International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

A New Meaningful Adaptive Region Incrementing Visual Secret Sharing Based on Error Diffusion and Permutation Encoding with Cheating Prevention

Anju Mohan[1]

Computer Science and Engineering, ICET,Mahathma Gandhi University, Muvattupuzha, Kerala,India

Abstract: ***Visual secret sharing, or the so-called visual cryptography, is a well-known scheme that encrypts a secret image into several meaningless share images, usually printed on transparencies, and decrypts as stacking some or all share images by the human visual system. More and more researches about visual secret sharing and its applications have been recently proposed. Here a novel image sharing scheme is proposed to encode a secret into meaningful host images. It consists of Error Diffusion, Permutation Encoding, Steganography and Cheating Prevention. Since the secret images are grayscale images, we first apply EDBTC, then the secret image is encrypted based on permutation. Finally hide the shares created by adaptive region incrementing and cheating prevention algorithm into host images.***

Keywords: Error Diffusion, Permutation Encoding, Steganography, Cheating Prevention, EDBTC

1. Introduction

The basic principle of VCS was first introduced by Naor and Shamir [1]. The idea of visual cryptography model is to split a secret image into two random shares (printed on transparencies) which separately reveal no information about the secret image. The secret image is composed of black-and-white pixels. The secret image can be recovered by superimposing the two shares. The VCS is such a secret sharing scheme for protect image based secret, thereafter attracted many researchers attention and many schemes were proposed to improve the efficiency and exhibit different revealing effects to the secret image.

Block truncation coding (BTC), which was proposed by Delp and Mitchell in 1979 [2], is a technique for image compression. The basic concept of this technique is to divide the original image into many non-overlapped blocks, each of which is represented by two distinct values. In traditional BTC, the two values preserve the first- and second-moment characteristics of the original block. When a BTC image is transmitted, a pair of values (2 × 8 bits/block) and the corresponding bitmap which addresses the arrangement of the two values in each block (1 bit/pixel) are required. Although BTC cannot provide a comparable coding gain to other modern compression techniques, such as JPEG or JPEG2000, the complexity of the BTC is much lower than that of the above techniques.

Images can be stored in the storage devices or transmitted through the communication channel. However, store or transmit them in the plain form have risks. The adversary can steal or tap the plain-images, so that confidentiality of plain-images need to be protected. Images encryption is the solution to this problem. The plain images are encrypted so that it cannot be recognized by unauthorized party.

Many image encryption algorithms have been proposed. Most of the algorithms operate in spatial domain, usually by modifying the most significant bit(s) (or MSB) of the cipher images using an encryption key. Encryption in spatial domain has disadvantage, namely once the cipher image is modified (by common image processing operations such as JPEG compression, adding noise, brightness/contrast adjustment, image resizing, etc), the MSB-bits also change, so that the cipher-images cannot be decrypted back into the original images. In other words, encryption in spatial domain is not robust to common image processing.

XOR-based VC for GAS [3] is designed to implement sharing strategy for GAS with advantages such as perfect reconstruction of the secret, no pixel expansion and no code book requirement.

Multimedia steganography is one of the most recent and secure forms of steganography. Visual steganography is the most widely practiced form of steganography. It started with concealing messages within the lowest bits of noisy images or sound files. We shall perform steganography on image files and hide the message in an encrypted format, thus achieving a multiple cryptographic system. The most commonly used technique is Least Significant Bit steganography (LSB steganography)[4]. But instead of traditional LSB encoding, we will use a modified encoding technique which will first transform the image using a Lazy Lifting Wavelet transform and then apply LSB in the image that we have gotten.

Cheating in secret sharing schemes [7] has been widely investigated for decades. In 1999 Yang and Laih presented two cheating prevention VC schemes to break the misleading secrets forged by dishonest participants. The first method generates an additional verification share to check the validness to each share, where the verification share should be hold by the trusted authority (TA) to verify the validness to each share.

In this paper exploit a new method for cheating prevention is to embedd the keys in the form of integers into the shares of the secret image. This is random processes which replace the any pixels of the share images. And at the receiver side check the shares by extracting the keys.

2. Related Work

2.1 Review Stage

Thesis purpose is to transfer the image without any misbehaving or cheating factors. So firstly error is induced by choosing an output color is distributed to neighboring pixels using ordered dither block truncation coding. And the diffused image is encrypted by using permutation encoding. Here image encryption algorithm is in frequency domain using chaotic permutation. The encrypted image is devided into shares by region incrementing VC for general access structure (GAS).Since the shares are in the form of black and white pixels, the security is low. Also others should have to identify that something is hide in the shares. So these shares are hide into color images by using steganography. It doubles the security of the shares. At last keys are write into the shares for knowing any misbehaving is done or not.

