A VISUAL CRYPTOGRAPHIC SCHEME FOR OWNER AUTHENTICATION USING EMBEDDED SHARES

Ratheesh V.R.
University Institute of Technology, University of Kerala, Kollam, Kerala, India
rathvr@gmail.com

Jogesh J.
University Institute of Technology, University of Kerala, Kollam, Kerala, India
jogeshj55@gmail.com

Jayamohan M.
College of Applied Science, Adoor, Kerala, India
jmohanm@gmail.com

Abstract

A new scheme for user authentication is proposed using visual cryptography and digital watermarking. The original image, mostly the photograph of the authorized person is split into shares. One of the shares is kept within the server and the other one will be printed on the identification card issued to the user. The personal information unique to the user along with his signature will be embedded within the printed share. Least significant bit watermark insertion algorithm has been used for embedding data. Experiments show that the method is efficient and effective. It was possible to retrieve the watermark information from the printed share read through a reading device with no distortion. The method can be implemented with minimum processing cost.

***Keywords*:** Visual Cryptography; Watermarking; user authentication; embedded shares.

1. Introduction

Secret sharing has been a serious concern even before the digital era. One can find a lot of methods and practices which shows the applications and demand of techniques historically. The widespread wings of global networks has turned Information Technology to be a world of links; no user can exist without being networked. Disseminating knowledge to different locations and accessing as and when necessary is the working policy now. The world of internet is densely populated with people entering from every corner to access maximum information crossing all barriers of security and privacy. The scene makes it difficult to have private communication. Sending information without leakage, without tampering, without noise to the intended recipient is the biggest challenge in IT now. Equally challenging is the authentication and genuineness of information at the recipient side.

The field of secure messaging can be broadly classified into two- cryptography and steganography. Cryptography is the art of secure messaging, may not be secret. The information is not hidden, but supposed to be protected against all types of third-party attacks, denial of ownership or receipt. The conventional practices in cryptography use an encryption procedure which is generally a mixture of complex procedures for substitution and transposition of bits being communicated. Though the techniques are providing all sorts of security services including user authentication, data integrity, non-repudiation and confidentiality, the computational complexity of encryption and decryption makes it heavy to manage and practice. Attempts for improving the strength of a cipher multiplied the computational and implementation costs, sometimes exponentially. Visual Cryptography, which uses the support of human visual system for encryption and decryption becomes promising in these circumstances.

2. Visual Cryptography Schemes

In 1994, Naor and Shamir proposed a cryptography scheme called the "(k, n)-threshold visual secret sharing scheme," and the idea they raised has ever since been referred to as "visual cryptography (VC)" [Naor & Shamir, 1994]. The major feature of their scheme is that the secret image can be decrypted simply by the human visual system without having to resort to any complex computation. The message to be transmitted is split into a set of images called shares, which will be communicated in separate packets among different users. The decryption can be done only when a specified number of shares are available at the receiving end. The original proposal had been a work on binary images. Each pixel in the original image had been replaced by a set of

subpixels. For example, consider the case of a (2,2) scheme. We can use a 2x2 pixel grid in place of original image pixels. The pixel grids can be as given in figure 1.

The pixels of the	white □						black■					
share *A*												
share *B*												
Stacking												

Figure 1. subpixel grids in a 2x2 scheme

Each black pixel in the original image will be replaced with complimentary grids from both sets, whereas each white pixel will be replaced with a pair of identical grids. When a pair of black grids are stacked we get a black area and when a pair of identical grids are stacked we get a black-white area. The newly generated image shares will be meaningless having no similarity with the original image. No information is available on the pixel values of original secret. Since the pixels are either black or white, no probability distributions can be generated [macPherson, 2000].

