Visual Cryptography Scheme with RDH Algorithm for Color Images

[1]Arun T Nair
Dept. of Electronics and Communication .
KMCT College of Engineering
Calicut, India

[2]Ms. Ramya N
Dept. of Electronics and Communication .
KMCT College of Engineering
Calicut, India

Abstract **-In this paper, a region based visual cryptography scheme deals with sharing of image based upon splitting the image into various shares. The main concept of visual secret sharing scheme is to encrypt a secret image into n meaningless share images. It cannot leak any information about the original image unless all the shares are obtained. All the Shares of original image is embedded into host images by means of reversible data hiding (RDH) algorithm. Algorithm also deals with the extraction of share's and host images. The proposed algorithm enhances the contrast of a host image to improve its visual quality. The highest two bins in the histogram are selected for data embedding so that histogram equalization can be performed by repeating the process. The original image is obtained by superimposing all the shares directly, so that the human visual system can recognize the shared secret image without using any complex computation all devices. Propose a region based visual secret sharing scheme with RDH algorithm for color images with no pixel expansion and high security.**

Keywords - Visual Cryptography, Visual Secret Sharing, Reversible Data Hiding, Histogram Modification, Contrast Enhancement.

I. INTRODUCTION

Security as a condition is the degree of resistance to, or protection from, harm. It applies to any vulnerable and valuable asset, such as a person, dwelling, community, nation, or organization. Establishing or maintaining a sufficient degree of security is the aim of the work, structures, and processes called "security". Security management for networks is different for all kinds of situations. A home or small office may only require basic security while large businesses may require high maintenance and advanced software and hardware to prevent malicious attacks from hacking and spamming. Security attack is an intelligent act that attempt to intrude the security services and violate the security policy of a system. Collection of tools to protect data and resources from hackers is known as computer security. The security measures for protecting data during data transmission through network is known as network security and protecting data during transmission across inter connected network is known is internet security. Security measures to prevent, detect and correct security violation during transmission of data across interconnected networks.

Visual Cryptography[1] is the scheme which encrypts image using cryptographic technique, but decrypt original image without any cryptographic computation. This scheme is secure and easy to implement. The cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that decryption becomes a mechanical operation that does not require a computer. Visual Cryptography is a method of encrypting a Secret image into shares such that stacking a sufficient number of shares reveals the secret image. Visual Secret Sharing (VSS), one of the secret communication technologies, aims to share a secret image with several participants by a dealer. Reversible data hiding (RDH)[2] has been intensively studied in the community of signal processing. Also referred as invertible or lossless data hiding, RDH is to embed a piece of information (ie, the encoded values of the shares from visual cryptography) into a cover image to generate the marked one, from which the original image can be exactly recovered after extracting the embedded data. The technique of RDH is useful in some sensitive applications where no permanent change is allowed on the cover image. To evaluate the performance of a RDH algorithm, the hiding rate and the marked image quality are important metrics. There exists a trade-off between them because increasing the hiding rate often causes more distortion in image content. To measure the distortion, the peak signal-to-noise ratio (PSNR) value of the marked image is often calculated. Firstly, the two peaks (i.e. the highest two bins) in the histogram are found out. The bins between the peaks are unchanged while the outer bins are shifted outward so that each of the two peaks can be split into two adjacent bins. To increase the embedding capacity, the highest two bins in the modified histogram can be further chosen to be split, and so on until satisfactory contrast enhancement effect is achieved. To avoid the overflows and underflows due to histogram modification, the bounding pixel values are pre-processed and a location map is generated to memorize their locations. For the recovery of the original image, the location map is embedded into the cover image, together with the message bits and other side information.

