IJETST- Vol.||02||Issue||12||Pages 3410-3414||December||ISSN 2348-9480 2015

Open access Journal International Journal of Emerging Trends in Science and Technology

DOI: http://dx.doi.org/10.18535/ijetst/v2i12.05

Securing Digital Images Using visual Cryptography

Authors
Kirti P. Sahare[1], Prof. S. A. Murab[2], Prof. M. V. Sarode[3], Prof. M. G. Ghonge[4]
[1]Dept of computer Engg, Amravati University, Amravati
Email: *Kirtisahare4u@rediffmail.com*
[2]Dept of computer Engg, Amravati University, Amravati
Email: *Sachinmurab21@gmail.com*
[3]Dept. of Computer Engg, Amravati University, Amravati
Email: *Mvsarode2013@gmail.com*
[4]Dept. of Computer Engg, Amravati University, Amravati
Email: *Mangesh.cse@gmail.com*

Abstract:
Visual cryptography technique allows the visual information to be encrypted in such a way that their decryption can be performed by human visual system. Security has become an inseparable issue as Information Technology is ruling the world now. Cryptography in the study of mathematical techniques related aspects of information security such as confidentialities, data security, entity authentication, but it is not only the means of providing information security, rather one of the techniques. Visual cryptography can be applied for copy right for images, access control to user images ,visual authentication and identification any kind images of images like(normal or digital).Visual cryptography is a new technique which provides information security which user simple algorithm unlike the complex, computationally intensive algorithms used in other techniques like traditional cryptography. This technique allows visual information (pictures, text, etc)to be encrypted in such a way that their decryption can be performed by the human visual system, without any complex cryptographic algorithms. This technique encrypts a secret image into shares such that stacking sufficient number of shares reveals the secret image. Shares are visually presented in transparencies.

Keywords: *Pixels, Contrast, Secret sharing, Shares.*

INTRODUCTION

Now a day's security plays a vital role in every field. So to provide protection to images we use visual cryptography for encryption and decryption. When we transfer images from sender to receiver image can't be hacked in medium channel. There are various visual cryptography types which can be used to provide security. In classical cryptography there are two methods. One of them is symmetric key cryptography, where same key will be used for encryption as well as decryption also, but will be used in opposite manner. Another method is asymmetric key, where encryption will be done using public key which may be known to all but decryption will be done by private key that is known to the user/receiver only. The basic idea of cryptography is that the computation process should be complex enough such that nobody i.e. the intruder will be able to break the system. In 1994, Naor and Shamir introduced first time securing data without cryptographic computation, termed as Visual Cryptography (VC). It exploits human visual system to read messages from some overlapping shares, which reduces the computational overhead that is the disadvantage of complex computation in classical cryptography. 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. Visual cryptography does not need any special decryption algorithm, the secret image can be decrypted by necked eyes. Visual Cryptography is necessary for security purpose, while sending confidential information over air.

Background

Various watermarking schemes are available based on Visual Cryptography [5]–[9]. Most of them [5], [7] convert the gray-level host images into two-tone images, using halftone techniques before embedding a binary watermark.

Hwang proposed a scheme[6] which hides binary watermarks in grey-level images directly. Hwang's watermark is based on simple (2, 2) VC scheme. In his method a secret key is used as a seed to select random pixels within the host image. The most significant bits of the selected pixels are used to form the first share, known as Verification Share. Then the binary watermark and the first share are combined to generate the second share, known as Master Share using the principles of (2, 2) VC. The Master Share must be registered with a trusted third party. While resolving the rightful ownership, the same secret key is to be used as a seed, to select the most significant bits of the modified image. The resulted Verification Share and the Master Share are combined to recover the hidden watermark. The Hwang's scheme doesn't provide security always. For example, if 90% of the pixels in the host image have gray-levels greater than 128, then 90% of the most significant bits will have the value as logic1, regardless of the secret key. The Verification Share is revealed without the knowledge of the secret key, indirectly. This drawback of Hwang's scheme makes it unsuitable for digital image copyright protection. This paper proposes a watermarking scheme that overcomes the drawbacks of Hwang's scheme and offers better security.

Disadvantage of Basic Watermarking

- Selection of pixels is random, when restored watermark pattern from image.
- An image with some similarities with the original image M, watermark pattern p should be restored the image.

Hwang proposed method to overcome basic technique for selecting specific pixels from the original image instead of random selection of pixels. The user will select watermark pattern p which specify image, user can characterize an image M using the watermark pattern and the expanded key S. pk represents the length of the watermark pattern P, Mk represents the length of the image M and M′k represents the length of the image M′.

The method uses different steps to assign the length key and verification of ownership of image.

Types of Visual Cryptography

Simple working of VCS is that the transparencies (shares) of the image is created and in one of the transparency the secret image is hidden. But to encrypt the secret we need both the transparency, without any of them we can't reveal the secret image.

