ISSN: 2321-7782 (Online)
Volume 3, Issue 2, February 2015
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

Novel Approach for Visual Cryptography Using Adaptive Local Filter

Vandana G. Pujari[1]
ME (E & TC) student
D. Y. Patil college of Engg. & Tech.
Kolhapur, Maharashtra, India

S. R. Khot[2]
Asso. Prof. Dept. of Information Technology
D. Y. Patil college of Engg. & Tech.
Kolhapur, Maharashtra, India

Abstract: ***Visual Cryptography Scheme is an encryption method that is used to encode secret written materials into an image and encode this image into n share 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. A distinctive property of visual cryptography scheme is that one can visually, without computation, decode the secret by superimposing share images. This paper focuses on the sharing of color secret image into the cover images as share images. The quality of decrypted image is increased by applying adaptive local filter which reduces noise introduced during encryption and decryption process. The result analysis has been performed by using different image analysis quality parameters which is applying on original and decrypted image.***

Keywords: Encryption; Visual Cryptography; Security; Decryption; Adaptive Local Filter; Color halftoning

I. INTRODUCTION

With the rapid development of the Internet, the transferring of digital media over the internet becomes increasingly popular. Hence, the copyright protection of digital media becomes a hot topic since the digital media can be obtained and distributed easily over the Internet. Visual Cryptography is a new cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that the decryption can be performed by human, without any decryption algorithm. Visual Cryptography (VC) is a method of encrypting a secret image into shares such that stacking a sufficient number of shares reveals the secret image. Naor and Shamir introduced a simple but perfectly secure way that allows secret sharing without any cryptographic computation, termed as Visual Cryptography Scheme (VCS). Any visual secret information (pictures, text, etc) is considered as image and encryption is performed using simple algorithm to generate n copies of shares depending on type of access structure schemes. The simplest access structure is the 2 out of 2 scheme. Basically, Visual Cryptography Scheme 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 requires only selecting some subset of these n images, making transparencies of them, and stacking them on top of each other.

The two-out-of-two visual threshold scheme demonstrates a special case of k-out-of-n schemes. Inside k-out-of-n scheme to reduce the problem of contrast loss in the reconstructed images. The concept of access structure was developed which focused on the qualified and forbidden subsets of shares. The participants in a qualified subset can recover the secret image while the participants in a forbidden subset cannot. The properties of a k-out-of-n scheme including the conditions needed for optimal contrast and the minimum pixel expansion attainable. The concepts of VC have been extended such that the secret image is allowed to be a grey-level image rather than a binary image. Although the secret image is grey scale, shares are still constructed by random binary patterns. Halftone visual cryptography used to increase the quality of the meaningful shares based on the principle of void and cluster dithering. In this modifying the pixel in the original halftone image depends on the content of the pixel chosen and thus results in visible image residual features of the original halftone images. This paper focuses on the method of dividing the particular secret image into four shares by using different cover images.

II. Literature Review

Several new methods for VC have been introduced recently in the literature. Visual cryptography (VC) is a type of secret sharing scheme introduced by Naor and Shamir [1] presented a k-out-of-n scheme of visual cryptography, a secret binary image is encoded in to n shares and distributed amongst n participants, one for each participant. No participant knows the share given to another participant. By stacking the k shares decode the secret image. Less than k shares cannot be decoded by secret image. Ateniese [2] presented a more general method for VC scheme based upon general access structure. The access structure is a specification of qualified and forbidden subsets of shares. The participants in a qualified subset can recover the secret image while the participants of forbidden subset cannot recover secret image. M. S. Fu et. al.[3]. Presented Joint visual cryptography and watermarking (JVW) algorithm. In this researcher paper they work on both watermarking and visual cryptography involve a hidden secret image. For visual cryptography secret image encoded into shares, more shares are required to decode the secret image. For watermarking secret image embedded into watermark halftone image.

C. S. Hsu et. at. [4] Presented research work visual cryptography and sampling method used for digital images copyright protection. This method can register multiple secret images without altering the host image and can identify the rightful ownership without resorting to the original image. Chang-Chou Lin et. al. [5] presented visual cryptography for gray level images by dithering techniques. Instead of using gray sub-pixels directly to constructed shares, a dithering technique is used to convert gray level images into binary images and a visual cryptography method for binary images is then applied to the resulting dither image. M. Nakajima et. al. [6] developed extended visual cryptography for natural images constructs meaningful binary images as shares.