II. RELATED STUDY

Visual cryptography, introduced by Noar and Shamir (1995)[3], is a type of secret sharing techniques for images. The idea of visual cryptography scheme is to split an image into collection of shares which separately reveals no information about the original secret image. The image is composed of black and white pixels, and can be recovered by superimposing all the shares without any computations involved. By applying the Noar and Shamir 2-out-of-2 visual cryptography algorithm, two shares are created, which separately reveals no information about the original secret image. It can only be recovered when both of the shares are obtained and superimposed. Note that the size of the image is expanded by the factor of 2. In Tsung-lieh [4] proposed a secret sharing scheme which is described for binary image, with no pixel expansion. The rotation degree was 180 for revealing the second secret image. In this scheme the encryption process include three stages: DSP (dividing and separating process):SP(sticking process):CMP(camouflaging).In DSP, the first function is to divide each secret image into blocks with n x n size, and the second function was to separate each block of the secret image into two subsets obtained by DSP to generate the share images, and two subsets of secret image were stuck to obtain both the share image respectively. The first subset of secret image 2 was directly stuck on the corresponding position of secret image 1. While the second subset of secret image 2 is rotated 180 degree and stuck to the corresponding position of share 2. The function of the camouflage is to make the density of the black pixel on each block of one share image to be equal by referencing the maximum block density of all blocks. Though the scheme has no pixel expansion it still faces the problems like time complexity that it takes long time and low contrast of image. This scheme adopted two rectangular share images to share two rectangular secret images. Divide each secret image into blocks with n*n size. Separate each block of the secret image into subset by dsp. Time complexity and low contrast of image. There is No pixel expansion. S j shyu [5] Lin proposed a new approach for colored visual cryptography scheme. Proposed three different approaches for color image representation. In first approach, colors in the secret image can be printed on the shares directly. It works similar to basic visual cryptography model. Limitations of this approach are large pixel expansion and quality of decoded image is degraded. In second approach, separate three color channels are used: Red, green, blue for additive model and cyan, magenta and yellow for subtractive model. Then normal visual cryptography scheme for black and white images is applied to each of the color channels. This approach reduces the pixel expansion but quality of image gets degraded. In third approach, binary representation of color of a pixel is used and secret image is encrypted at bit-level. This results in better quality of image. Multiple Secret Sharing Scheme introduced by Wu and Chen [7]. Visual cryptography were focused on securing only one image at a time. Cryptography scheme to share two secret images in two shares. In this scheme, two secret binary images can be hidden into two random share namely A and B. The first secret can be seen by stacking the two shares, denoted by A$\otimes$ B. The second secret can be obtained by rotating A by 90 degree anti-clockwise. Image quality high. Reversible data hiding method is introduced by C. W. Honsinger and P. Jones [7]. It is carried out in the spatial domain. It uses modulo 256 addition to embed the hash value of the original image for authentication. The embedding formula is Iw=(I+W)mod(256), I denotes the original image, Iw the marked image, and W=W(H(I),K) the watermark, H(I) denotes the hash function operated on the original image I, and K secret key. Because of Using modulo 256 addition, the over/underflow is prevented and the reversibility is achieved. Disadvantages of this scheme is presence of Salt-and-pepper noise.

II. THE PROPOSED SCHEME

The image that carries secret information is converted in to multiple secret shares using encryption model and the original image is obtained from the shares by decryption model and these shares are embedded into cover images by RDH algorithm. Both models use secret keys to increase security. The Specialty of this scheme is to generate any number of shares and to maintain the visual quality of the image.

A.The Encryption Model

Shares are obtained from the original secret image by using the generalized format as explained in the encryption model. The encryption model comprises of first finding the number of shares (n) to be generated. The user can give any value for n. Before separating the shares, the basic matrices are first constructed based upon the number of shares to be created. A random Key is generated at the encryption side based on block n x n. Usually the block size will be 4 x 4 or 8 x 8.

B.Construction of Basic Matrices

The original image A is the input; If we want to create 2^b number of shares then b number of basic matrices are constructed, where b >= 2. The basic matrices are obtained by dividing each and every pixel value in A by b. For example, let the pixel value in A is 127, b is 3. 127/3 = 42.33. So the corresponding pixel value in the first and second basic matrix is 42 and the third basic matrix is 43. Therefore 42+42+43 = 127. If b = 3 then the number of shares to be produced are 2^3 = 8. The shares can be constructed by XOR-ing basic matrices on different combination.

Algorithm1: Encryption model

```
Input: The original image A, Secret Key K.
Output: Shares S1, S2
1   Construct basic matrices    B1,B2,…………..Bb.
2   Divide the basic matrices into blocks.
3.  For each block do the following to create shares.
        S1 = B1XOR K
        S2 = B1 XOR B2
        S3 = B2 XOR S1
```

S4 = S1 XOR S2
S5 = S2 XOR S3
S6 = S3 XOR S4
………………...
Sn= Sn-3 XOR

4. Encoded data of shares are embedded into the cover image by means of RDH algorithm.
5. Cover images are transmitted to different persons.

