Volume 7, Issue 5, May 2017 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Analysis and Extraction of Password Image using Visual Cryptography and Steganography

[1]Nirupama Bhat Mundukur*, [2]Mastan Rao Chundi, [3]Prashanti Guttikonda
[1, 2] Department of CSE, Chebrolu Engineering College, Chebrolu, Guntur Dist., A.P, India
[3] Department of CSE, Vignan's Lara Institute of Technology & Science, Vadlamudi, Guntur Dist., A.P, India

Abstract— The digital age expects to store or communicate information in a secured way. The primary method of securing the information is through passwords. An individual can access the information using password. In banking applications, like Netbanking or ATM pins, the passwords are sent to the receiver through registered post or courier. Instead of personally distributing the password, automation of the password is proposed. In this paper, a password processing method is suggested using visual cryptography and steganography to securely deliver the password in the form of an image shares hidden in a cover image, to the receiver. The receiver at the destination extracts the password and uses with ease.

Keywords— banking applications, visual cryptography, steganography, automation, password processing

I. INTRODUCTION

Secure Information Storage and Communication plays a vital role in the Digital Age.All the Financial and Banking applications were moving towards cashless transactions. Thus the data, passwords, documents and other important information must be secured from disclosure. Computers and mobiles are being used for data processing, storage, retrieval and communication of information.

In the banking system, when an authenticated customer requests for a ATM card, the ATM card will be sent to the customer through mail.A separate document that contains a temporary PIN number is also sent to the customer or it has to be collected by the customer from the respective bank where the customer has the account. This is the traditional system that is being followed till date. During the studies in Visual Cryptography, an interesting area to implement the existingideas was found. An application based on visual cryptography and Steganography was proposed to communicate the PIN password in a secured way to the authenticated user.

Considering password as a secret image, it is divided into two shares using anyone of the Visual cryptography techniques.As both the shares look as random pixels, they can be hidden in a cover image and communicated to the authenticated customer. At the receiver side, the shares can be extracted from the cover image and combined to get back the original image password.It is found that the Visual Cryptography is unbreakable [1]. Thus it assures the security of the password in the form of shares from the intruders. Steganography is the art of hiding one data in another data. The data can be messages, images, or files. Depending on the cover file, the type of steganography changes. Here an image is used as the cover file, thus it is known as image steganography. As a steganography technique is used, if the cover file is captured bythe intruder, it is difficult to suspect the hidden data[2].

The organization of this paper is as follows:Literature survey is presented in Section 2;Section 3 describes theproposed application; Section 4 provides the Implementation, results and its analysis followed by Conclusions and future work givenin section 5.

II. LITERATURE SURVEY

To protect the secrets in the form of images[1], Naor and Shamir introduced a simple and interesting concept called Visual Cryptography. This is a powerful encryption technique to hide information in images in such a way that it can be decrypted by the human vision, when the correct key image is used. It uses two or more transient image layerscalled shares. The shares generated contains random pixels depending on each other. The easiest way to implement visual cryptography is to print the two layers onto a transparent sheet and put one on the other.It is impossible to retrieve the secret information from only one of the images.This scheme maintains perfect secrecy. It is very easy to implement as it uses a simple decryption method which does not require any complex algorithms or computers. Thus, it is a very convenient way to protect secrets.The same method is used to divide the password image into shares and extract back the shares using the computer as a tool.

For division of shares, a patterns consisting of 4 subpixels arranged in a 2 x 2 array is taken in one of the following ways as shown in figure 1. The half of 4 subpixelsis filled with black and the rest becomes transparent. It will makesix patterns which is diagonal, horizontal and vertical. If the pixel in the password image is white, that pixel is replaced with any one of the above patterns in both of the shares. If the pixel in the password image is black, that pixel is replaced with any one of the above patterns in one of the shares and its transpose in the other share.

