The International Journal Of Engineering And Science (IJES)
|| Volume || 4 || Issue || 4 || Pages || PP.67-72 || 2015 ||
ISSN (e): 2319 – 1813 ISSN (p): 2319 – 1805

Natural Image Based Visual Secret Sharing Scheme

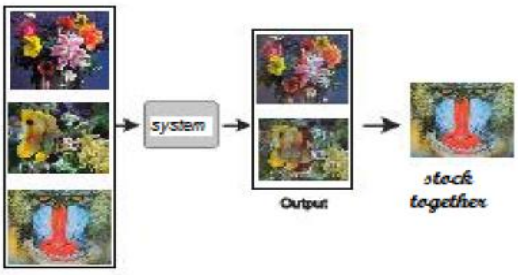
Vijina Varghese
PG Scholar, Department of Communications Systems,
Nehru Institutions of Engineering and Technology, Nehru Gardens.

ABSTRACT
Information security becomes more and more important while the internet communication grows up. Visual secret sharing (VSS) schemes hide secret images in shares that are either printed on transparencies or are encoded and stored in a digital form. Conventional visual secret sharing schemes suffers from a management problem, so that dealers cannot identify each share visually The approaches involving the EVCS for GAS suffers from a pixel expansion problem and also needs a sophisticated various encryption schemes. This paper presents natural image based visual secret sharing scheme that shares secret images via various carrier media to protect the secret and the participants during the transmission phase. The proposed (n, n) - NVSS scheme can share one digital secret image over n -1 arbitrary selected natural images (called natural shares) and one noise-like share . The natural shares can be photos or hand-painted pictures in digital form or in printed form. The noise-like share is generated based on these natural shares and the secret image

Date of Submission: 03-April-2015 Date of Accepted: 30-April-2015

I. INTRODUCTION

Cryptography is the practice and study of hiding information. In today's environment, cryptography is considered a branch of both mathematics and computer science, and is affiliated closely with information theory, computer security, and engineering. Cryptography is used in technologically advanced applications, including areas such as the security of ATM cards, computer passwords, Security in electronic voting, Security in ATM transactions and electronic commerce, which all depend on cryptography. Visual cryptography (VC), first proposed in 1994 by Naor and Shamir is a secret sharing scheme, based on black and-white or binary images. Secret images are divided into share images which, on their own, reveal no information of the original secret. Shares may be distributed to various parties so that only by collaborating with an appropriate number of other parties, can the resulting combined shares reveal the secret image. Recovery of the secret can be done by superimposing the share images and, hence, the decoding process requires no special hardware or software and can be simply done by the human eye.



basic 2-out-of-2 or (2; 2) visual cryptography scheme produces 2 share images from an original image and must stack both shares to reproduce the original image. More generally, a (k; n) scheme produces n shares, but only requires combining k shares to recover the secret image

The proposed NVSS scheme can share a digital secret image over n -1 arbitrary natural images (hereafter called natural shares) and one share. Instead of altering the contents of the natural images, the proposed approach extracts features from each natural share. These unaltered natural shares are totally innocuous, thus greatly reducing the interception probability of these shares. The generated share that is noise-like can be concealed by using data hiding techniques to increase the security level during the transmission phase. The NVSS scheme uses diverse media as a carrier; hence it has many possible scenarios for sharing secret images. For example, assume a dealer selects n-1 media as natural shares for sharing a secret image. To reduce the transmission risk, the dealer can choose an image that is not easily suspected as the content of the media (e.g., landscape, portrait photographs, hand-painted pictures, and flysheets). The digital shares can be

stored in a participant's digital devices (e.g., digital cameras or smart phones) to reduce the risk of being suspected. The printed media (e.g., flysheets or hand-painted pictures) can be sent via postal or direct mail marketing services. In such a way, the transmission channels are also diverse, further reducing the transmission risk.