This will encode secrets image more securely in to a shares and also describes the contrast enhancement method to improve the quality of the output images. Zhou et. al. [7] Presented halftone visual cryptography which increases the quality of the meaningful shares. In halftone visual cryptography a secret binary pixel „p is encoded into an array of Q1 X Q2 („m in basic model) sub pixels, referred to as halftone cell, in each of the „n shares. by using halftone cells with an appropriate size, visually pleasing halftone shares can be obtained. Also maintains contrast and security.

Plataniotis, et.at.[8] Presented Colour image secret sharing The method operates in the decomposed bit-levels of the input colour vectors to change both spatial and spectral correlation characteristics of the share outputs and produce random, colour-noise-like images for secure transmission and access. The decryption process satisfies the perfect reconstruction property and recovers the original colour image by logically decrypting the decomposed bit vector-arrays of the colour shares.

From above literature survey of different systems it is observed that many systems are currently present which performs the encryption. But, the quality of encrypted share image degrades when the secret image is added inside cover image. Also, the quality of the secret image degrades after the decryption.

III. System Architecture

The present work consists of visual cryptography encryption and decryption process. In this secret image is hide inside multiple cover images to form the share images and later they are decrypted to extract the secret image from the shares. The decrypted secret image has been processed to reduce the noise by applying adaptive local filter. This whole process has been depicted in fig. 1.

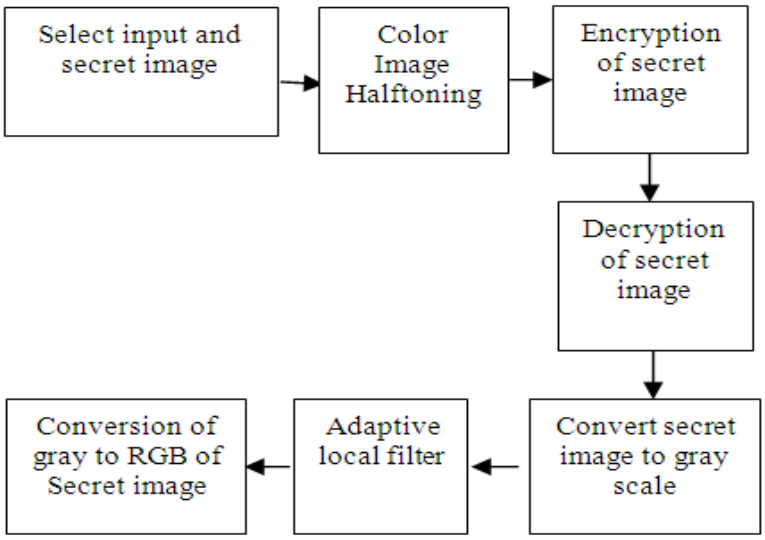


Fig 1: System architecture

The design and development of this system will be divided into five modules as –

a) *Color Image Halftoning*

In this module, the different input images in which the secret image is embedded and one secret image have been selected. To adjust the colors into limited range the Jarvis color halftoning has been applied on it. This halftoned image has been used as an input to the next stage.

b) Encryption of secret image

In this module, the halftoned images are used to generate the cover images by expanding the one pixel into 2x2 matrixes in which the secret image has been embedded diagonally, vertically or horizontally. After embedding the secret image into the two or more cover images the whole cover images are send any where through network.

c) Decryption of secret image

In the decryption process, secret image has been extracted from cover images and convert the secret image into original size. Here the AND & OR operations has been applied on the cover image for extraction of secret image.

d) Adaptive Local Filtering

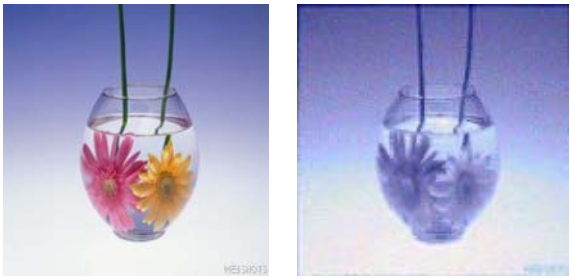
In this module the adaptive local filter has been applied to increase the quality and perfection of decrypted secret image. This process is required because the decrypted image contains the noise which degrades the quality of secret image. For applying this filter there is a need to convert the color image into gray scale image.

e) Gray to RGB conversion

After applying the average local filter to the secret image there is a need to convert gray scale secret image to RGB image. So to perform this, the decrypted image has been considered and compared for filling the color into the gray scale image.