When these shares are placed one on top of the other, the pixel are visually ORed. Hence a white subpixelstogether looks gray (half black and half white) and black subpixels look like a single black pixel. Thus the white pixels turn into grey in the recovered image[3]. Researchers have been using visual cryptography in various applications.Much more work is carried on to improve the contrast of the recovered image. New bounds on pixel expansion are introduced and pixel expansion is minimized by fixing the VCS parameters[4].Image size invariant visual cryptography scheme was developed where the recovered image is same as the size of the original image[5]. A new (k,n) Visual cryptography scheme with non-expansible shadow size based on the probabilistic method was devised where the frequency of white pixels is used to analyze the contrast of the recovered image[6] . VC schemes were extended to grey level and color images. A new visual cryptography scheme suitable for gray-level images is devisedwhere the image is converted to binary image and processing is performed[7]. VC schemes for the colored images were also proposed[8].

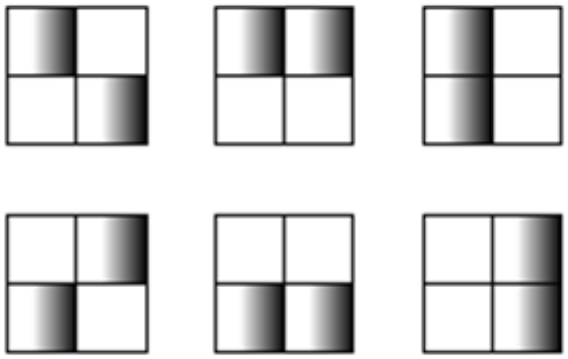

Fig 1. Possible 2 X 2 subpixel expansion

Steganography is a practice in which information in the form of messages, images, or files are hidden inside othermessages, images, or files. Image Steganography is a technique of hiding data in images using image layers [9]. A gray scale or a color image can be taken as the cover image and the image shares are hidden inside the cover image. The hiding process is done by using LSB method in the RGB layers of the cover image. Various researchers have extended different methods in using the LSB methods. A steganography system is designed for hiding and extracting a secret file embedded into an cover image file using random LSB insertion method in which the secret data spreads among the cover image in a random manner[10]. Two adjacent bits are embedded in a pair of pixels to minimize the alteration of histogram preserving the first order statistical property of cover image[11]. Multiple encrypted secret images are concealed in a cover image using LSB substitution[12].In order to improve the quality of stegoimage[13], neural networks is used for identifying the best locations in cover image to embed the secret data. An enhanced password processing scheme is used using Visual Cryptography and Optical Character Recognition[14].

III. PROPOSED METHOD

The proposed method is divided into three phases. They are

i) Division of shares
ii) Hiding the shares in the cover image and
iii) Recovery/ extraction of password.

Figure 2 gives a clear picture of Phase 1 and Phase 2 and Figure 3 gives the process of extraction of password.

A. Division of shares

The binary password image is taken. Using conventional visual cryptographic technique, it is divided into two shares with pixel expansion. This method is as follows:

C_0 = all the matrices obtained by permuting the columns of $\begin{bmatrix}1 & 0 & 1 & 0\\1 & 0 & 1 & 0\end{bmatrix}$

Thus $C_0 = \left\{\begin{bmatrix}1010\\1010\end{bmatrix}\begin{bmatrix}0101\\0101\end{bmatrix}\begin{bmatrix}0011\\0011\end{bmatrix}\begin{bmatrix}1100\\1100\end{bmatrix}\begin{bmatrix}1001\\1001\end{bmatrix}\begin{bmatrix}0110\\0110\end{bmatrix}\right\}$

C_1= all the matrices obtained by permuting the columns of $\begin{bmatrix}1 & 0 & 1 & 0\\0 & 1 & 0 & 1\end{bmatrix}$

$C_1 = \left\{\begin{bmatrix}1010\\0110\end{bmatrix}\begin{bmatrix}0101\\1010\end{bmatrix}\begin{bmatrix}0011\\1100\end{bmatrix}\begin{bmatrix}1100\\0011\end{bmatrix}\begin{bmatrix}1001\\0110\end{bmatrix}\begin{bmatrix}0110\\1001\end{bmatrix}\right\}$

C_0 represents subpixels of a white pixel and C_1 represents subpixels of a black pixel. One of the matrix C_0 or C_1 are selected, depending on the pixel value of the source image. Each row data is put as 2X2 matrix form in the generated share. The number of rows represent the number of shares to be divided and number of columns represents the pixel expansion(Here 4.i.e, 2X2).