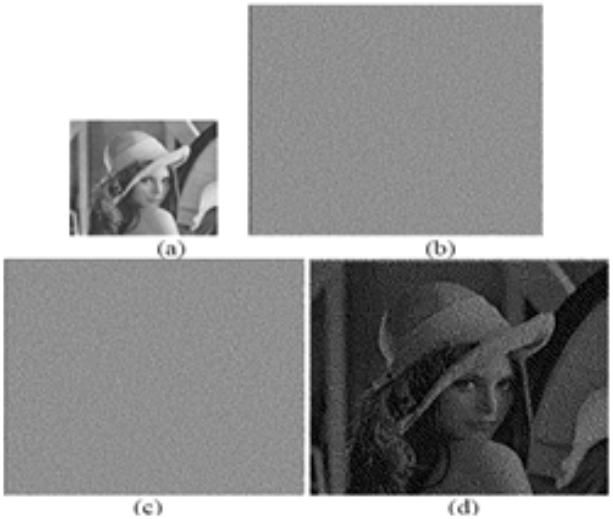


Figure 2. Example share generation using 2x2 scheme

As it is visible from figure 2, the new image will be of double the size of the original one.

Studies have been made on making the technique useful for grayscale images as well as color images [MacPherson, 2000, Wang et al. 2003, Shyu 2006]. Tuyles et al. have experimented an XOR- operation based scheme for decryption[Tuyls et al 2005]. An interferometric encryption technique with XOR operation has been proposed by Lee, et al.[Lee et al 2002]. Extended Visual Cryptographic schemes have been experimented on color images. Viet and Kurosawa attempted to improve the quality of reconstructed image with the use of NOT operation[Viet, Korosawa 2004]. The XOR operation has been implemented with the reversing of functions.

While conventional schemes generate meaningless shares, meaningful shares are generated in extended visual cryptographic schemes. When the set of shares are superimposed, these meaningful shares disappear and the original secret gets recovered [Naor, Shamir 1996].

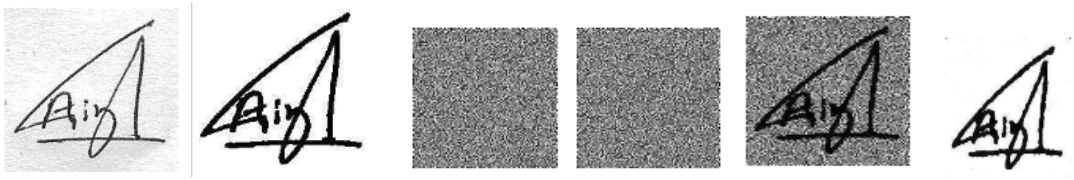
Apart from its adverse effects on contrast and image resolution, visual cryptographic schemes have been found heavily dependable for user authentication. Ito et.al. have attempted to generate size invariant shares[Nameer 2007]. Ito uses the traditional (k,n) scheme, with the number of subpixels being 1. The structure of the scheme is defined by a Boolean vector, generated based on the color of the pixel in various shares.

2.1 Visual Cryptography for User Authentication

Though Visual cryptographic schemes provide huge savings in computational requirements when compared to conventional cryptographic techniques, there are a lot of issues that prevent VC schemes to be used in message communication. Primarily, the size of the shares get doubled when a 2x2 scheme is used. Since the background information is getting tampered, the contrast of the image also gets affected. But in spite of all these issues VC schemes are being the best candidates for secret sharing purposes. When a secret is being shared among multiple users, nobody including the participants can identify the actual content until sufficient number of shares are aligned together.

Tunga and Mukherjee (2012) proposed a scheme that describes a safety mechanism based on Visual Cryptography. The mechanism described consists of a lock and a key. For every pair of lock and key there is a unique image associated, which is unknown to even the owner of the lock and key. This image is stored in the lock's internal memory. The secret image is then divided into two parts. One of these two parts is stored in the lock and the other part is stored in the key. The lock also contains a mechanism which can change the pixel distribution in the lock and the key. The secret images remains the same whereas the division changes. The lock consists of the first part of the first secret image and the key consists of the second part of the first secret image. Another secret image is used called as the second secret image. This second secret is also divided into two parts and stored similarly like the first secret. The lock of the safe opens only when both the shares of both the secret images get correctly matched.