The original image A and the secret key K is read from the user. Column permutation can be performed on the original image before basic matrices are constructed to increase security. The algorithm to be presented is primarily for gray-level images but can be easily extended to color images.

C. RDH ALGORITHM WITH CONTRAST ENHANCEMENT

1.Data Embedding by Histogram Modification

The algorithm to be presented in color images. Given an bit gray-level image I, the image histogram can be calculated by counting the pixels with a gray-level value J for J= {0,1,……….254,255 }. We use h_i to denote the image histogram so that h_i (j) represents the number of pixels with a value. Suppose i consists N of different pixel values. Then there are nonempty N bins in H_i, from which the two peaks (i.e. the highest two bins) are chosen and the corresponding smaller and bigger values are denoted by I_S and I_R, respectively. For a pixel counted in h_i with value i, data embedding is performed by

$$i' = \begin{cases} i-1, & \text{for } I_s \\ I_s-s, & \text{for } i=I_s \\ i, & \text{for } I_s<i<I_R \\ I_R+s, & \text{for } i=I_R \\ i+1, & \text{for } i>I_R \end{cases} \quad \ldots\ldots\ldots\ldots\ldots (1)$$

Where i' is the modified pixel value, and S is the k-th bit message of encoded (JPEG) shares (0 or 1) to be hidden. By applying Eq. (1) to every pixel counted in H_I, totally $H_I(I_S)+H_I(I_R)$ binary values are embedded. Given that there is no bounding value (0 or 255) in I otherwise pre-process is needed, there will be N+2 bins in the modified histogram. That is, the bins between the two peaks are unchanged while the outer ones are shifted outward so that each of the peaks can be split into two adjacent bins (i.e.I_S-1 and I_S,I_R and I_R-1, respectively). The peak values Is and I_R need to be provided to extract the embedded data. One way to keep them is to exclude 16 pixels in I from histogram computing. The least significant bits (LSB) of those pixels are collected and included in the binary values to be hidden. After applying Eq. (1) to each pixel counted in for data embedding, the values of Is and I_R (each with 8 bits) are used to replace the LSBs of the 16 excluded pixels by bitwise operation. To extract the embedded data, the peak values need to be retrieved and the histogram of the marked I' image is calculated excluding the 16 pixels aforementioned. In the extraction process, the last split peak values are retrieved and the data embedded with them are extracted with Eq. (2). Ie,

$$S = \begin{cases} 1 & \text{for } i'=I_s-1 \\ 0 & \text{for } i'=I_s \\ 0 & \text{for } i'=I_R \\ 1 & \text{for } i'=I_R+1 \end{cases} \quad \ldots\ldots\ldots\ldots\ldots(2)$$

After restoring the histogram with Eq.(3), the data embedded with the previously split peaks can also be extracted by processing them pair by pair. At last, the location map is obtained from the extracted data to identify the pixel values modified in the pre-process.

$$i= \begin{cases} I'+1, & \text{for } i'<I_s-1 \\ I_s, & \text{for } i'=I_s-1 \text{ or } i'=I_s \\ I_R, & \text{for } i'=I_R \text{ or } i'=I_R+1 \\ i'-1, & \text{for } i'>I_R+1 \end{cases} \quad \ldots\ldots\ldots.(3)$$

2.Pre-Process for Complete Recovery: In the aforementioned algorithm, it is required that all pixels counted in H_I are within [1……254]. If there is any bounding pixel value (0 or 255), overflow or underflow will be caused by histogram shifting. To avoid it, the histogram needs to be pre-processed prior to the histogram modification operations. Specifically, the pixel values of 0 and 255 are modified to 1 and 254, respectively. Therefore, no overflow or underflow will be caused because the possible change of each pixel value is i. To memorize the pre-processed pixels, a location map with the same size as the original image is generated by assigning 1 to the location of a modified pixel, and 0 to that of an unchanged one (including the 16 excluded pixels). In the extraction and recovery process, it can be obtained from the data extracted from the marked image so that the pixels modified in the pre-process can be identified. By restoring the original values of those pixels accordingly, the original image can be completely recovered.

