Design of XOR based visual cryptography scheme

Gayathri D[1], Dr T Gunasekran [2]

[1] PG scholar, Dept of ECE, Vivekananda College of Engineering for Wome.,

[2]Professor, Dept of ECE, Vivekananda College of Engineering for Women.

***Abstract*— In today's communication, security is the major issue the visual based cryptography scheme encodes the secret images into n shadow images which is distributed among n participants. The OR based VCS has the transparencies and it is easily viewed by human visual system. The OR based VCS has computation free decoding process. And also it degrades the contrast by its monotone property. So the XOR operation was proposed in decoding process to enhance the contrast.**

***Index terms*: VCS, Image secret sharing, visual secret sharing.**

I. INTRODUCTION

It is now common to transfer multimedia data via the Internet. With the coming era of electronic commerce, there is an urgent need to solve the problem of ensuring information safety in today's increasing open network environment. The encrypting technologies of traditional cryptography are usually used to protect information security. With such technologies the data become disordered after being encrypted and can then be recovered by a correct key. Without the correct key, the encrypted source content can hardly be detected even though unauthorized persons steal the data.

The simplest model of visual secret sharing problem assumes the message consists of the collection of black and white pixels and each pixel is handled separately. Each pixel is in n modified version as shares. Each share is a collection of m black and white pixel and they are printed close to each other so that the human visual system averages their individual black/white contributions.

The idea of using visual cryptography is for security. An image is split into two random shares which separately reveal no information on the original image. The original image can be reconstructed by superimposing the two shares. The visual crypto systems can be made unconditionally secure; they are not satisfactory from a practical point of view. Because of the One Time Pad property, a key can be used only once. Since transparencies are static objects, a user has to carry a pile of transparencies with him to update the keys and the physical properties (color, resolution, and contrast) make the system not very well suited for practical purposes.

VCS has poor visual quality of a reconstructed image. Another polynomial-based secret image sharing scheme can recover a distortion-less secret image, but its decoding needs Lagrange interpolation. The authors combined VCS and polynomial-based secret image sharing to design and develop a two-in-one VCS with different decoding options. In this two-in-one VCS, the first phase is stacking to see a vague reconstructed image like VCS, and the second phase is to perfectly reconstruct the secret image by Lagrange interpolation. The stacking operation in VCS is OR operation, and thus the conventional VCS is also referred to as OR-based VCS (OVCS). To enhance the visual quality, some XOR-based VCSs (XVCSs) allowing participants to perform XOR operations.

II. VISUAL SECRET SHARING WITH HALF REDUCTION OF SHADOW SIZE

The size reduced VSS using the deletion of some columns in the black and white matrices, but the scheme did not work for reducing the shadow size of (k, k) VSS schemes. An extreme size-reduced VSS scheme with no pixel expansion was first introduced. Both size reduced VSS and probabilistic concepts have no pixels expansion but recover the poor-quality secret image. Generalizations of the probabilistic model with any pixel expansion were also given for the pixel expansion with the contrast. Handling group of pixels, instead of each pixel separately yields better results. The half reduction of shadow size was achieved by processing of two-pixeled blocks every time[1].

ISSN: 2278 – 909X

The basic concept is to process a two pixeled block each time, by four corresponding sets $C1$, $C00$, $C10$ and $C01$. The first two sets are the contrast of the recovered image, while the last two sets determine the clearness of edges between black and white areas. Where 1 and 0 represents the black and white pixels respectively. If the stacked patterns V are not the same then it will lack consistency and the edge is irregular.

The pixel expansion is reduced by half this causes the line disappearance problem. To solve the thin line disappearance problem, there is always one black sub pixel in the left of the stacked result in $C10$ set for two-pixeled block (01), and one black sub pixel in the right of the stacked result in for two-pixeled block (10). Thus, we do not have the line disappearance. But in this method the reconstructed image has little irregular edges.

III. PROBABILISTIC VISUAL SECRET SHARING SCHEME

In Visual Secret Sharing pixel expansion is the major issue. A number of probabilistic VSS schemes with minimum pixel expansion is for binary secret images. The general probabilistic (k,n)-VSS scheme is for grey-scale images and another scheme for color images. In this method the pixel expansion can be set to a user-defined value. When this value is 1, there is no pixel expansion at all. The quality of reconstructed secret images, measured by average contrast or by average relative difference is equivalent to the contrast of existing deterministic VSS schemes[2].