Hegde et al. (2008) proposed a technique for the secure authentication for banking application based on signature. They first pre-processed the original secret image. The signature, which is widely and most commonly used in banking applications for authentication, is considered as the original secret image. After the image is being pre-processed, shares are being created base on the pre-processed image. In the authentication process, the shares are stacked one above the other and a post processing is done. The revealed secret signature then authenticates the customer of the bank as an authorized person to carry out transactions. Experimental results on signature authentication is illustrated in figure 3.



(a) (b) (c) (d) (e) (f)

Figure 3: (a) Original Signature (b) Signature after pre-processing (c) Share 1 (d) Share 2 (e) Revealed Signature (f) Signature after post-processing.

Fang (2011) proposed an algorithm for the authentication of offline QR (Quick Response**)** code. He used Visual Secret Sharing Scheme for the authentication. A QR code is matrix barcode which is readable by specific readers dedicated to QR code. The code consists of a white background on which black modules are arranged in a square pattern. The information that is encoded in a QR code can be any text or URL or any other data.

3. Proposed Work

Visual Cryptography can be used as a means for verifying user identification. The most popular identification scheme for users in restricted areas is to use photo-printed identification cards. It is a practice in competitive examinations also. This leaves a chance of doing masquerade and repudiation by stamping the photograph of a different person. In the proposed work, the photograph of the user will be split into two shares. One of the shares with the signature and other unique identification details embedded within that can be inserted on the ID card, while keeping the alternate share within a server system. At the entry point, a card reader device along with a display unit will be set-up. The user has to insert the card into the device. The information embedded within the share on the card will be extracted first. Then the share will be stacked with the alternate share available with the server and the resultant image will be displayed on the screen. The user can be verified by an authorized person, or through a direct photograph using a camera connected with the machine at entry point.

The Least Significant Bit (LSB) insertion algorithm is used for watermarking. The LSB insertion algorithm is the simplest watermarking algorithm, with the limitations that any tampering on the pixel information may result in loss or distortion of watermark. But in the proposed scene, the watermarked share is being printed on a card, and hence there is no question of tampering the digital contents. The watermark is extracted just before decryption.

3.1 Algorithm

An identification document will be issued to an authorized user in the following manner:

1. Read the image and watermark information. The watermark information can be in a coded form, in order to reduce the size.
2. If the photograph is (i) a grayscale image, split into eight bit planes.
   (ii) a color image, separate it into three color layers. Each layer acts like a grayscale image.
3. Generate two shares for each bit plane out of the image.
4. Watermark the share1 along with identification details into a cover image using LSB insertion.
5. Generate ID card with share1.

At the access point the following procedure will be carried out:

1. Read the image in the specified area on the inserted card.
2. Extract watermarked information.
3. Separate share1 and identification details.
4. Get corresponding share2 from the server based on the information extracted.
5. Stack the shares and generate the photograph.
6. Display the actual photograph at access point.

An example for generation of shares based on the algorithm described is given in figure 4.

