Volume 5, Issue 5, May 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Review Paper

Available online at: www.ijarcsse.com

A Survey: Novel Study for Visual Cryptography in Discrete Wavelet Transforms

Nazimul Islam
Mtech Scholar
Department of ECE
PDM College of Engineering
MDU, Rohtak (Haryana), India

Shaloo Kikan
Assistant Professor
Department of ECE
PDM College of Engineering
MDU, Rohtak (Haryana), India

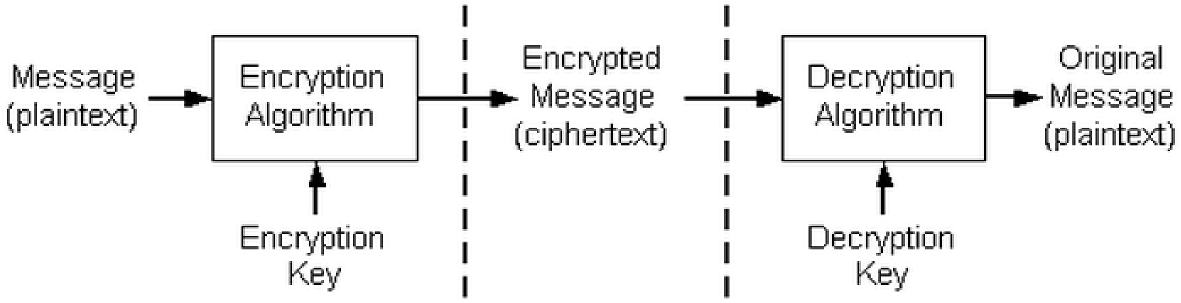
Abstract: Visual Cryptography Scheme (VCS) is an encryption method that uses combinatorial techniques to encode secret written materials. The idea is to convert the written material into an image and encode this image into n shadow images. The decoding only requires only selecting some subset of these n images, making transparencies of them, and stacking them on top of each other. In this survey paper, we will provide the readers an overview of the basic VCS constructions, as well as several extended work in the area. In addition, we also review several state-of-art applications that take full advantage of such simple yet secure scheme.

Keyword: VCS, Half-toned, encrypt & decrypt etc.

I. INTRODUCTION

Visual cryptography is introduced by first in 1994 Noar and Shamir [1]. Visual cryptography is a cryptographic technique which allows visual information (e.g. printed text, handwritten notes and pictures) to be encrypted in such a way that the decryption can be performed by the human visual system, without the aid of computers.

Encrypted data can be stored on non-secure media or transmitted over a non-secure network. Later, the data can be decrypted into its original form. This process is shown in the following illustration.



When data is encrypted, the message and an *encryption* key are passed to the encryption algorithm. To decrypt the data, the ciphertext and a *decryption* key are passed to the decryption algorithm. Encryption and decryption can be done by using a single key in a process called symmetric encryption.

Visual cryptography scheme eliminates complex computation problem in decryption process, and the secret images can be restored by stacking operation. This property makes visual cryptography especially useful for the low computation load requirement. Various confidential data 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, various image secret sharing schemes have been developed.

This paper provides overview of various visual cryptography schemes. Taking limited bandwidth and storage into consideration two criteria pixel expansion and number of shares encoded is of significance. Smaller pixel expansion results in smaller size of the share. Encoding multiple secret images into the same share images requires less overhead while sharing multiple secrets.

II. LITERATURE SURVEY

M. Naor and B. Pinkas [2], describe the visual authentication and visual identification methods which are the methods for human users based on visual cryptography. These methods are very natural and easy to use and can be implemented using very common “low tech” technology. The advantages of this system are that the physical requirements are linear in the size of the message and logarithmic in the fault probability p.

Extended visual cryptography scheme (EVCS) is kind of visual cryptography scheme first introduced by Naor in [3].EVCS consist of meaningful shares and VCS consist of random shares. Input to EVCS is secret image and n original shares images. re meaningful images hence these shares are less suspicious. Limitation of EVCS is bad visual quality of the shares and recovered secret image. Another limitation is that pixel expansion is large and requires complementary share images. Embedded EVCS is a visual cryptography scheme proposed by **Feng Liu and ChuankunWu[3].**

Chin Chen chang, Min- Shian Hwang, and Tung ShouChen[5] have proposed a fast encryption algorithm for image cryptosystems in 2001. Vector Quantization, cryptography and other number theorem is the main platform for this cryptosystems.VQ is an useful technique to low bit rate image compression. In VQ first decomposition of images into vectors takes place and then vector by vector then are sequentially encoded.