2.2 Ordered Dither Block Truncation Coding

The ordered dither BTC (ODBTC) to improve the processing efficiency of the EDBTC [5] by employing look-up-table dither arrays. Yet, the quantization error cannot be compensated with the ordered dithering halftoning [8], and thus the ODBTC yields lower image quality compared to that of the EDBTC. The traditional algorithm will be firstly introduced for a better comprehension. Given an original image of size P × Q, and which is divided into many non-overlapped blocks of size M × N, then each block can be processed independently and eventually represented by two values. The independent processing property yields the additional excellent parallelism advantage. To begin with, the first-, second-moment, and the corresponding variance are obtained by,

$$\overline{x} = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N} x_{i,j}$$

$$\overline{x^2} = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N} x^2{}_{i,j}$$

$$\sigma^2 = \overline{x^2} - \left(\overline{x}\right)^2$$

where the variable $x_{i,j}$ denotes the grayscale pixel value in a block. Since BTC is a one-bit quantizer with a threshold x to binarize the block, the block is then replaced by bitmap as defined below,

$$h_{i,j} = \begin{cases} 1, if x_{i,j} \geq \overline{x} \\ 0, if x_{i,j} \leq \overline{x} \end{cases}$$

$$y_{i,j} = \begin{cases} b, if h_{i,j} = 1 \\ a, if h_{i,j} = 0 \end{cases}$$

where the variable $h_{i,j}$ denotes the bitmap, which is employed to address the arranged positions of low mean (a) and high mean (b). The concept of the BTC is to preserve the first- and second-moments of a block when the original value is substituted by its high or low means. Thus, the following two equations should be maintained,

$$m\overline{h} = (m-q)a + qb$$

$$m\overline{h^2} = (m-q)a^2 + qb^2$$

where m = M × N, and q denotes the number of pixels greater than x. The high and low means can be evaluated as follows,

$$a = \overline{x} - \sigma\sqrt{\frac{q}{m-q}}$$

$$b = \overline{x} + \sigma\sqrt{\frac{m-q}{q}}$$

Suppose the original image and the divided block are of sizes P × Q and M × N, respectively, and each block can be processed independently. For each block, the processing order of pixels is defined by the class matrix is adopted, the original image is divided into blocks of the same size 8 × 8 as that of the class matrix. Each divided block maps to the same class matrix, and all of pixels associated with number zero in the class matrix are processed firstly. The corresponding equations are given below,

$$v_{i,,j} = x_{i,j} + x'_{i,j}, where x'_{i,j} = \sum_{(m,n)\in R} \frac{e_{i+m,j+n} \times k_{m,n}}{sum}$$

$$e_{i,j} = v_{i,j} - y_{i,j}, where y_{i,j} = \begin{cases} 0. if v_{i,j} \leq 128 \\ 255, if v_{i,j} \geq 128 \end{cases}$$

where the variable $x_{i,j}$ denotes the current input grayscale value, variable $x_{i,j}$ denotes the diffused error accumulated from neighboring processed pixels, and variable $v_{i,j}$ denotes the modified grayscale output. The variable $y_{i,j}$ denotes the binary output in the bitmap, and variable $e_{i,j}$ denotes the difference between the modified grayscale output $v_{i,j}$ and the binary output $y_{i,j}$.

2.3 Permutation Encoding

An image encryption algorithm in frequency domain is transformed by Discrete Cosine Transform (DCT). Now try to develop block-based encryption algorithm. As know DCT is used in JPEG compression process in which the original image is divided into blocks of size 8 × 8 pixel, and each block is transformed by DCT. In order to compatible to JPEG compression, in the proposed algorithm the original image is also divided into the such blocks. The DCT coefficients of each block is scrambled with an chaos-based permutation, i.e Arnold Cat Map[6].

Arnold Cat Map is 2-D chaos map that transforms an element from a position to another position in the same area. Because

of DCT is lossy transformation, the proposed encryption algorithm is also lossy, that means the decrypted images are not exactly same as the original images. However, since on DCT domain, the encrypted images are robust to many image processing, such as JPEG compression, noising, etc. Need to randomize the pixels of plain-image before encrypt the DCT blocks. Thus, use Arnold Cat Map twice, the first for scrambling the pixels of plain-image in spatial domain, and the second for scrambling the DCT coefficients of each block 8 × 8. Outline of the proposed selective encryption algorithm is as follows,

1. Scramble the plain-image with Arnold Cat map.
2. Divide the scramble image into blocks of size 8 × 8
3. Apply DCT for each block.
4. Apply Arnold Cat Map to scramble the AC coefficients.
5. Apply IDCT to each block to get the cipher-image.

