Volume 5, Issue 1, January 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Security Approach by Using Visual Cryptographic Technique

Ritesh D.Yelane*
Dept of Electronics Engg.(Comm.)
SDCOE Selukate, Wardha,
Maharashtra, India

Dr. Nitiket. N. Mhala
Prof. and Head of Electronics Engg.
BDCOE, Sevagram, Wardha,
Maharashtra, India

Prof. B. J. Chilke
Dept of Electronics Engg.(Comm.)
SDCOE Selukate, Wardha,
Maharashtra, India

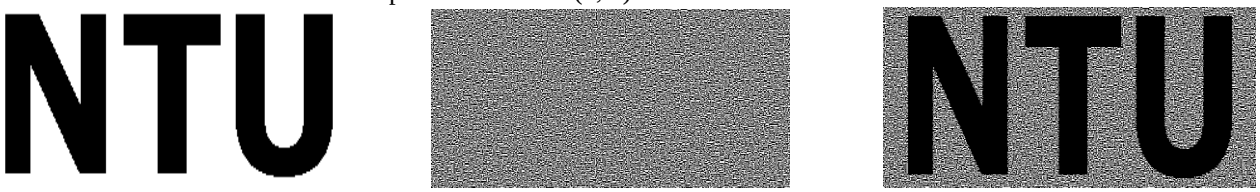
Abstract: Nowadays each and every transmission system is depending on internet which increases security, efficiency and reduces response time. Visual Cryptography is also taking advantages of real time on internet and also at destination user for security purpose.

In our proposed system, we are interested to provide information security mechanism by using visual cryptography scheme on condition that Authentication, authorization, Confidentiality, Privacy and security are maintained in VCS. For this system we work with digital gray scale images for secrete and covering image, data confidentiality using asymmetric cover image encryption and finally it will improve the contrast of the recovered secret image and produce clear resultant image.

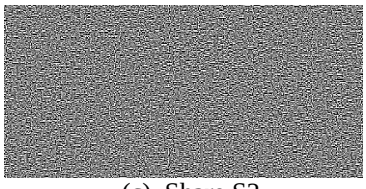
Keywords- Embedded Extended Visual Cryptography Scheme, Secret Sharing, Halftoning, Privacy and security, Evcs.

I. INTRODUCTION

Now days, the transmission of data through computer network is increasing rapidly. So the security of transmitted data is very important issue. To provide the security to transmitted data we can use cryptography. It consists of two main algorithms 1) encryption algorithm and 2) decryption algorithm. Encryption algorithm is used to convert readable text (plain text) into unreadable text (cipher text).decryption algorithm is used exactly reverse of the encryption algorithm .above processes require the computation knowledge to recover the secret image. The basic principle of the visual cryptography scheme (VCS) was first introduced by Naor and Shamir. VCS is a kind of secret sharing scheme that focuses on sharing secret images. The idea of the visual cryptography model 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. It is a special encryption technique to hide information in images in such a way that it can be decrypted by the human vision if the correct key image is used. This property makes visual cryptography especially useful for the low computation load requirement. The above explanation is shown below as an example of traditional (2, 2) – VCS.



(a) The Secret Image (b) Share S1 (d) Decrypted Image from S1 & S2



(c) Share S2

Fig 1. Example of traditional (2, 2) -VCS

It generates noise-like random pixels on share images to hide secret information. This technique is known as conventional visual secret sharing schemes. It suffers a management problem, because of which dealers cannot visually identify each share. This problem is solved by the extended visual cryptography scheme (EVCS), which adds a meaningful cover image in each share. EVCS is realized by embedding random shares into meaningful covering shares.

To overcome the drawbacks of EVCS systems we can use embedded extended visual cryptography scheme. This scheme ensures that the secrete image can be visually observed by stacking the eligible subsets of shares. The shares are all significant in the sense that parts of the information of the original shares images are preserved. The ratio of the information of the original share images are preserved in the shares. In this method secrete image is encrypted by the

VCS, and then embed its shares into the covering shares. This project work is the generation of (n, n) secret sharing scheme which will use multiple secrets. By rotating one of the shares we can recover one of the secret.

The VCS system has many applications in the real world. They include transmission of military orders securely, authentication and authorization, transmitting passwords, Information forensics and security and so on. With the rapid improvement of network technology, multimedia information can be sent over the internet easily. Number of secret information's 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, a variety of image secret sharing schemes have been developed. This is the best and easy way to hide the secret data for application of sending, on computer network in real time.