Visual cryptography (VC) is a technique that encrypt secret image into *n* shares, with each participant holding one or more shares. Anyone who holds fewer than *n* shares cannot reveal any information about the secret image. Stacking the *n* shares reveals the secret image and it can be recognized directly by the human visual system .Secret images can be of various types: images, handwritten documents, photographs, and others. Sharing and delivering secret images is also known as a visual secret sharing (VSS) scheme.

II. PROPOSED METHOD

In (*n, n*)-NVSS scheme, includes two main phases: feature extraction and encryption. In the feature extraction phase, 24 binary feature images are extracted from each natural share to reduce the transmission risk of share S, the share is concealed behind cover media or disguised with another appearance by the data hiding process. The resultant share S_ is called the generated share. The *n* - 1 innocuous natural shares and the generated share are *n* shares in the (*n, n*)-NVSS scheme. When all *n* shares are received, the decryption end extracts *n* -1 feature images from all natural shares and then executes the XOR operation with share***)*** In the encryption phase, the n - 1 feature images (F1,…, Fn-1)_ with 24-bit/pixel color depth and the secret image execute the XOR operation to generate one noise-like share S with 24-bit/pixel color depth.

III. THE FEATURE EXTRACTION

There are some existing methods that are used to extract features from images, such as the wavelet transform. However, the appearance of the extracted feature may remain some texture of the original image. It will result in decreasing the randomness of the generated share and eventually reduce security of the scheme. To ensure security of the propose scheme, we develop a feature extraction method to yield noise like feature images from natural images such that the generated share is also a noise-like image.

Assume that the size of the natural shares and the secret image are(w , h) pixels and that each natural share is divided into a number of (b,b) pixel blocks before feature extraction starts. As Fig shows, the feature extraction module consists of three processes—binarization, stabilization, and chaos processes. First, a binary feature matrix is extracted from natural image N via the binarization process. Then, the stabilization balances the occurrence frequency of values 1 and 0 in the matrix. Finally, chaos process scatters the clustered feature values in the matrix.

In the binarization process, the binary feature value of a pixel can be determined by a simple threshold function *F* with a set threshold. To obtain an approximate appearance probability for binary values 0 and 1, the median value Move pixels in the same block is an obvious selection as the threshold.

Fig .image preparation

$$f^{x,y}=F(H^{x,y})=\begin{cases}1 & H^{x,y} \geq M \\ 0\,; otherwise\end{cases}$$

The stabilization process is used to balance the number of black and white pixels of an extracted feature image in each block. The number of unbalanced black pixels Qs can be calculated as follows:

$$Q_s = \begin{pmatrix} \sum_{\forall x_1 \le x \le xb} fx, y \\ \forall x_1 \le y \le y_b \end{pmatrix} - \frac{b^2}{2}$$

In the process, there are Qs pixels in which *f (x,y)* = 1 is randomly selected and then the value of these pixels is set to 0. The process ensures that the number of black and white pixels in each block is equal. In a natural image, pixels with the same or approximately the same values may cluster together in a continuous region. These clustered pixels have the same feature value; hence it will lead to the feature image and to the generated share revealing some textures of the natural image in the subsequent encryption process. The chaos process is used to eliminate the texture that may appear on the extracted feature images and the generated share.

IV. THE IMAGE PREPARATION AND PIXEL SWAPPING PROCESSES

The image preparation and pixel swapping processes are used for preprocessing printed images and for post-processing the feature matrices that are extracted from the printed images. The printed images were selected for sharing secret images, but the contents of the printed images

must be acquired by computational devices and then be transformed into digital data. Images can be acquired by popular electronic devices, such as digital scanners and digital cameras. To reduce the difference in the content of the acquired images between the encryption and decryption processes, the type of the acquisition devices and the parameter settings (e.g., resolution, image size) of the devices should be the same or similar in both processes.

The next step is to crop the extra images. Finally, the images are resized so they have the same dimensions as natural shares. The hand-painted picture is drawn on A4 paper. First, the picture is captured using a popular smart phone, Apple I Phone 4S, as shown in Fig. The picture then is processed using the Paint application in Microsoft Windows 7. Eventually, the picture is cropped and resized as a rectangular image as shown in Fig.