B. Hiding the shares in the cover image

A cover image of size twice of the image share is taken. The first share is placed in the least significant bit plane and the second share is placed as continuation in the least significant bit plane of the cover image. The cover image is transmitted to the receiver.

C. Recovery/ Extraction of password

At the receiver end, the bits of the LSB plane of the cover image is extracted into 2 shares. OR operation is performed on the extracted shares and complemented. The secret is recovered. But as per the algorithm 50% of the white pixels in the password image will be turned to grey.

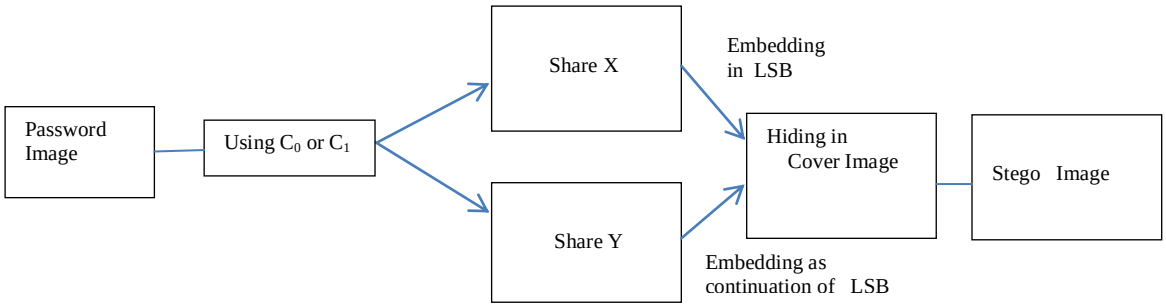

Fig 2: Division and Embedding the image shares in the cover image

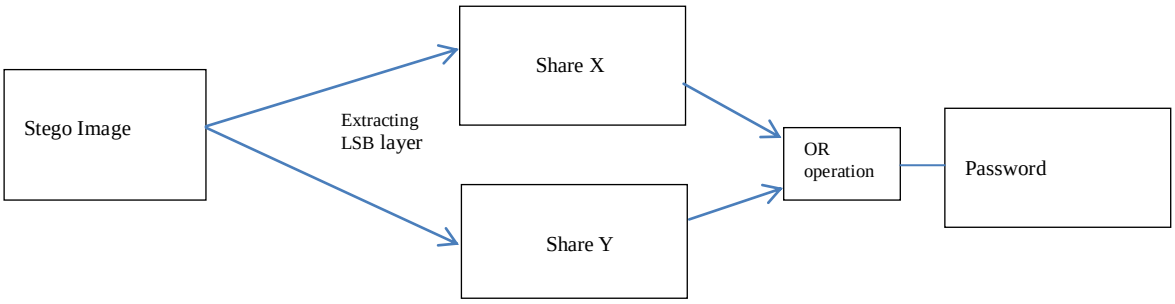

Fig 3 Extraction of Embedded image shares and then password image

IV. IMPLEMENTATION

A grey cover image is taken from the internet source as a cover image and resized to 1024X512. The password image is taken and resized to a 256X256 image. According to the above algorithm, the shares are generated and displayed. These two shares are hidden in LSB layer one after the other. The shares hidden in cover image is communicated to the receiver. At the receiver end, the share plane is extracted and stacked to get back the password image. The original password image and the shares of the image are given in figure 4. The cover image, the cover image embedded with the shares (stego image) and their respective histograms are shown in figure 5 and 6. There is no much change found in the histograms. The extracted password image is shown in figure 7.This implementation procedure is repeated by taking different cover images and analyzed by calculating Mean Squared Error (MSE) and Peak Signal-to-noise ratio (PSNR) values. Three different cover images are taken and the process of hiding the shares is performed. The MSE and PSNR values of original and stego images of various cover images are tabulated in Table 1.There is no much changes found in these values. Much error is not identified in the cover image.

