Volume 4, Issue V, May 2016
ISSN 2320-6802

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

Analytical Review of Visual Cryptography Scheme

Deepa Bajaj[1], Sumit Rana[2]

[1] Master of Technology, Dept. of CSE,
Geeta Engineering College, Panipat, Haryana (India)
er.deepabajaj@gmail.com)
[2]Assistant Professor, Dept. of CSE,
Geeta Engineering College, Panipat, Haryana (India)
sumitcse@geeta.edu.in

***Abstract*—*In this paper, we have surveyed that preserving the privacy of digital biometric data (e.g. face images) stored in a central database has become of paramount importance. Conventional 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. The shares can appear as noise-like pixels or as meaningful images; but it will arouse suspicion and increase interception risk during transmission of the shares. In this paper, we studied a visual cryptography scheme without dithering. This scheme takes grayscale input images to cover a target image across gray scale images and produces grayscale output images which are very close to the input images. Since the output images are visibly harmless and natural, it may be easy to pass visual inspection, which is a very desirable property in terms of the steganography aspect. This scheme satisfies the security and contrast conditions. It can reveal more details of original images in the decoded images than ordinary visual cryptography scheme. Upturn of the secret image can be performed by superimposing the shares. Hence, the process does not require any special software or hardware for cryptographic computations. However, loss of resolution and contrast, and also the image size expansion which results in the need for storage space, the operation is time consuming for large operands, are resulting problems and have been the focus of many researchers. The most important result is the improvement of the visual quality of both the share-images and the stack-image to their theoretical maximum. Although, in the application of grayscale VCS, the contrast is much lower than that of the binary cases. Therefore, it is more desirable to improve the contrast in the grayscale image reconstruction.*

Keywords: *VCS (visual cryptography scheme),VSS (visual secret sharing), steganography, dithering.*

1. INTRODUCTION

Increasing access to the Internet and information resources has a great impact on our everyday lives and is making humans more dependent on computer systems and networks. This dependency has brought many threats to information security. Thus, a number of studies have been done by researchers to protect secret information and data in a system. Cryptography is a well-known approach to protecting data information by writing it in secret codes and transmitting in a secure way. Visual cryptography is a kind of cryptographic technique that shares a visual secret among *n* participants by breaking up an image into *n* shares so that only he or she who has all of *n* shares can decrypt the image by overlaying each of the shares over each other [1]. In 1994, Naor and Shamir propose the visual cryptographic technique first. A generalized version of the visual cryptography is the (*k*, *n*)-threshold visual cryptography that encodes a target image into *n* shares such that any *k* or more shares enable the visual recovery of the hidden image. However, by inspecting less than *k* shares one cannot gain any information on the secret image. The 2-out of-2 visual cryptography scheme can be thought of as a private key system. One of the two shares will be a private share and the other serves as a public share. A visual cryptography that reveals the target image by stacking meaningful images is called the Extended Visual Cryptography. Here the sheets are the output images and the target image is the resulting image reconstructed by stacking the sheets all together. An access structure is a rule, which defines how to share a secret. The general access structure is represented by three components: *P* is the set of participants, *F* is a collection of forbidden sets, and *Q* is a collection of the qualified sets. An element of a forbidden set or a qualified set represents a sheet held by the corresponding participant. Stacking all the forbidden sheets of a forbidden set cannot reveal any information about the target image while stacking all the sheets of a qualified set can reproduce the target image.

It is assumed that a white pixel in a share is transparent and a black pixel is opaque so that superimposing shares can result in recovering the secret image. Since the shares are selected randomly, it is impossible to get any information about the secret images from shares individually or even subsets of the total shares. An advantage of VSS is that, unlike other cryptography techniques, this secret recovery does not need difficult computations. The secret information can easily be recovered with enough shares and requires human vision instead of special software or hardware devices. Naor and Shamir proposed a (*k*, *n*) VSS scheme and assumed that the image or message is a collection of binary 1's and 0's displayed as black and white pixels respectively.

Image contrast and the number of subpixels of the shares are two main parameters in visual cryptography schemes. The number of subpixels represents expansion of the image and should be as small as possible. In Naor and Shamir's visual secret sharing scheme (traditional VSS), each pixel in the secret image is mapped into an m×l block in each share, so the shortcoming of traditional VSS is that the shares and the recovered secret image are m × l times larger than the original secret image. Moreover, the recovered image is poor in

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

contrast since only black pixels are perfectly reconstructed while all the white pixels turn into half black and half white pixels. Therefore the secret image can be hard to interpret.

The basic model of the conventional visual cryptography assumes that on each transparency a cipher text indistinguishable from white noise is printed. However, noise-like sheets seem to be suspicious and thus are susceptible to attacks by wardens in the middle. Naor and Shamir have mentioned an extension of the visual cryptography scheme that conceals the very existence of the secret message (that is, target image), which is important from the point of secret communications like steganography.

Therefore, producing meaningful sheets like pictures rather than random dots is important. In the black-and-white scheme (that is, with binary images) the pixel is *black* if the number of black subpixels is more than a constant threshold *t*, and *white* if the number of black subpixels is less than the threshold when the transparencies are stacked together. The threshold visual cryptography is a visual cryptography based on the threshold value used as a criterion of determining black dots or white dots.