V. ENCRYPTION/DECRYPTION

The proposed (*n, n*)-NVSS scheme can encipher a true-color secret image by *n* - 1 innocuous natural shares and one noise like share. For one image, we denote a bit with the same weighted value in the same color as a bit plane; then a true color secret image has 24 bit-planes. Thus, the feature images and the noise-like share also are extended to 24 bit-planes. Each bit-plane of a feature image consists of a binary feature matrix that corresponds to the same bit-plane as the secret image.
Pixel values in a feature image are distributed randomly.

The binary feature values of a natural mage are a function of the image content and a random number generator G. Pixel values in the natural image can be treated as a random sequence with h, w samples, but the image contents are unpredictable. Hence, the binary features are random.

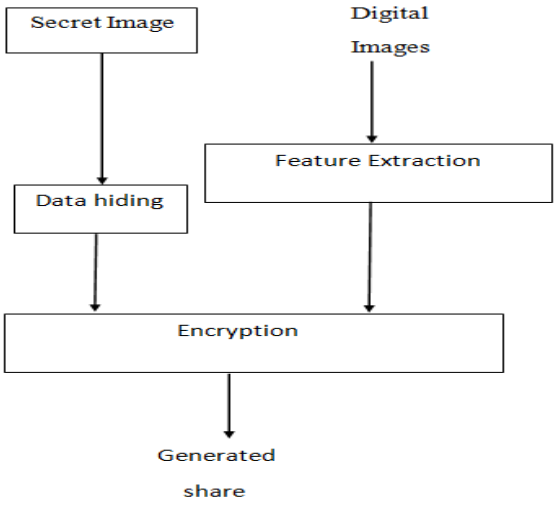


Fig. Encryption

Pixel values in the feature image are composed of 8 binary feature matrices, so the pixel values are distributed randomly. The generated share is secure.Before encryption (resp. decrypt) of each bit-plane of the secret image, the proposed algorithm first extracts *n*-1 feature matrices from *n* - 1 natural shares. Then the bit-plane of the secret image (resp. noise-like share) and *n* - 1 feature matrices execute the XOR operation (denoted by __ to obtain the bit-plane of the share image (resp. recovered image). Therefore, to encrypt (resp. decrypt) a true-color secret image, the encryption (resp. decryption) procedure must be performed. In decryption process after XOR operation and data extraction secret image will be obtained. The pseudo code of the algorithm is for true-color secret images; however it is also applicable for 8-bit gray and binary images.

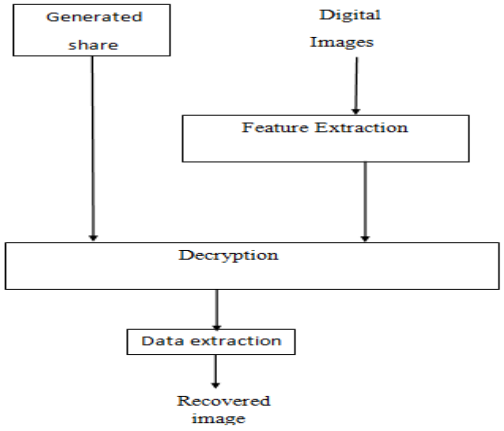


Fig. Decryption

VI. HIDING OF NOISE LIKE SHARE

QR code techniques are introduced to conceal the noise-like share and further reduce intercepted risk for the share during the transmission phase. The QR code is a two-dimensional code first designed for the automotive industry by DENSO WAVE in 1994 . The QR code, which encodes meaningful information in both dimensions and in the vertical and horizontal directions, can carry up to several hundred times the amount of data carried by barcodes. The code is printed on physical material and can be read and decoded by various devices, such as barcode readers and smart phones. Today, the QR code is widely used in daily life, and is widely visible, on the surface of products, in commercial catalogs and flyers, in electronic media, and elsewhere. It is this ubiquitous nature of the QR code that makes it suitable for use as a carrier of secret communications.