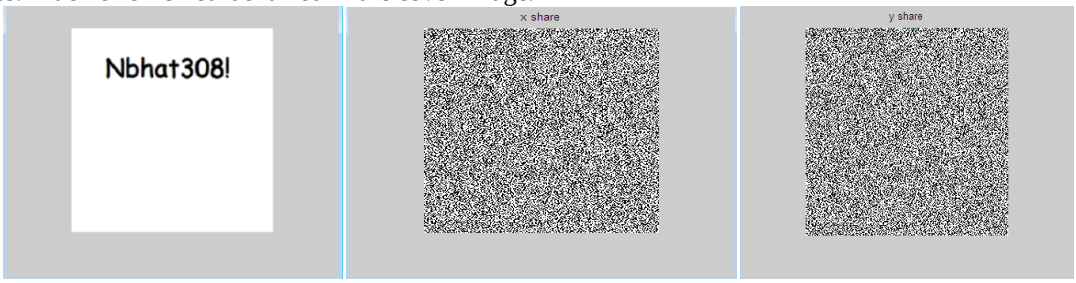

Fig 4 a) OriginalPassword b) X Share c) Y Share

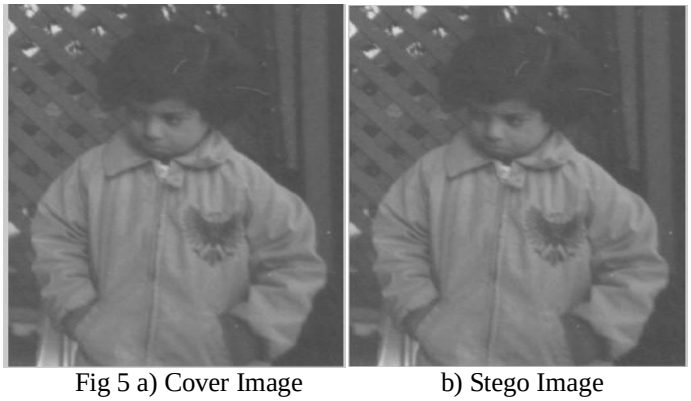

Fig 5 a) Cover Image b) Stego Image

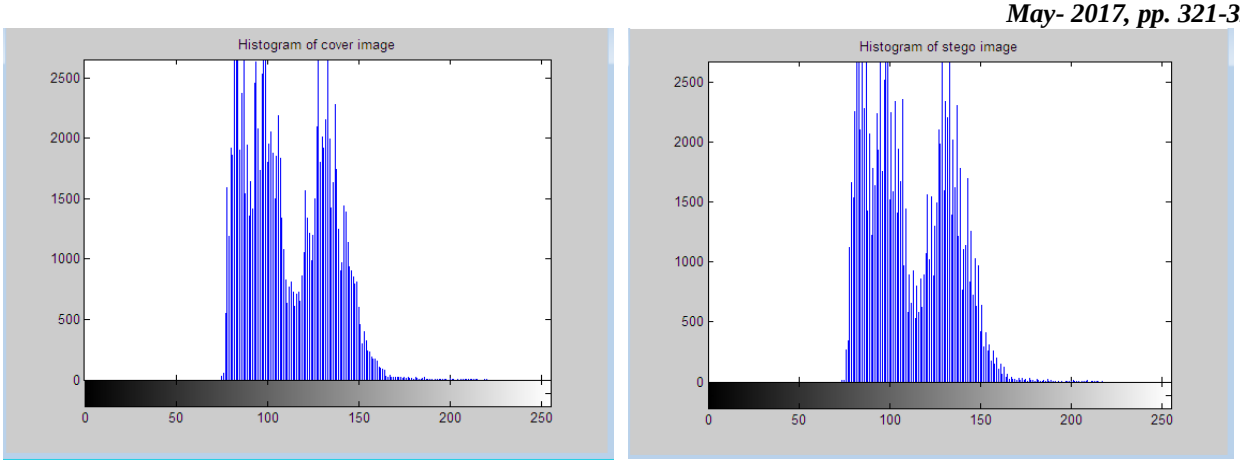

Fig 6 Histogram of Cover and Stego images (pout)