IV. Result Analysis

The whole system has been developed by using the MATLAB language. The four input images of same size and one secret image is used as input for this system. Fig. 2 shows the original secret image and the decrypted secret image after applying the average local filter.



a) Original Secret Image *b) Decrypted secret image*

Fig. 2 Original and decrypted secret image

From the fig. 2 it is clear that the final decrypted image quality is very much similar to the original secret image. The result analysis has been made by applying this system on various images of different size. The image quality has been measured by considering different image quality analysis parameters as Mean Square Error (MSE), Peak signal to Noise Ratio (PSNR), Structural Content (SC), Maximum difference (MD) and Normalized Absolute Error (NAE). The values of these parameters for different size images are shown in Table 1.

TABLE I
Image quality parameters for different size images

Size	MSE	PSNR	SC	MD	NAE
177x177	350.0429	22.6896	1.0828	133	0.1094
280x210	432.9834	21.7661	0.0412	154	0.0850
533x400	740.1536	19.4376	0.9925	183	0.0523
800x600	284.2120	23.5944	1.0439	139	0.0798
900x720	405.6102	22.0497	0.9897	117	0.1088
1024x768	730.4694	19.4948	0.9908	198	0.0626

Here, in Table 1. Low value of MSE shows higher quality decrypted image. For low MSE the PSNAR value is high. Large value of SC, MD and NAE indicates the poor quality image.

V. CONCLUSION

In this paper a new technique used for to hide a color secret image into multiple colored images. The generated image contain less noise compared to the previously techniques. This developed method does not require any additional cryptographic computations. For decryption the share are used to get original secret image. The adaptive local filter has been applied on decrypted image to reduce the noise. As noise is decreased the MSE is less and PSNR value is high for decrypted secret image. The 80% image quality has been maintained after applying the adaptive local filter.

References

1. M. Naor and A. Shamir, “Visual cryptography,” in Proc. EUROCRYPT, 1994, pp. 1–12.
2. G. Ateniese, C. Blundo, A. D. Santis, and D. R. Stinson, “Visual cryptography for general access structures,” Inf. Comput., vol. 129, no. 2, pp. 86–106, 1996.
3. M. S. Fu and O. C. Au, “Joint visual cryptography and watermarking,”in Proc. IEEE Int. Conf. Multimedia Expo, 2004, pp. 975–978.
4. C. S. Hsu and Y. C. Hou, “Copyright protection scheme for digital images using visual cryptography and sampling methods,” Opt. Eng., vol. 44, p. 077003, 2005.
5. C. C. Lin and W. H. Tsai, “Visual cryptography for gray-level images by dithering techniques,” Pattern Recognit. Lett., vol. 24, pp. 349–358, 2003.
6. M. Nakajima and Y. Yamaguchi, “Extended visual cryptography for natural images,” J. WSCG, vol. 10, no. 2, 2002.
7. 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.

8. R. Lukac and K. N. Plataniotis, "Colour image secret sharing," Electron. Lett., vol. 40, no. 9, pp. 529–531, Apr.2004.
9. E. Myodo, S. Sakazawa, and Y. Takishima, "Visual cryptography based on void-and-cluster halftoning technique," in Proc. IEEE Int. Conf. Image Process., 2006, pp. 97–100.
10. Y. C. Hou, "Visual cryptography for color images," Pattern Recognit., vol. 36, pp. 1619–1629, 2003
11. 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.
12. C.M. Hu and W.G. Tzeng, "Cheating Prevention in Visual Cryptography," IEEE Transactions on Image Processing, Vol. 16, No. 1, pp. 36-45, 2007.

AUTHOR(S) PROFILE

Vandana G. pujari, received the BE (Electronics) from D. K. T. E. society's Textile and Enginerring Institute, Ichalkaranji in 2011 and pursuing ME (Electronics and telecommunications) from D. Y. Patil college of Engg. & Tech., Kolhapur. Her area of research is image processing. She is a life ime member of ISTE.

S. R. Khot, received the BE degree in Electronics in 1988.He received ME degree in Electronics in 1998. His research interest is in computational vision and image processing. He is a professional member of the ISTE. He has published 18 papers in national and 18 papers in international conferences. He is working as Associate Professor in D. Y. Patil college of Engg. & Tech., Kolhapur.