However, white or black color is a logical concept. Note that, in case of grayscale images, the pixel value 0 represents the darkest black and the value 255 the brightest white color. Most of the visual cryptographic schemes need to expand pixels. Consequently, the sheet is *m* times the size of the target image, and that leads to not only distortion of images but also inconvenience of carrying large size of sheets and waste of the storage space. This situation is more serious for grayscale or color images. The parameter *m* is called the *pixel expansion*, and the case of "*m*=1" refers to situation that the size of the sheets is same to the target. The existing schemes are mostly based on the half-toning or dithering methods to expand the binary or grayscale images. However, half-tone images are still unnatural and low in visual quality.

2. LITERATURE SURVEY

In paper Yuan Tai Hsu et. al [2], a new construction principle of visual cryptography which was suitable for sharing still images was presented. First, modify SFCOD (Space Filling Curve Ordered Dither - one of the techniques of half toning) to transform a gray-level image into an image with fewer grayscale values. Then extend the basic visual cryptography model to handle more than two grayscale values. Then the extended visual cryptography model can be applied to encode the image. This scheme satisfies the security and contrast conditions of basic visual cryptography model.

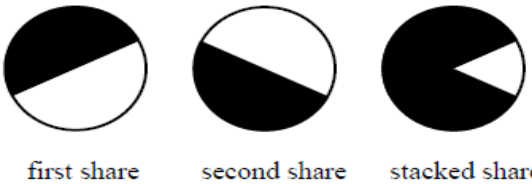

Figure 1: Visual Cryptography Scheme for Gray Images Using Circle Pixels [1]

Arun Ross et. al [3] presented few template protection approaches like:

1) Diversity: Since different applications can adopt different sets of host images for encrypting the same private face image, cross-matching across applications to reveal the identity of a private face image will be difficult. For iris codes and fingerprints, the sheets appear as random noise making it difficult to match them across databases.

2) Revocability: If the private data is deemed to be compromised, then it can be decomposed again into two new sheets based on new host images. However, in reality, break-ins to a server are very hard to detect when the attacker simply steals certain information without modifying the stored data. To strengthen security, the decomposing operation can be periodically invoked at regular time intervals.

3) Security: It is computationally hard to obtain the private biometric image from the individual stored sheets due to the use of visual cryptography. Furthermore, the private image is revealed only when both sheets are simultaneously available. By using distributed servers to store the sheets, the possibility of obtaining the original private image is minimized. There have been numerous efforts in the literature to guarantee that the data stored in distributed databases are protected from unauthorized modification and inaccurate updates.

4) Performance: It means, the recognition performance due to the reconstructed image is not degraded after decryption.

Nazanin Askari et. al [4] discussed that a visual secret sharing scheme without image size expansion is also possible. Compared to traditional VSS, the advantage of this scheme is that the secret image and all the share images have the same size. Compared to other VSS schemes that do not have expansion, our scheme results in a less noisy recovered image. Our method splits the secret image into the same size share images and recovers the secret image with good contrast by stacking them together with the logical XOR operation.

Figure 2: Shares of Binary Image Generated with Original Visual Cryptography Algorithm

In [5], two theorems are given to show that an OVCS is also a XVCS and vice versa. Also, in paper it is theoretically proved that the contrast of XVCS is 2(k−1) times greater than OVCS. This observation gives a new decoding option of VCS. Users may decode according to their convenience and need. You can easily decode the secret image by stacking operation, or we may choose the complex operation (XOR) to enhance the contrast of reconstructed image. In this paper we do not consider the monotonously increasing property in contrast condition for (k, n)-XVCS. But it is possible to modify the

condition to achieve the monotonously increasing property. Young-Chang Hou et. al [6] proposed a user-friendly visual secret sharing scheme, not only maintains the security and pixel non-expanding benefits of the random-grid method, but also allows for the production of meaningful share-images, while satisfying the requirements of being easy to carry and easy to manage is proposed. Moreover, all pixels in the cover-image and the secret image are used to perform encryption, which ensures that the contrast on the share-images and the stack-image can reach the theoretical maximum. This method also removes some unnecessary encryption restrictions (e.g., having to use only one cover-image, having to take enough black pixels from the secret image) which makes the encryption process more flexible. The findings show that this user-friendly visual secret sharing is better than the method proposed by Chen and Tsao. Kai-Hui Lee et. al [8] presented a VSS scheme, (n, n)-NVSS scheme, that can share a digital image using diverse image media. 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. Fourth, we develop a method to store the noise share as the QR code. In paper [9], we studied three novel architectures to implement binary modular exponentiation algorithm. The implementation device used is an FPGA (field-programmable gate array). The authors compared the space and time requirements of the three prototypes as well as the architecture proposed by *Blum* and *Paar* for different operand sizes. The results show clearly that despite of requiring much more hardware area, the systolic implementation improves substantially the time requirement are area x time and the product when the operand size is bigger than 512 bits, which is almost always the case in RSA encryption decryption systems. In paper James Goodman et. al [10], given a specific domain of functionality such as public-key cryptography, it is possible to provide a limited degree of domain- specific reconfigurability to provide flexibility while minimizing the overhead that is typically associated with reprogrammable logic. In paper [11] a new generic construction scheme was proposed for signcryption. A signcryption scheme is secure if it is semantically secure against adaptive chosen cipher text attack (SC-IND-CCA) and existentially unforgeable against chosen message attack (SC-EUF-CMA). The generic signcryption scheme was shown secure without random oracle while both of the concrete constructions are based on PKE-RRs which are secure in the random oracle model. One question that remains open is to construct an efficient instantiation which does not relying on random oracles. Med Lassaad Kaddachi et. al [12], proposed a new scheme for low-power image compression and transmission in wireless sensor networks are useful. The proposed solution was based on the use of Cordic Loeffler DCT (discrete cosine transform is a technique for converting a signal into elementary frequency components, widely used in image compression) transform combined with a zonal coding approach. The main idea behind is to reduce the number of operations per coefficient and the number of coefficients to be processed. As a consequence, less time and energy are expected to be required for the image processing.