II. LITERATURE SURVEY

A paper [1], proposed a construction of EVCS which is realized by embedding random shares into meaningful covering shares, and we call it the embedded EVCS. This scheme defines traditional VCS, halftoning technique by using dithering matrix. In order to deal with the gray-scale image, the halftoning technique was introduced into the visual cryptography. The halftoning technique (or dithering technique) is used to convert the gray-scale image into the binary image. In this paper, they make use of the patterning dithering. The patterning dithering makes use of a certain percentage of black and white pixels, often called patterns, to achieve a sense of gray scale in the overall point of view. They used two algorithms i) The halftoning process for each pixel in input image: It includes Generating the covering shares by using the dithering matrices, Generating the covering subsets with minimum average black ratio, Converting the covering subsets into dithering matrices and then Embedding the corresponding VCS into the covering shares. ii) The embedding process: It includes embedding of all shares and stacking of these shares, also improvements on the visual quality of the shares such as reducing the black ratio of the covering subsets. The proposed embedded EVCS has many specific advantages against different well-known schemes, such as the fact that it can deal with gray-scale input images, has smaller pixel expansion, is always unconditionally secure, does not require complementary share images, one participant only needs to carry one share, and can be applied for general access structure.

A paper [2], proposed system divides the secret image into number of shares. These shares get embedded into selected positions of Cyan, Magenta, Yellow, Black shares of the meaningful cover image. In the proposed system the above mentioned embedded EVCS would like to implement on color image as a secrete image. Further improvement will give you more contrast image and will produce more clear the resultant secrete image. This proposed method was applied on general access structure and is always unconditionally secure which is inherited from the corresponding VCS. This system will give more contrast result of the recovered color secret image which is not possible with existing Embedded EVCS.

The proposed method in paper [3] describes that a color visual cryptography scheme producing meaningful shares is proposed. These meaningful shares will not arouse the attention of hackers. The proposed scheme utilizes the halftone technique, cover coding table and secret coding table to generate two meaningful shares. Also it uses halftone gray scale and color visual cryptography, visual cryptography with perfect restoration, color visual secret scheme. They provide three steps for implementation such as Interface design using Applet frame work, Embedded Visual cryptography Implementation**,** and Integration**.** Visual color methods used same technique to decompose the color secret image into three images such as Cyan, Magenta and Yellow. Then halftone technique used to translate the three color images into halftone images, a color halftone image can be generated. The proposed scheme must first learn the colors of the extracted pixels from the secret image. Then obtained colors must meet their matches in the coding table so that a suitable block can be produced. They also proposed a method to improve the visual quality of the share images, extend a single pixel into a 2×4 block. However, the size of the share remains the same as what happens in the 2×2 pixel expansion case. This way, a considerable part of the storage space can be saved.

A paper [4] proposed system overcome the difficulties in the existing system by using the Error Diffusion Method in Half tonic technique which improves visual quality. Its main use is to convert a multi-level image into a binary image, though it has other applications. This application was developed using java desktop application. The application featured with four sections. Each section performs the following functions. They are: VCS Shares Creation, Covering Share Creation, Embedding VCS and Covering Shares and Stacking Process. The proposed privacy scheme in visual cryptography via error diffusion technique just shares the error values to neighbouring pixels. So that it makes the binary image to achieve some effect as gray image. It also enhances the edges of image. So, that the text in the image become sharper and makes more readable. In both secret share generation and decryption part, OR operation is used, which makes the scheme very simple. But the main disadvantage of this scheme, it has much more computation than other methods of visual cryptography. The original image can be encrypted using a key to provide more security to this scheme. The key may be a text or a small image. This technique is more effective in providing security from illicit attacks.

III. PROPOSED WORK

In Visual Cryptography the encoding scheme which allows a secret image shares into n participants. Set of participants is able to recover the secret image without any cryptographic knowledge. To share this kind of construction our analysis realized by embedding random shares into meaningful covering shares and we call it integrated embedded visual cryptography.

Our proposed system will be consisting of four phases as:

A. Generation of secret image into n shares
B. Generation of covering image to all these shares.
C. Embedding the VCS into covering images.
D. Reconstruction of the secret image by stacking of shares.