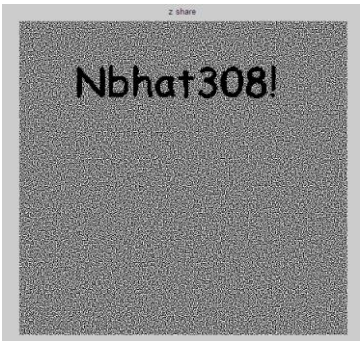

Fig 7 Extracted password

Table 1 PSNR and MSE Values of Cover And Stego Images

IMAGE	IMAGE SIZE	PSNR VALUE	MSE VALUE
Circuit.tif	512*256	54.1799	0.5006
Cameraman.tif	512*256	54.1944	0.4990
Pout.tif	512*256	54.2048	0.4978

V. CONCLUSION AND FUTURE WORK

The password image is divided into two shares using the conventional visual cryptography technique. Least significant bit is used to hide both the shares one after other. Extraction of the shares from the layers of the stego image is done. And OR operation is performed on the shares during the extraction of password image. This process can be put as an application. The combination of visual cryptography and steganography provides a better security during communication as there is no much difference observed in the image quality the cover image and stego image. Further this can be applied on color images with the combination of techniques of visual cryptography and steganography methods and compared for quality. This method could be converted as an application and used in banking applications.

REFERENCES

[1] Noar M., Shamir A., *Visual cryptography: Advances in Cryptography*, Eurocrypt'94, Lecture Notes in Computer Science, vol. 950,Springer-Verlag. 1 – 12 1995

[2] Bailey, K., and Curran, K., "An Evaluation of Image Based Steganography Methods", Journal of Multimedia Toolsand Applications, Vol. 30, No. 1, pp. 55-88, 2006.

[3] M.NirupamaBhat, K.Usha Rani," Analysis of (2,2) Visual Cryptographic Scheme", Publications Of Problems & Application In Engineering Research, Vol, 4, Special Issue 01, 2013, ISSN: 2230-8547; e-ISSN: 2230-8555

[4] P. A. Eisen and D. R. Stinson. "Threshold visual cryptography schemes with specified whiteness levels of reconstructed pixels", Designs, Codes and Cryptography, 25(1):15–61,2002.

[5] R. Ito, H. Kuwakado, and H. Tanaka, R. Ito, H. Kuwakado, and H. Tanaka. "Image size invariant visual cryptography" *IEICETrans. Fundamentals*, E82–A(10):2172–2176, 1999

[6] Yang, C.-N., " New visual secret sharing schemes using probabilistic method" Pattern Recogn.Lett., 25, 481–494. 2004

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

[8] Young-Chang Hou, "Visual cryptography for color images", Pattern Recognition, 36 :1619–1629, 2003

[9] O. Kurtuldu and N. Arica, "A new steganography method using image layers," in Computer and Information Sciences, *23rd International Symposium on, ISCIS '08*, 2008, pp. 1-4.

[10] M.S.Sutaone, M.V.Khandare ,"Image based steganography using LSB insertion technique" IET International Conference on Wireless, Mobile and Multimedia Networks pp 146 – 151, 2008

[11] Ling Xi,XijianPing,Tao Zhang ,"Improved LSB matching steganography resistinghistogram attacks", 3rd International Conference on Computer Science and InformationTechnology pp 203 – 206, 2010.doi: 10.1109/ICCSIT.2010.5564086.

[12] Pallavi Das, Satish Chandra Kushwaha, Madhuparna Chakraborthy,"Multiple embedding secret key image steganography using LSB substitution and Arnold Transform", *2nd International Conference on Electronics and Communication Systems (ICECS)* pp845 – 849, 2015.

[13] K.S. Seethalakshmi , Usha B A , Sangeetha K N, "Security enhancement in image steganography using neural networks and visual cryptography", *International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS)*, 2016 DOI: 10.1109/CSITSS.2016.7779393

[14] Dana Yang, InshilDoh, Kijoon Cha, "Enhanced Password Processing Scheme Based on Visual Cryptography and OCR", *IEEE ICOIN 2017*, 978-1-5090-5124-3/17