There are various types of visual cryptography based on black & white and colour images.

VC on Black & White image:

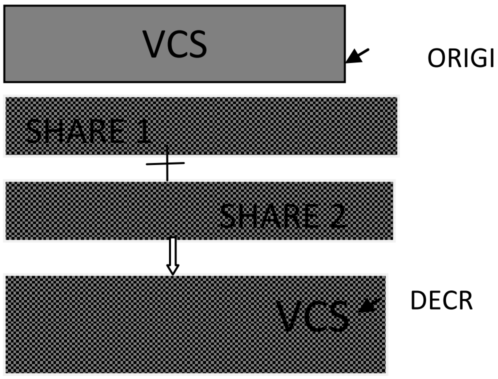

Fig. 1 example of VC of black and white image

VCS of colour image:

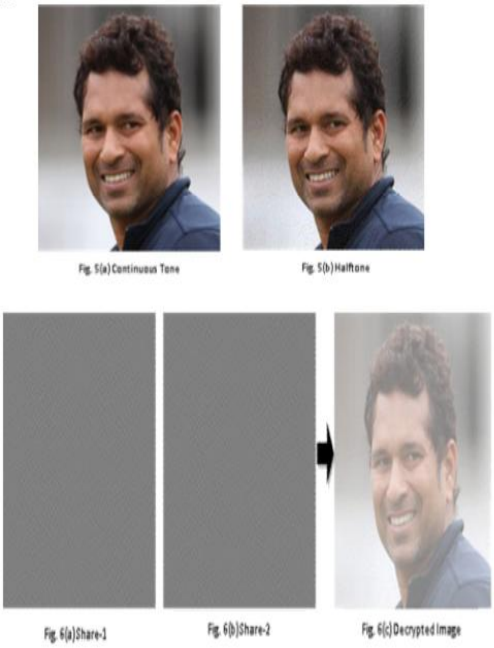

Fig. 2 example of VC OF colour image

Joint visual cryptography

Joint Visual Cryptography (VC) was first introduced by Noar and Shamir at Eurocrypt'94 [4]. To encode a secret employing a (2, 2) VC Scheme, the original image is divided into two shares such that each pixel in the original image is replaced with a non-overlapping block of two sub-pixels. Anyone who holds only one share will not be able to reveal any information about the secret. To decode the image, each of these shares is xeroxed onto a transparency. Stacking both these transparencies will permit visual recovery of the secret. Table 1 illustrates the scheme of encoding one pixel in a (2, 2) VC scheme. A white pixel is shared into two identical blocks of sub-pixels. A black pixel is shared into two complementary blocks of sub-pixels. While creating the shares, if the given pixel *p* in the original image is white, then the encoder randomly chooses one of the first two columns of Table 1. If the given pixel *p* is black, then the encoder randomly chooses one of the last two columns of Table 1. Each block has half white and half black sub-pixels, independent of whether the corresponding pixel in the secret image is black or white. All the pixels in the original image are encrypted similarly using independent random selection of columns. Thus no information is gained by looking at any group of pixels on a share, either

Table 1. A (2, 2) Visual Cryptography Scheme

Pixel	White □		Black ■	
Prob.	50%	50%	50%	50%
Share1	◧	◨	◧	◨
Share2	◧	◨	◨	◧
Stack Share1&2	◧	◨	■	■

Figure 3 shows the results of basic (2, 2) VC Scheme. When the two shares are stacked together, as in Figure 1(d), the black pixels in the original image remain black and the white pixels become gray. Although some contrast loss occurs, the decoded image can be clearly identified. Since each pixel in the original image is replaced by two sub-pixels in each share, the width of the decoded image is twice that of the original image.

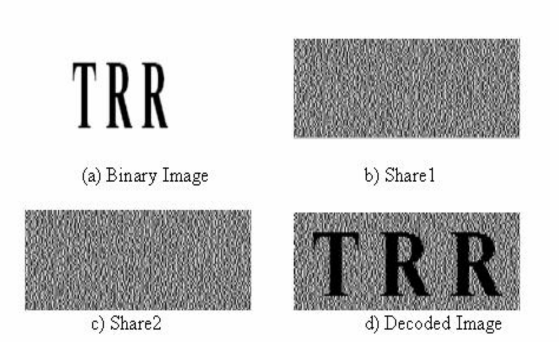

Figure 3. Example of (2, 2) Visual Cryptography Scheme

Colour Visual Cryptography

There are some researches that deal with visual cryptography for colour images. In this section, we will explore several representative work over the years.[3] discussed the visual cryptography scheme which reconstructs a message with two colours, by arranging the coloured or transparent sub pixels, they only discussed construction of (k,n)-threshold scheme where a subset X 2 is a qualified set if and only if |X| = k. Koga et al. devised a lattice based (k, n) scheme [4]. The approach by [5] is basically similar to Koga's. Both approaches assign a colour to a sub pixel at a certain position, which means that displaying m colours uses m−1 sub pixels. The resulting pixels contain one colouredsub pixel and the rest of the sub pixels are black. Therefore the more colours are used, the worse the contrast of the images becomes significantly. Their approaches cannot be applied to the extended visual cryptography, either. Rijmen and Preneel talked about enabling multicolours with relatively less sub pixels (24 colours with m = 4) [6]. However each sheets must contain colour random images, which means applying this approach to the extended visual cryptography is impossible.[7]