1) Generation of secret image into n shares:

It interacts with the user to get the information such as the location of the secret image and the number of shares it has to create. Here the limitation of creating the share is 5 and size of image should be 225 x 225 pixels. It also locates the address where the share has been created. After giving location of the share and number of shares, click the create button. Then, the application will generate the VCS Shares.

2) Generation of covering image to all these shares:

The Covering share creation is performed in the second phase of this application. It gets the location of covering image and name of the covering share and creates the Covering share. After providing the location and the cover name, click the create button.

3) Embedding the VCS into covering images:

The third phase performs the embedding operation of the VCS shares and the covering shares. The user must notify the location of VCS shares and the covering share. Then, user has to provide the name of the creating embedded shares. After providing the location of share image, cover image and name of embedded image, click the Embed button which embeds both VCS and Covering Shares. The location generated Embedded Shares is displayed in the text area.

4) Reconstruction of the secret image by stacking of shares:

This is the fourth phase, it is the process of joining all the embedded shares together to obtain secret image. The user must select the number of shares needed to recover the images and click OK. If we select the 3 in the application will display 3 columns where we want to enter the share location. After that when we click the 3 out of n stack button, it retrieves the original image. If we select the two in No of shares: column, two share location will be displayed. And then select the location of shares we want to stack. If we select the two in no. of shares: column, two share location will be displayed. And then select the location of Embedded Shares we want to stack. Then Click *2* out of *n* stack button to get the secret image.

IV. CONCLUSIONS

In this paper, we proposed a construction of EVCS which was realized by embedding the random shares into the meaningful covering shares. The shares of the proposed scheme are meaningful images, and the stacking of a qualified subset of shares will recover the secret image visually. We show two methods to generate the covering shares, and proved the optimality on the black ratio of the threshold covering subsets. We also proposed a method to improve the visual quality of the share images. At last, the embedded EVCS is flexible in the sense that there exist two trade-offs between the share pixel expansion and the visual quality of the shares and between the secret image pixel expansion and the visual quality of the shares. This flexibility allows the dealer to choose the proper parameters for different applications.

ACKNOWLEDGMENT

I would like to thank my guide Dr. Nitiket. N. Mhala and Prof. B. J. Chilke for their guidance and support and Department of Electronics Engineering (Comm.), S. D. College of Engineering, Selukate, Wardha.

REFERENCES

[1] Feng Liu and Chuankun Wu, "Embedded Extended Visual Cryptography Schemes" in IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 6, NO. 2, JUNE 2011.

[2] Mrs. Bhandare Shital, Mr. Jhade Manoj, Mrs. Jadhav Angarika, "An Improved Approach for Extended Visual Cryptography Scheme for Colour Image" in International Journal of Computer Applications (0975-8887)-2011.

[3] Ch. Priyanka, Prof Thaduri Venkata Ramana, T. Somashekara, "Analysis Of Secret Sharing And Review On Visual Cryptography Schemes" International Journal Of Engineering Inventions, Issn 2278-7461, Isbn-2319-6491, Pp:43-51, Issue 10, November 2012.

[4] Mr. A. Duraisamy, Mr. M. Sathiyamoorthy, Mr. S. Chandrasekar, "Protection of Privacy in Visual Cryptography Scheme Using Error Diffusion Technique" IJCSN International Journal of Computer Science and Network, Vol 2, Issue 2, April 2013.

[5] T. Rajitha, Prof P. Pradeep Kumar, V. Laxmi, "Construction of Extended Visual Cryptography Scheme for Secret Sharing" in International Journal of Computer Science and Network (IJCSN) Volume 1, Issue 4, August 2012

[6] M. Naor and A. Shamir, "Visual cryptography" in Proc. EUROCRYPT' 94, Berlin, Germany, 1995, vol. 950, pp. 1–12, Springer- Verlag, LNCS, 1995.

[7] M. Nakajima and Y. Yamaguchi, "Extended visual cryptography for natural images" in Proc. WSCG Conf. 2002, pp. 303–412, 2002.

[8] Chang-Chou Lin, Wen-Hsiang Tsai, "Visual cryptography for gray-level images by dithering techniques, Pattern Recognition Letters 24 (2003) 349–358.

[9] Z. M. Wang, G. R. Arce and G. Di Crescenzo, "Halftone visual cryptography via error diffusion," In IEEE Transaction on Information Forensics & Security,vol.4,no.3,pp. 383-396,Sep.2009.