Previously the probabilistic scheme is only used for binary images. A probabilistic (2,n) secret sharing scheme for binary images based on Boolean XOR and AND operations. The binary (2,n)-secret sharing scheme has been extended to grey-scale image and color image (2,n)-VSS schemes. The pixel expansion of our schemes is from 1 (no pixel expansion) to a user-specified value. The quality of the reconstructed image, measured in terms of contrast is the same as the conventional deterministic VSS schemes. This technique can be used to extend almost any existing deterministic VSS schemes to Probabilistic VSS schemes.

IV. VISUAL CRYPTOGRAPHY FOR COLOR IMAGE

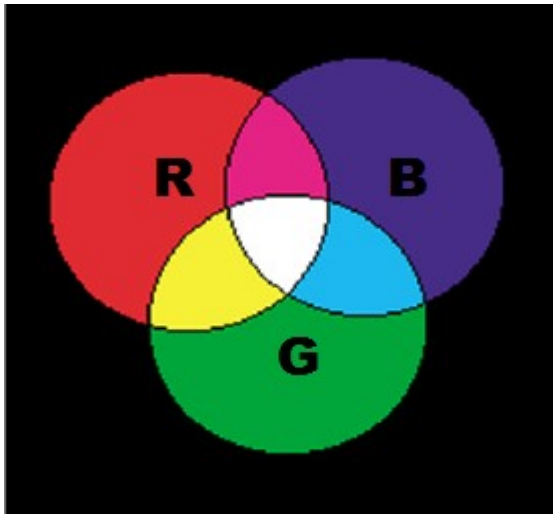
Visual cryptography for color image combines the previous results in visual cryptography, the halftone technology, and the color decomposition principle to develop algorithms of visual cryptography for gray-level and color images. This method retains the advantage of traditional visual cryptography, namely, decrypting secret images by human eyes without any cryptography computation. For information security, it also ensures that hackers cannot perceive any clue about the secret image from any individual sharing image.

Visual cryptography methods not only retain the advantages of black-and-white visual cryptography, which exploits the human visual system to decrypt secret images without computation, but also have the backward compatibility with the previous results in black-and-white visual cryptography, such as the t out of n threshold scheme, and can be applied to gray-level and color images easily.

Each pixel of the color secret image is expanded into a 2×2 block to form two sharing images. Each 2×2 block on the sharing image is filled with red, green, blue and white (transparent), respectively, and hence no clue about the secret image can be identified from any one of these two shares alone.

The additive and subtractive models (Fig. 1 & 2) are commonly used to describe the constitutions of colors. In the additive system, the primaries are red, green and blue (RGB), with desired colors being obtained by mixing different RGB components. By controlling the intensity of red (green or blue) component, we can modulate the amount of red (green or blue) in the compound light.

When mixing all red, green and blue components with equal intensity will results in white color[3].



ISSN: 2278 – 909X

Fig 1 Additive model

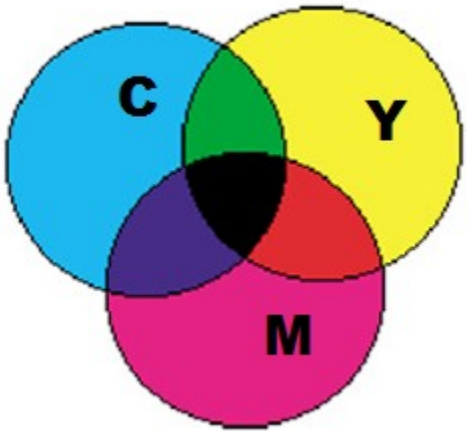


Fig 2 Subtractive model

The more the pigment we add, the lower is the intensity of the light, and thus the darker is the light. This is why it is called the subtractive model. C, M and Y are the three primitive colors of pigment, which cannot be composed from other colors. The color printer is a typical application of the subtractive model.

V. THE HALFTONE TECHNOLOGY

According to their physical characteristics, different media use different ways to represent the color level of images. The computer screen uses the electric current to control the lightness of the pixels. The diversity of the lightness generates different color levels. The general printer, such as dot matrix printers, laser printers, and jet printers, can only control a single pixel to be printed (black pixel) or not to be printed (white pixel), instead of displaying the gray level or the color tone of an image directly[4]. As such, the way to represent the gray level of images is to use the density of printed dots; for example, the printed dots in the bright part of an image are sparse, and those in the dark part are dense.

The method that uses the density of the net dots to simulate the gray level is called "Halftone" and transforms an image with gray level into a binary image before processing. Take the gray-level image and the every pixel of the transformed halftone image has only two possible color levels (black or white). Because human eyes cannot identify too tiny printed dots and, when viewing a dot, tend to cover its nearby dot and simulate different gray levels through the density of printed dots, even though the transformed image actually has only two colors black and white.

