce, and G. Di Crescenzo, "Halftone visual cryptography via error diffusion," IEEE Trans. Inf. Forensics Security, vol. 4 pp 383–396, Sep.2009.
[7]. G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, "Visual cryptography for general access structures," Inf. Comput., vol. 129, no. 2, pp. 86–106, Sep. 1996.