Young-Chang Hou[6] have presented a technique for visual cryptography of color images in 2002 which consist of three methods for visual cryptography of gray-level and color images based on past studies in black and white visual cryptography, the halftone technology method, and the color decomposition method. His technique gives us backward compability with the ols results in black and white VS along with advantages of black and white VS which is very helpful visual system to decrypt secret image without computation like t out of n threshold scheme which can be applied to gray level and colorful images

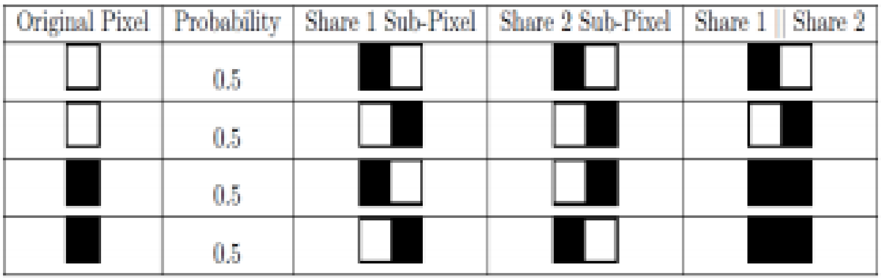
III. DISCUSSION

VARIOUS VISUAL CRYPTOGRAPHY SCHEMES

1. (2, 2) Visual Cryptography Scheme

In (2, 2) Visual Cryptography Scheme, original image is divided into 2 shares. Each pixel in original image is represented by non-overlapping block of 2 or 4 sub-pixels in each share. Anyone, having only one share will not be able to reveal any secret information. Both the shares are required to be superimposed to reveal the secret image [3]

There are many techniques for encoding the pixels of original image. In a technique, in which each pixel in original image is represented by two sub-pixels in each share, while reading the pixels in original image, if a white pixel is encountered, one of the first two rows in Figure 1 is selected with probability 0.5, and the shares are assigned 2 pixel blocks as shown in the third and fourth columns in figure 1. Similarly, if a black pixel is encountered, one of the last two rows is selected with probability 0.5, from which a sub-pixel block is assigned to each share. When two shares are superimposed, if two white pixels overlap, the resultant pixel will be white and if a black pixel in one share overlaps with either a white or black pixel in another share, the resultant pixel will be black. This implies that the superimposition of the shares represents the Boolean OR function. The last column in Figure 1 shows the resulting sub-pixel when the sub-pixels of both the shares in the third and fourth columns are superimposed [3].



Original Pixel	Probability	Share 1 Sub-Pixel	Share 2 Sub-Pixel	Share 1 || Share 2
□	0.5	■□	■□	■□
□	0.5	□■	□■	□■
■	0.5	■□	□■	■■
■	0.5	□■	■□	■■

Figure 1: 2 out of 2 using 2 sub pixel per original pixel

2. Halftone Visual Cryptography

In this paper, a novel technique named halftone visual cryptography is proposed to achieve visual cryptography via halftoning. Based on the blue-noise dithering principles, the proposed method utilizes the void and cluster algorithm [2] to encode a secret binary image into halftone shares (images) carrying significant visual information. The simulation shows that the visual quality of the obtained halftone shares is observably better than that attained by any available visual cryptography method known to date.

3. Visual Cryptography for scan and print applications

The shares of visual cryptography are printed on transparencies which need to be superimposed. However, it is not very easy to do precise superposition due to the fine resolution as well as printing noise. Furthermore, many visual cryptography applications need to print shares on paper in which case scanning of the share is necessary. The print and scan process can introduce noise as well which can make the alignment difficult. In this paper, we consider the problem of precise alignment of printed and scanned visual cryptography shares. Due to the vulnerabilities in the spatial domain, we have developed a frequency domain alignment scheme.

4. Recursive Threshold visual cryptography

The (k,n) visual cryptography explained in section I needs „k‟ shares to reconstruct the secret image. Each share consists at most [1/k] bits of secrets. This approach suffers from inefficiency in terms of number of bits of secret conveyed per bit of shares. Recursive threshold visual cryptography proposed by Abhishek Parakh and Subhas Kak [4] eliminates this problem by hiding of smaller secrets in shares of larger secrets with secret sizes doubling at every step. When Recursive threshold visual cryptography is used in network application, network load is reduced.

IV. CONCLUSION

In this paper, we briefly reviewed the literature of visual cryptography schemes. This paper provides a review on various visual cryptography techniques. The visual cryptography (VC) scheme techniques can decode concealed images without cryptography techniques Currently, many new schemes are proposed in the field of Color Visual Cryptography. We have seen that all the schemes discussed above, use Naor and Shamir's basic model of visual cryptography as the basis. But at the same time, the shares produced by all the methods above are either meaningless or are dependent upon some factors like the number of colors in the secret image. Compared with existing schemes, the proposed scheme i.e. wavelet based can effectively minimize transmission risk and provide the highest level of user friendliness, both for shares and for participants.

REFERENCES

[1] MoniNaor and Adi Shamir, "Visual Cryptography", advances in cryptology– Eurocrypt, pp 1-12,1995.

[2] M. Naor and B. Pinkas, "Visual authentication and identification," Springer-Verlag LNCS, vol. 1294,

[3] F. Liu and C. Wu, "Embedded extended visual cryptography schemes" , IEEE Trans. Inf. Forensics Security, vol. 6, no. 2, pp. 307–322, Jun.2011pp. 322–336, 1997.

[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] Chin chenChang,MinShian Hwang and Tung Shou Chen," A new image encryption algorithm for image cryptosystems",the journal of system and software 58(2001.

[6] Young-ChangHou" Visual cryptography for color images" Pattern Recognition 36 (2002) .