VI. SYMMETRIC KEY VISUAL CRYPTOGRAPHY

A block based symmetry key visual cryptography algorithm converts image in encrypted form and decrypt the encrypted image into original form. The symmetric key has been generated from a real number. The encryption and decryption algorithm have been designed based on symmetry key. The algorithm with key has been used to encrypt image into single share and decrypt the single share into original image. The real number has been used to form the key may be predefined or may be sent by secure channel to the receiver. The symmetric key algorithm can be applied to any type images i.e. binary, gray scale and color images.

The basic approach was to split the image into 2 shares are generated from the original secret image and by stacking together the secret is reveal. This approach was restricted in binary images which is insufficient in real time applications. Instead of using gray sub pixels directly to constructed shares, a dithering technique is used to convert gray level images into approximate binary images. The limitation lies in the fact that all shares are inherently random patterns carrying no visual information, raising the suspicion of data encryption.

This algorithm was used in visual cryptography without using share concept. The input image has been encrypted by image element and key value. The distribution of image gray values are in such a way that the encrypted image has been treated as single share. The encrypted image has been decrypted by same proposed algorithm. The key has been generated automatically by using a number. The value of the number has been taken from 0 to 1. This value can be pre - agreement between the sender and receiver or it can be sent by any secret means to the receiver. The result of this approach is much more secure and less bandwidth consuming.

VII. PROPOSED WORK

VCS has poor visual quality of a reconstructed image. Another polynomial-based secret image sharing scheme can recover a distortion-less secret image, but its decoding needs Lagrange interpolation. The authors combined VCS and polynomial-based secret image sharing to design and

ISSN: 2278 – 909X

develop a two-in-one VCS with different decoding options. In this two-in-one VCS, the first phase is stacking to see a vague reconstructed image like VCS, and the second phase is to perfectly reconstruct the secret image by Lagrange interpolation. The stacking operation in VCS is OR operation, and thus the conventional VCS is also referred to as OR-based VCS (OVCS). To enhance the visual quality, some XOR-based VCSs (XVCSs) allowing participants to perform XOR operations were accordingly proposed.

The XOR schemes have the good contrast property. Actually, their operations can be mathematically represented by the XOR operation. A completely different kind of VCS with reversing was proposed allowing participants to perform reversing operation, which can change black pixels to white pixels and vice-versa. This reversing operation (NOT operation) can be realized by a copy machine. By this reversing-based VCS, one can perfectly reconstruct the secret by more runs. Because XOR operation can be implemented by four NOTs and three ORs XOR operation can be realized by using a copy machine and transparency.

VIII. CONCLUSION

The OR operation causes that black sub pixel in a shadow cannot be undone by the color of another sub pixel laid over it. Therefore, the OVCS cannot obtain the pure white whiteness (a white pixel is represented by *m* white sub pixels), while it may be achieved by XOR operation. The two-in-one VCS need Lagrange interpolation for decoding in the second decoding phase, but XVCS only needs the simple logical XOR operation. The contrast of XVCS is $2(k-1)$ times greater than OVCS.

REFERENCES

[1] H. Kuwakado and H. Tanaka, "Size-reduced visual secret sharing scheme," *IEICE Trans. Fundamentals Electron. Commun. Comput. Sci.*, vol. E87-A, no. 5, pp. 1193–1197, May 2004.
[2] D. S. Wang, F. Yi, and X. Li, "Probabilistic visual secret sharing schemes for gray-scale images and color images," *Inform. Sci.*, vol. 181, no. 11, pp. 2189–2208, 2011.
[3] J.C. Hou, "Visual cryptography for color images," *Pattern Recognit.*, vol. 36, no. 7, pp. 1619–1629, Jul. 2003.
[4] C.C. Lin and W.H. Tsai, "Visual cryptography for gray-level images by dithering techniques," *Pattern Recognit. Lett.*, vol. 24, pp, 349–358, Jan.2003.

Authors Profile

Ms D.GAYATHRI, Completed Under Graduate in Electronics and Communication Engineering from Mahendra College of Engineering ,Salem in 2012. She is currently pursuing Master of Engineering in VLSI Design in Vivekanandha College of Engineering for Women. Her area of interest includes Networks and VLSI Design.

Dr T GUNASEKAREN, received his Bachelors Degree in Electronics and Communication Engineering from Kongu Engineering College, Erode in 2000. He completed his Master Degree in Communication Engineering from Birla Institute of Technology and Science (BITS), Pilani, Rajasthan in 2003.He obtained his Doctorate in Micro strip Array Antennas ,in Anna University, Chennai in 2013. Presently, he is working as HOD in ECE of Vivekananda College of Engineering for Women. His area of interest is Microwave Antenna and Digital Signal Processing.
.

ISSN: 2278 – 909X