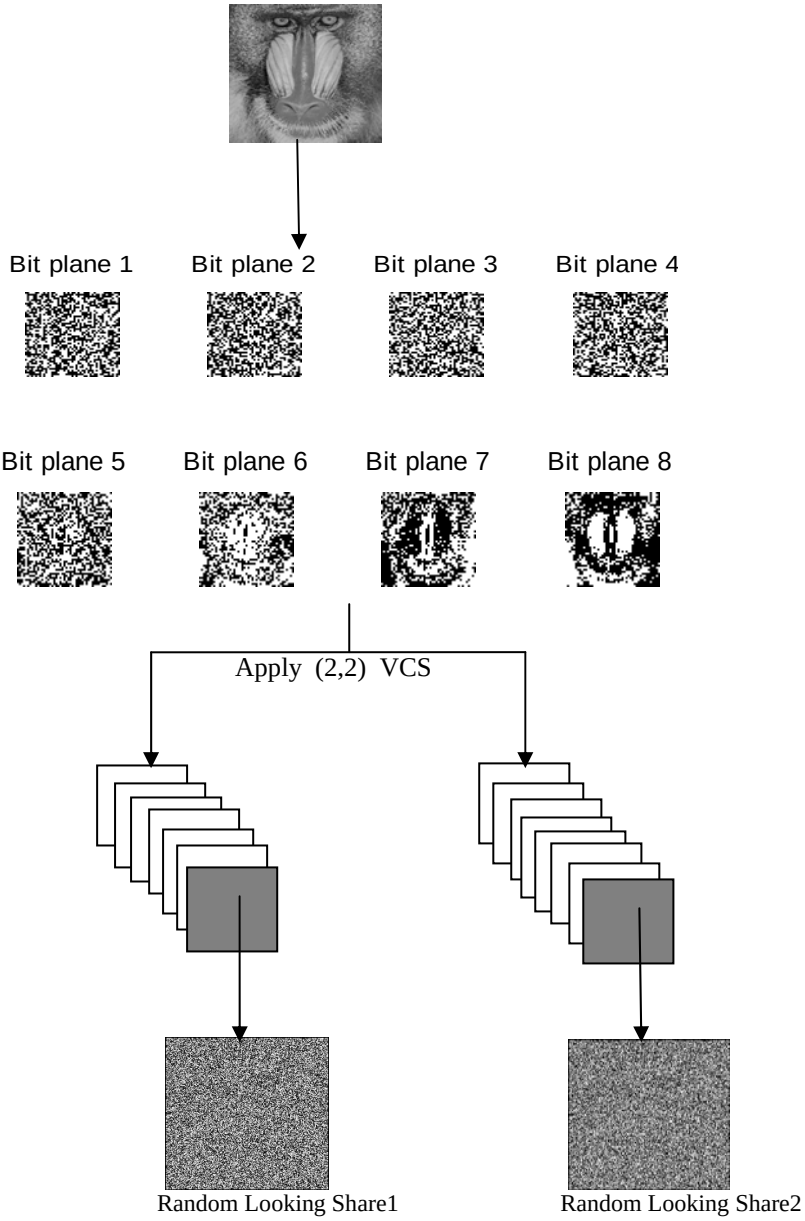
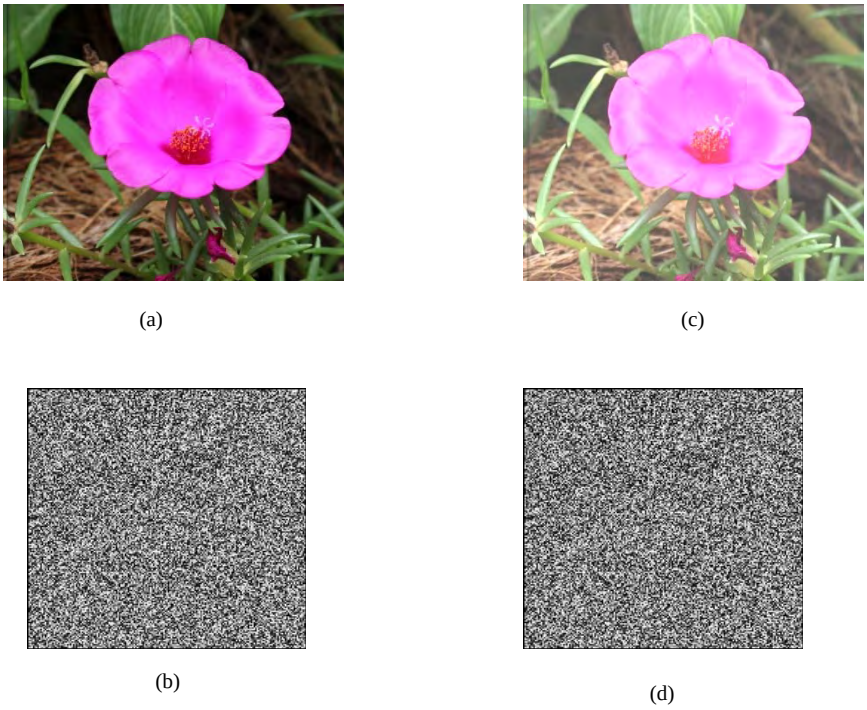