3. PROPOSED METHODOLOGY

According to our proposed work, we will try to divide the complete cryptography task into 4 steps.

Firstly we input the binary secret image, followed by second step that is Divide the image into two parts according to black and white pixels.

The steps involved in this process are:

- Transform the gray-level image into a black-and-white halftone image.
- For each black or white pixel in the halftone image, decompose it into a 2×2 block of the two transparencies.
- If the pixel is white, randomly select one combination from the former two rows as the content of blocks in Shares 1 and 2.
- If the pixel is black, randomly select one combination from the latter two rows as the content of the blocks in the two transparencies.
- Repeat Step 2 until every pixel in the halftone image is decomposed, hence resulting in two transparencies of visual cryptography to share the secret image.

In third step we will get the image which is divided in to two parts and the fourth step will be the overlapping of parts to generate a secret image.

4. CONCLUSION

With the rapid advancement of network technology, multimedia information is transmitted over the internet conveniently. 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, various image secret sharing schemes have been developed. But these techniques have more computations. But, Visual cryptography scheme eliminates complex computation problem in decryption process, and the secret images can be restored by stacking operation. It needs neither cryptography knowledge nor complex computation. For security concerns, it also ensures that hackers cannot perceive any clues about a secret image from individual cover images. This property

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

makes visual cryptography especially useful for the low computation load requirement.

REFERENCES

[1] Hyoung Joong Kim, Yongsoo Choi "A New Visual Cryptography Using Natural Images" IEEE, pp: 5537-5440, 2005.

[2] Yuan Tai Hsu, Long Wen Chang "A New Construction Algorithm of Visual Crytography for Gray Level Images" IEEE, pp: 1430-1434, 2006.

[3] Arun Ross and Asem Othman "Visual Cryptography for Biometric Privacy" IEEE transactions on information forensics and security, VOL. 6, NO. 1, pp: 70-81, MARCH 2011.

[4] Nazanin Askari, Cecilia Moloney, H.M. Heys "A Novel Visual Secret Sharing Scheme without Image Size Expansion" 25th IEEE Canadian Conference on Electrical and Computer Engineering (CCECE), 2012.

[5] Ching-Nung Yang and Dao-Shun Wang, "Property Analysis of XOR-Based Visual Cryptography" IEEE transactions on circuits and systems for video technology, vol. 24, no. 2, pp: 189-197 February 2014.

[6] Young-Chang Hou, Shih-Chieh Wei, and Chia-Yin Lin, "Random-grid-based Visual Cryptography Schemes" IEEE, 2013.

[7] Dao-Shun Wang, Tao Song, Lin Dong, and Ching-Nung Yang, "Optimal Contrast Grayscale Visual Cryptography Schemes With Reversing" IEEE transactions on information forensics and security, vol. 8, no. 12, pp. 2059-2071, December 2013.

[8] Kai-Hui Lee and Pei-Ling Chiu "Digital Image Sharing by Diverse Image Media" IEEE transactions on information forensics and security, vol. 9, no. 1, pp.88-98, January 2014.

[9] Nadia Nedjah and Luiza de Macedo Mourelle "Three Hardware Architectures for the Binary Modular Exponentiation: Sequential, Parallel, and Systolic" IEEE transactions on circuits and systems—i: regular papers, vol. 53, no. 3, pp.627-633, March 2006.

[10] James Goodman and Anantha P. Chandrakasan, "An Energy-Efficient Reconfigurable Public-Key Cryptography Processor" IEEE journal of solid-state circuits, vol. 36, no. 11, pp. 1808-1820, November 2001.

[11] Chung Ki Li, Duncan S. Wong, "Signcryption from randomness recoverable public key encryption" Science direct, pp. 549-559, 2009.

[12] **Med Lassaad Kaddachi, Adel Soudani, Vincent Lecuire, Leila Makkaoui, Jean-Marie Moureaux, Kholdoun Torki "Design and performance analysis of a zonal DCT-based image encoder for Wireless Camera Sensor Networks" Microelectronics Journal, pp. 809–817, 2012.**