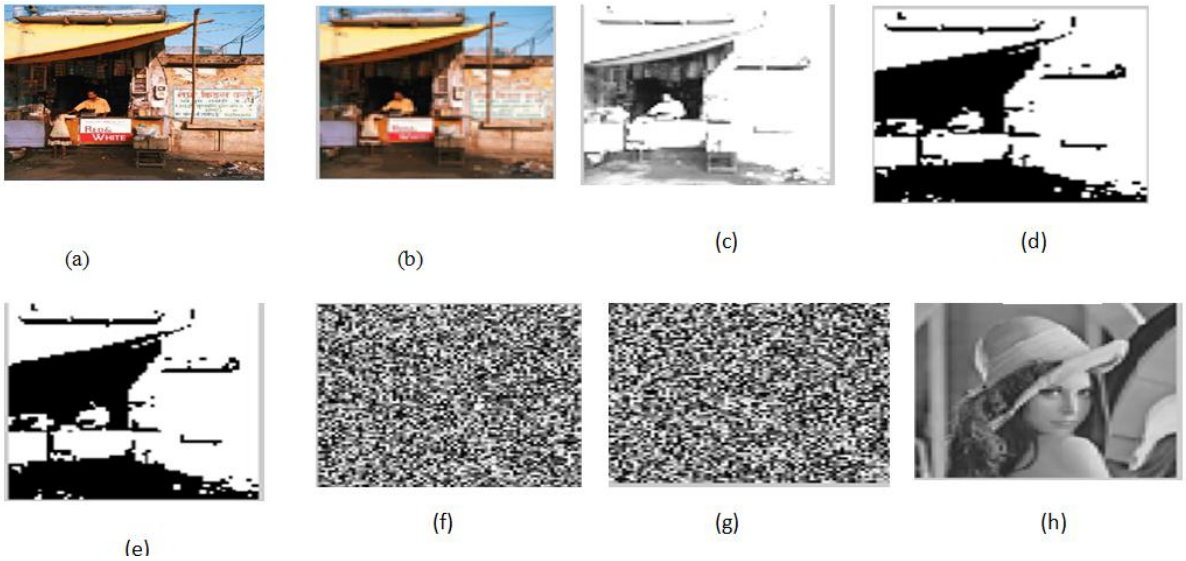


Fig Output Images: (a) Input Image,(b)BlockRepresentationOf Input Image,(c)Sum Of RGB Layers,(c)Binearization Of Input Image (e)Stabilization Of Binearized Image,(f)Natural Share,(g)Feature Extracted Share,(h)secret image

VII. RESULTS AND DISCUSSION

In the proposed method a secret image is hiding by a natural image. For that mainly three processes are used, feature extraction module, encryption and decryption, hiding of the. Sum of the RGB layers find out and the image is produced. In feature extraction process binearization, stabilization and chaos generation are Included. In the binearization process the natural image converted as the binary values. Then black and white pixels are stabilized. Itwill changed to the confusing form. The encryption done by using XOR operation. After the decryption the secret image can be recovered. Encryption has long been used by militaries and governments to facilitate secret communication. It is now commonly used in protecting information within many kinds of civilian systems. For example, the Computer Security Institute reported that in 2007, 71%of companies surveyed utilized encryption for some of their data in transit, and 53%utilized encryption for some of their data in storage Decryption is exactly the reverse procedure of encryption .The xor operation is performed between the noise like share and feature extracted image. The data extraction and image recovery proceed by finding which part has been flipped in one block. This process can be realized with the help of spatial correlation in decrypted image

VIII. CONCLUSION

The paper proposes a VSS scheme, (n,n)-NVSS scheme, that can share a digital image using diverse image media. The extracted feature from the digital image(natural image) is encrypted with the secret image in the encryption phase with the help of XOR operation .The secret image is retrieved by performing the XOR operation between the encrypted image and the natural image in the decryption phase.The media that include n-1 randomly chosen images are unaltered in the encryption phase. Therefore, they are totally innocuous. Regardless of the number of participants n increases, the NVSS scheme uses only one noise share for sharing the secret image. Compared with existing VSS schemes, the proposed NVSS scheme can effectively reduce transmission risk and provide the highest level of user friendliness, both for shares and for participants. This study provides four major contributions. First, this is the first attempt to share images via heterogeneous carriers in a VSS scheme. Second, we successfully introduce hand-printed images for images-haring schemes. Third, this study proposes a useful concept and method for using unaltered images as shares in a VSS scheme.