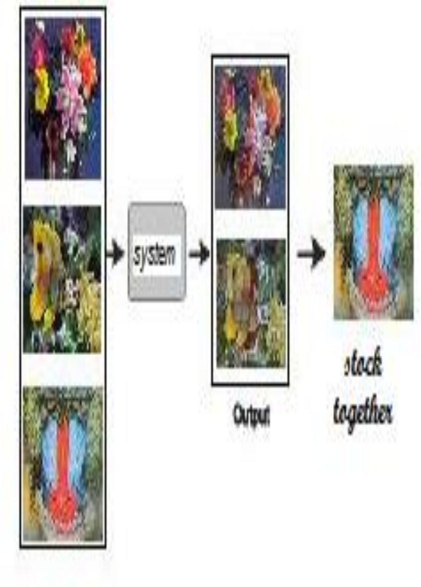

Fig. colour visual cryptography.

Application of visual cryptography

1. Watermarking
2. Biometric security
3. Steganography
4. Remote electronic voting
5. Bank customer identification

FUTURE WORK

The future work is to improve the contrast and produce more clearly the resultant secret image. Further extend this work to use this technique with to he format of colour images. Also consider 3D images for creating the shares that have partial secret and reveal that secret by stacking to each other. In reality, however, such ideal subtractive colour mixture is unlikely due to the properties of ink, transparencies, etc. It needs to establish a sophisticated colour mixing model for the extended visual cryptography with better colour quality.

CONCLUSION

This paper discusses the introduction of different types of Visual Cryptography schemes. It compares the image quality and security using various visual cryptography schemes. In order to hide the secrecy we go for expansion and increasing of the number of shares, but this affects the resolution. Therefore an optimum number of shares are required to hide the secrecy. At the same time security is also an important issue. Hence research in visual cryptography (VC) is towards maintaining the contrast at the same time maintaining the security

REFERENCES

1. Zhongmin Wang, Gonzalo R. Arce, and Giovanni Di Crescenzo, “Halftone Visual Cryptography Via Error Diffusion,” IEEE Transactions on Information Forensics and Security, vol. 4, no. 3, September 2009
2. M. Naor and B. Pinkas, “Visual authentication and identification,” Crypto97, LNCS, vol. 1294, pp. 322–340, 1997.
3. Zhou, G. R. Arce, and G. Di Crescenzo, “Halftone Visual Cryptography,” IEEE transactions on Image Processing, to appear in 2006.
4. M. Naor and A. Shamir, “Visual Cryptography,” in Proceedings of Euro crypt 1994, lecture notes in Computer Science, 1994, vol. 950, pp. 1–12.
5. A. Bonnis and A. Santis, “Randomness in secret sharing and visual cryptography schemes,” Theory. Computer. Science, 314, pp 351- 374 (2004).
6. E.Myodo, S. Sakazawa, Andy. Takishima, “Visual cryptography based on void-and-

cluster half toning technique," in Proc. IEEE ICIP, Atlanta, GA, Oct. 2006.

7. R. Hwang, "A digital Image Copyright Protection Scheme Based on Visual Cryptography," Tambang Journal of science and Engineering, vol.3, No.2, pp. 97-106 (2000).
8. M. Naor and B. Pinkas, "Visual authentication and identification," Crypto97, LNCS, vol. 1294, pp. 322–340, 1997.
9. M. Nakajima and Y. Yamaguchi, "Extended visual cryptography for natural images," J. WSCG, vol. 10, no. 2, pp. 303–310, 2002.
10. R. A. Ulichney, "The Void-and-cluster Method for Dither Array Generation," in Proc. of SPIE, HumanVision, Visual Processing, Digital Displays, 1996, vol.1913.
11. Z. Zhou, G. R Arce, and G. Di Crescenzo, "Halftone Visual Cryptography," in Proc. of IEEE International Conference on Image Processing, Barcelona, Spain,Sept 2003, vol. 1, pp. 521–52
12. Hiroki Koga and Hirosuke Yamamoto, 1998. *Proposal of a lattice-based visual secret sharingscheme for color and gray-scale images*. IEICE Transaction on Fundamentals, E81-A(6):1262– 1269.