IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 11, November 2015

Visual Cryptography with Color Error Diffusion and Digital Watermarking

Prof Akhil Anjikar[1], Prof. Rahul Bambodkar[2]

Assistant Professor, Information Technology, RGCER, Nagpur, India [1]

Assistant Professor, Computer Science & Engineering, DMIETER, Wardha, India [2]

Abstract: Visual Cryptography is a special encryption technique that encrypts the secret image into n number of shares to hide information in images in such a way that it can be decrypted by the human visual system, without any cryptographic knowledge and computation devices. To reveal the secret information at least a certain number of shares (k) or more are superimposed. Visual Cryptography using color Error Diffusion objective of this scheme is to apply the VCS for color image and get better quality decrypted image with the size of decrypted image should be same as original image. Visual Cryptography using Random number generator and digital Watermarking where divided shares are enveloped in other images using invisible digital watermarking. The shares are generated using Random Number.

Keywords: Visual cryptography, color error diffusion, random number, digital watermarking.

I. INTRODUCTION

Until the year 1997 visual cryptography schemes were applied to only black and white images. First colored visual cryptography scheme was developed by Verheul and Van Tilborg. Colored secret images can be shared with the concept of arcs to construct a colored visual cryptography scheme. Visual cryptography is one of the solution for Encryption. Visual cryptography is proposed in 1994 by Naor and Shamir who introduced a simple but perfectly secure way that allows secret sharing without any cryptographic computation, which they termed as Visual Cryptography Scheme (VCS) [1].

Cryptography is study of mathematical technique to provide the methods for information security. It provides such services like authentication, data security, and confidentiality. Visual cryptography is one of the techniques used in modern world to maintain the secret massage transmission. In this technique no need of any cryptographic algorithms likes symmetric (DES, AES, TRIPLE DES etc) and asymmetric (RSA, Diffie- Hellman, Elliptic Curve Cryptographic) algorithms [5]. Noar and Shamir introduce visual cryptography in 1994. This technique is used to reduce complexity of encrypted and decrypted method and also two way communication can be achieved very securely. Traditional techniques use private and public key concepts. But it could be achieved only by the distribution of keys. It uses the Diffie-Hellman approach and other mathematical computations are used for encryption and decryption. Visual cryptography is based on the images and is obtained by sending pixel information. Visual cryptography schemes depend on sub-pixels and its complexity, computation, reliability, etc. The image consists of black and white, grayscale color images. Visual cryptography uses participates to send secret information. It consists of multiple party or multi-party methods.

Error diffusion is the type of half toning in which quantization (image processing is lossy compression technique achieved by compression of arrangement of values to single quantum value) and residual is distributed to neighboring pixel that have not been processed [2][3][4].

In digital watermarking original image is divided into number of shares, produced by k-n secret sharing visual cryptography are embedded into the envelope images by LSB replacement [6]. The color change of the envelope images are not sensed by human eye [7]. (More than 16.7 million i.e.224 different colors are produced by RGB color model. But human eye can discriminate only a few of them.). This technique is known as invisible digital watermarking as human eye cannot identify the change in the envelope image and the enveloped (Produced after LSB replacement) image [8]. In the decryption process k number of embedded envelope images are taken and LSB are retrieved from each of them followed by OR operation to generated the original image.

II. ANALYSIS OF ABOVE METHODS

A. VISUAL CRYPTOGRAPHY USING COLOR ERROR DIFFUSION

The Error diffusion technique is a dispersed dot dither method. In this method for each point in the image closest color available is found and difference between the value in the image and the color is calculated. Then Divide these error values and distributes it over the neighbouring pixels. For the later pixels it adds the errors distributed from the earlier ones and if needed clip the values to the allowed range. There are many ways to distribute the errors and many ways to scan the image. The two basic ways to scan the image are with a normal left-to-right and top-to-bottom raster, or with an alternative left-to-right and right-to-left raster.

In Encryption the shares are generated from the color image. The color image is decomposed into R, G and B

channels. From these channels the shares are created using following steps:

1) Color halftone: The color image I is decomposed into IR, IG and IB channels. Then apply the halftone for each channel to get IRhft, Ighft, Ibhft.

2) Sharing of channels by using VCS (2,2).
In the decryption the color image channels are reconstructed by stacking the shares of channels. These color image channels are combined to get the secret color image.

1) Stacking of shares: The stacking (XOR) operation is performed to recover the image of each channel. IT uses XOR operation for stacking share image to get less distorted decrypted image and sub sampling 2 X 2 block into a single pixel produces a decrypted image with same size as original image.

2) Combining all channels: Combining recovered image of all channels we get the secrete color image.

B .Visual Cryptography using Random number generator and digital Watermarking
Original image is divided into shares, with k-n secret sharing visual cryptography scheme an enveloping technique is proposed where the secret shares are enveloped within apparently innocent covers of digital pictures using LSB replacement digital watermarking. This adds security to visual cryptography technique from illicit attack as it befools the hacker's eye. K-n secret sharing process is simple as random number is used. Shares contain the original image contents; if anyone gets shares then original image can be obtained.
The shares are enveloped into apparently innocent cover of digital pictures and can be sent through same or different communication channels. Invisible digital watermarking befools the hacker. Watermarking is a technique to put a signature of the owner within the creation.

III.CONCLUSION

This paper discusses the Visual cryptography using color error diffusion and Visual cryptography using random number generator and digital watermarking with their advantages and disadvantages. Compared to error diffusion technique watermarking technique provides more security than visual cryptography schemes. Authentication of the image is verified in watermarking concepts. But, in error diffusion there is no concepts of providing keys. Quality of image is high in watermarking technique compared to error diffusion. But changes in decoded image are less in error diffusion. We can combine both the schemes to get better results.

REFERENCES

[1] M. Naor and A. Shamir, "Visual cryptography," Advances in Cryptology-Eurocrypt"94, pp. 1–12, 1995.
[2] Z. Zhou, G. R. Arce, and G. Di Crescenzo, "Halftone Visual Cryptography," IEEE Transactions on Image Processing, to appear in 2006.
[3] M. Naor and A. Shamir, "Visual Cryptography," in Proceedings of Eurocrypt 1994, lecture notes in Computer Science, 1994, vol. 950, pp. 1–12.
[4] E.Myodo, S. Sakazawa, and Y. Takishima, "Visual cryptography based on void-and-cluster half toning technique," in Proc. IEEE ICIP, Atlanta, GA, Oct. 2006.
[5] M.Amarnath Reddy, P.Shanthi Bala, G.Aghila "visual cryptography schemes comparision", Vol. 3 No. 5 May 2011
[6] Naskar P., Chaudhuri A, Chaudhuri Atal, Image Secret Sharing using a Novel Secret Sharing Technique with Steganography, IEEE CASCOM, Jadavpur University, 2010, pp 62-65.
[7] Hartung F., Kuttter M., "Multimedia Watermarking Techniques", IEEE, 1999.
[8] S. Craver, N. Memon, B. L. Yeo, and M. M. Yeung. Resolving Rightful Ownerships with Invisible Watermarking Techniques: Limitations, Attacks and Implications. IEEE Journal on Selected Areas in Communications, Vol16, No.4 May 1998, pp.573–586,.
[9] 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.

DOI 10.17148/IJARCCE.2015.41174