For decryption process, the process is same but in reverse order. Figure 1 shows each of encryption and decryption diagram of the proposed algorithm. The secret keys of the algorithm are b, c, and m. Image encryption and decryption requires the same keys. Because of the DCT is a lossy transformation, then the image decryption does not yield exactly same as the original image. The image size must be square to ensure the implementation of Arnold Cat Map. If the size is not square then it needs additional pixels so that the image size is square.

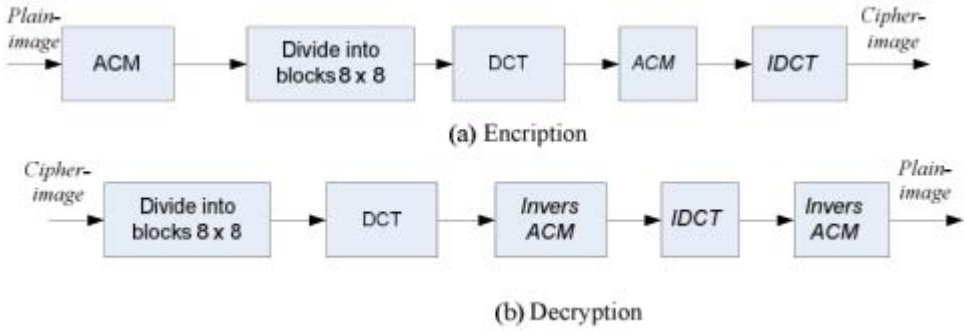

Figure 1: An encryption and decryption diagram of the algorithm.

2.4 Adaptive Region Incrementing XOR-Based VC

Here, describe the generation of shares for the adaptive region incrementing XOR-based VC [3]. A binary secret image with k security levels L_1,.....L_k are considered as input, as well as minimal qualified sets in Γ_0 assigned with initial security levels. First of all, the remaining qualified sets, which are not assigned the initial security levels, are automatically given the associated security levels by the assignment algorithm. When the security level assignment completes, the share construction begins. The construction is an approach derived from the XOR-based VC for GAS. Similarly, it comprises two parts:

• The construction of t pixels.
• The generation of the remaining n - t pixels.

For each time, a pixel s is constructed based on the security level of given secret pixel. A qualified set, which contains t participants, is randomly chosen from the set of qualified sets. At the next step, t − 1 shared pixels are constructed randomly, and the tth shared pixel is generated based on the t − 1 random pixels and pixel s. The remaining n − t shared pixels are iteratively constructed by pixel s and the former shared pixels that have been assigned values. Similarly, the iterative generation of the n − t shared pixels helps enhancing the visual quality. Note that, a qualified set Q is assigned a security level only when all the qualified sets contained in Q have been assigned the security levels. In the proposed method, all the minimal qualified sets are assigned initial security levels according to the sharing strategy, but some qualified sets are not, the above algorithm is used to automatically complete the security level assignment. For example, a sharing strategy with three participants {1,2,3} and a three security level secret image is considered. Let Γ_0 = {{1,2},{1,3}} and Γ_{Qual} = {{1,2},{1,3},{1,2,3}}. Then assign the initial security level L_1 to L_2 and assign L_2 to L_3. Then, the algorithm completes the security level assignment for qualified set {1,2,3}. The highest security level obtained from the qualified sets contained in {1,2,3} is L_2. Therefore, the security level of {1,2,3} is L_3.

2.5 Lazy Wavelet Transform Based Steganography in Image

Multimedia steganography is one of the most recent and secure forms of steganography. Visual steganography is the most widely practiced form of steganography. It started with concealing messages within the lowest bits of noisy images or sound files [4]. The Visual Cryptographic Steganography Model will encrypt the message using the symmetric key algorithm, and after that hide the data into a video file, which will act like cover. At the receiving side, will first extract the hidden data from the received video file, and then decrypt it using the shared key that already know.

2.5.1 Hiding Procedure

The secret data is hidden in sequential frames. Each frame is treated as a different image and an image steganography method is applied to them. Use the 2D - Lazy Wavelet Transform on each frame to get four sub-bands. The data is then hidden in these four subbands using LSB to hide 3 bits in each element of the subband. The length of the data stream

which is encoded into the image is stored in the cover image using simple LSB. The proposed method consists of the following phases:

1. Encrypting the Given Secret Data File

Given the secure data that want to send, first apply encryption on it so that the data is converted to a cipher text and is not readable. Then apply the Rijndael 256 bit algorithm on the secret data, using the utility mcrypt. This provides reasonable amount of security with good encrypting speed performance.