Figure 4. share generation

4. Experimental Results

The algorithm has been implemented using MATLAB, and tested with a set of selected images. Along with passport size photographs, a group of natural scenes also were used to estimate the loss of contrast and to test the recoverability of watermarks. The watermarked share was printed on glossy photo printing papers with varying stiffness of gsm 80 to gsm 140. The printed shares were scanned through a good quality image scanner for extraction and verification.

The loss of contrast on the cover image is not an issue since the authentication and verification depends on the embedded information alone. LSB insertion algorithm was used for watermarking. Sample images are given in figure 5.



(a) (c)

(b) (d)

Figure 5. (a) Original cover image, (b) original share, (c) cover image after embedding, (d) extracted share

7. Conclusive Remarks

Visual cryptographic scheme is a computationally feasible alternative for user authentication requirements as well as secret messaging. We have made an attempt to apply VC schemes with meaningful shares along with digital watermarking for user authentication. The method can be improved using contrast enhancement schemes. We have implemented the algorithm for grayscale images. The method can be easily extended for color images.

Studies are to be done on using the candidate image itself as cover image, but it necessitates the use of a technique which outputs the image without distortions after watermarking.

References

[1] Ateniese, G. et al. (1996) “Visual cryptography for general access structures,” *Inf. Computation*, vol.129, pp. 86-106.

[2] Fang, W. (2011), “Offline QR Code Authorization Based on Visual Cryptography”,Seventh International Conference on Intelligent Information Hiding and Multimedia Signal Processing, pp. 89-92.

[3] Hegde, C., et al. (2008) , “Secure Authentication using Image Processing and Visual Cryptography for Banking Applications”, ADCOM, pp. 65-72.

[4] Lee, J.C et al. (2002), “Visual cryptography based on an interferometric encryption technique,” ETRI journal, vol.24, no.5,pp.373-380.

[5] MacPherson, L.A. (2000) “ Gray level Visual Cryptography for General Access Structure”, Uni. Waterloo, Ontario, Canada.

[6] Nameer, N. EL-Emam (2007), “Hiding a large amount of data with high security using stegnagraphy algorithm”, Journal of Computer science ISSN 1549-3636, vol. 3, No.4,pp. 355-372.

[7] Naor, M. and Shamir, A. (1995), “Visual cryptography,” *Advances in Cryptology-EUROCRYPT’94*, pp. 1-12.

[8] Naor, M. and Shamir, A. (1996), “Visual cryptography: improving the contrast via the cover base,” *presented at Security in Communication Networks*.

[9] Shyu, S.J. (2006), “ Efficient Visual secret sharing scheme for color images”, Pattern Recog., Vo. 39, No.5, pp.866-880.

[10] Tunga, H. and Mukherjee, S. (2012), “ Design and Implementation of a Novel Authentication Algorithm for Fool-Proof Lock- Key System Based On Visual Secret Sharing Scheme”, IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 3, No 1, May 2012, pp.-182-186.

[11] Tuyls, P et al. (2005)"XOR-based visual cryptography schemes" , Design codes and Cryptography, vol. 37 , pp.169-186.
[12] Viet, D.Q. and Kurosawa, K. (2004), "Almost ideal contrast visual cryptography with reversing, " *Topics in Cryptology*-CT-RSA,pp.353-365.
[13] Wang, Z.M., Arce, G.R. and Crescenzo, G. (2003), "halftone Visual Cryptography with Error Diffusion", IEEE Trans. On Info. Forensics Security, Vol.4 (3), pp.383-396.