REFERENCES

[1] Kai-hui Lee and Pei-Ling Chiu january 2014 "Digital Image Sharing By Diverse Image Media" IEEE transactions on information forensics and security, vol. 9, no. 1,

[2] C. Guo, C. C. Chang, and C. Qin, Sep. 2012 "A multi-threshold secret image sharing scheme based on MSP ,"Pattern Recognit .Lett,., vol. 33, no. 12,. 1594–1600,.

[3] X. Wu, D. Ou, Q. Liang, and W. Sun, Aug. 2012 "A user-friendly secret image sharing scheme with reversible steganography based on cellular automata ,"J.Syst.soft. ", vol. 85, no. 8, pp. 1852–1863,.

[4] T. H. N. Le, C. C. Lin, C. C. Chang, and H. B. Le, Dec. 2011 "A high quality and small shadow size visual secret sharing scheme based on hybrid strategy for grayscale images ,"Digit .Signal Process, vol. 21, no. 6,pp. 734–745,.

[5] F. Liu and C. Wu, Jun.201 1. "Embedded extended visual cryptography schemes," IEEE Trans. Inf .Forensics Security, vol. 6, no. 2, pp. 307–322,

[6] I. Kang, G. R. Arce, and H. K. Lee, Jan. 2011. "Color extended visual cryptography using error diffusion," IEEE Trans .Image Process., vol. 20, no. 1, pp. 132–145,

[7] A. Nissar and A. H. Mir, Dec. 2010. "Classification of steganalysis techniques: A study, "Digit Signal Process., vol. 20, no. 6, pp. 1758–1770,

[8] R. Z.Wang, Y. C. Lan, Y. K. Lee, S. Y. Huang, S. J. Shyu, and T. L. Chia Nov. 2010,"Incrementing visual cryptography using random grids," Opt .Commun .*Opt.* vol. 283, no. 21, pp. 4242–4249,.

[9] Z. Wang, G. R. Arce, and G. D. Crescenzo, Sep. 2009 "Halftone visual cryptography via error diffusion," IEEE Trans. Inf. Forensics Security, vol. 4, no. 3, pp. 383–396,

[10] D. S. Tsai, G. Horng, T. H. Chen, and Y. T. Huang, Sep. 2009 "A novel secret image sharing scheme for true-color images with size constraint, "Inf. Sci , vol. 179, no. 19, pp. 3247–3254,

[11] C. N. Yang and T. S. Chen, Aug. 2007. "Extended visual secret sharing schemes: Improving the shadow image quality ,"Int,J. Pattern Recognit. Artif .Intell, vol. 21, no. 5, pp. 879–898,

[12] J. Fridrich, M. Goljan, and D. Soukal, Sep. 2004 "Perturbed quantization steganography with wet paper codes," in Proc. Workshop Multimedia Sec., Magdeburg, Germany, , pp. 4–15.

[13] G. Ateniese, C. Blundo, A. D. Santis, and D. R. Stinson, Sep. 2004 "Extended capabilities for visual cryptography," Theoretical Comput.sci.., vol. 250,nos. 1–2, pp. 143–161,

[14] M. Naor and A. Shamir, 1995 "Visual cryptography,"in Advances in cryptology vol.950 . New York, NY, USA: Springer-Verlag, , pp. 112. .

[15] P. L. Chiu, K. H. Lee, K. W. Peng, and S. Y. Cheng, Jul. 2012 "A new color image sharing scheme with natural shadows," in Proc .10th WCICA, Beijing, China, , pp. 4568–4573.