2. Converting Given Encrypted Cipher Data into a Stream of Bits

Since will be dealing with the individual bits of the encrypted file, which will hide inside the cover image, will convert the given file into a series of bits. This will read the file character by character (since after encryption, the file has been converted to only ASCII characters), and then break the eight bit characters into strings of bits. This bit stream can now be encoded into the image.

3. Applying Lazy Wavelet Transform on the Image

On these separate images, apply image transformation techniques. Use wavelets to transform the given image in the spatial domain into the frequency domain. Values in the multimedia data are stored as integers, but many wavelet transforms return real values, which cause data loss when stored in a multimedia file and then retrieved [7]. To overcome this, use the Lazy Lifting Scheme, by applying an Integer Wavelet Transform. The lifting scheme calculates wavelet transforms in an efficient way, and can easily be converted to an integer transform. It can easily do this by adding some rounding operators.

4. Hiding Three bits in Transform Coefficients of the Four Sub-bands

Performing the Integer Wavelet Transform on the image will give us four subbands for each image. Will hide the message in the least significant bits (LSB) of the transform coefficients. With three LSBs to store the bits in each transform coefficient, get a PSNR of 31.23.

2.6 Cheating Prevention

To prevent the cheating or misbehaving in visual secret sharing , the method need to write the key into the shares. The keys are in the form of integers. That is binary key is converted into integers and then write it in the shares with random order. That is randomly replace the keys in the cover images. To check the originality of the share have to check the secret message are presented on that share or not. The proposed scheme can recognize the fake share while collecting the shares from participant by checking the secret key embedded within them before staking, if the key is intact then that is the original share otherwise it is fake share which can detect possible cheating in VCS by validation. No need to send extra share for verification. The algorithm for writing key is given below,

Step 1: Consider 4 shares S1[2i][2j], S2[2i][2j], S3[2i][2j], S4[2i][2j] , and the secret key.

Step 2: Consider the secret key in integer formed matrix, M[x][y].

Step 3: Using pseudo random, create locr[x][y], and locc[x][y] , which denote some random locations of row and column respectively.

Step 4: Then replace the key in the shared images.

Step 5: Extract the keys from shares and then check the keys are same or not.

Step 6: Misbehave if keys are not same and proceeds if same.

Step 7: End.

3. Conclusion

The proposed novel image sharing scheme such as error diffusion, permutation encoding, steganography and cheating prevention yields excellent image security and faster image sharing strategy. Since the secret images are grayscale images, first apply EDBTC, then the secret image is encrypted based on permutation. Then the shares of secret image is hide into meaningful cover images by using steganography and cheating prevention algorithm into host images. This technique provides a high level security for the share images.

4. Acknowledgment

The Author would like to thank Liyamol Aliyar. Assistant Professor, Department of Information Technology, Ilahia College of Engineering and Technology, Muvattupuzha for her moral and technical support.

References

[1] M. Naor and A. Shamir, “Visual cryptography,” in Advances in Cryptology (Lecture Notes in Computer Science), vol. 950. Berlin, Germany: Springer-Verlag, 1995, pp. 1–12.
[2] E. J. Delp and O. R. Mitchell, “Image compression using block truncation coding,” IEEE Trans. Commun., vol. 27, no. 9, pp. 1335–1342, Sep. 1979.
[3] Xiaotian Wu and Wei Sun, “Extended Capabilities for XOR –Based Visual Cryptography”, IEEE Transactions On Information Forensics And Security, Vol. 9, No. 10, October 2014.
[4] Khushman Patel, Kul Kauwid Rora, Kamini Singh, Shekhar Verma, “Lazy Wavelet Transform Based Steganography in Video”,2013 International Conference on Communication Systems and Network Technologies.
[5] Jing-Ming Guo, “Improved Block Truncation Coding Using Optimized Dot Diffusion”, IEEE transactions on image processing, vol. 23, no. 3, march 2014.
[6] Rinaldi Munir, “A Block-based Image Encryption Algorithm in Frequency Domain using Chaotic Permutation”, IEEE transactions 2014.
[7] Biswapati Jana, Partha Chowdhuri, Madhumita Mallick ,Shyamal Kumar Mondal , “Cheating Prevention in Visual Cryptographic using Steganographic System”, Designs, Codes and Cryptography, Vol. 38, pp. 219–236, 2014.

Author Profile

Anju Mohan received the Bachelor of Technology degree in Information Technology from Anna University, Chennai. She is currently doing Master of Technology degree in Computer Science and Engineering with Specialization in Information Systems from Mahatma Gandhi University, Kerala.