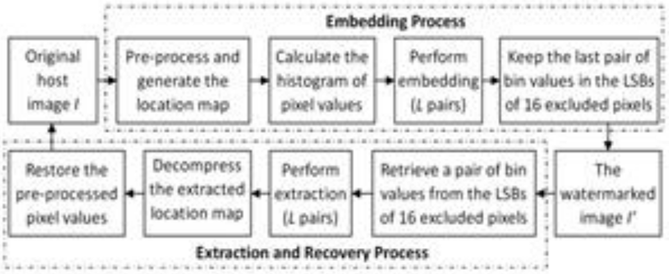
Embedding Process
Original host image I
Pre-process and generate the location map
Calculate the histogram of pixel values
Perform embedding (L pairs)
Keep the last pair of bin values in the LSBs of 16 excluded pixels
Restore the pre-processed pixel values
Decompress the extracted location map
Perform extraction (L pairs)
Retrieve a pair of bin values from the LSBs of 16 excluded pixels
The watermarked image I'
Extraction and Recovery Process

Fig.1. Procedure of the RDH algorithm

Reversible data hiding (RDH) algorithm is proposed for digital images. Instead of trying to keep the PSNR value high, Besides the PSNR value, Relative contrast error (RCE), relative entropy error (REE), Relative mean brightness error (RMBE) and Relative structural similarity (RSS) [8] used in were calculated between the original and contrast-enhanced images to evaluate the enhancement effect and image quality. The RCE and REE values greater than or equal to 0.5 indicate the enhanced contrast and increased image data, respectively. The less difference in mean brightness from the original image, the closer RMBE is to 1. The greater the structural similarity between them, the closer RSS is to 1.

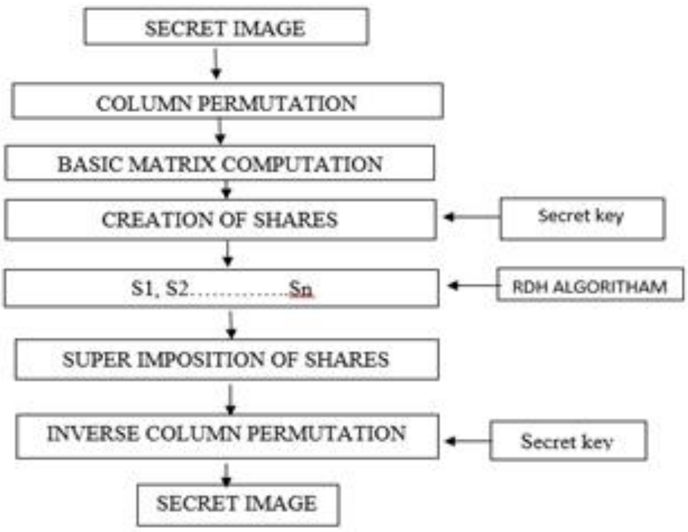

Fig.2. The general block diagram of proposed scheme

D.The Decryption Model

Once all the cover images are received at the receiver end, The cover images are decoded into shares and cover images by means of RDH algorithm. Then, the shares are superimposed (XORed) in order to get the original image. The secret key K also XORed with shares.

D = S1 XOR S2 XOR S3 . . . XOR Sn XOR K

The decrypted image D has same visual quality as original image A in the sender side. If the receiver has all the shares and key then only he can decrypt. Otherwise he can't get any details about original image.

IV. EXPERIMENTAL RESULTS

A good visual secret sharing scheme with RDH algorithm must have lower pixel expansion and higher contrast. Our proposed scheme did not use a pattern book to generate a share images. We paid more attention to evaluate the contrast of revealed images and the security result of the generated share images. The data of shares are embedded in to cover images by RDH algorithm. The marked images were obtained by splitting L pairs of histogram peaks for data embedding, respectively. It can be seen that the embedded data were invisible in the contrast-enhanced images. The more histogram peaks were split for data embedding, the more contrast enhancement effect was obtained. Although the PSNR value of the contrast-enhanced images decrease with the data hiding rate, the visual quality has been preserved. We used MATLAB tool to generate the code according to the algorithm. PSNR=34.16 db, RCE=.5072, RMBE=1.0012, RSS=.8137, REE=.500, RMSE=4.7521.

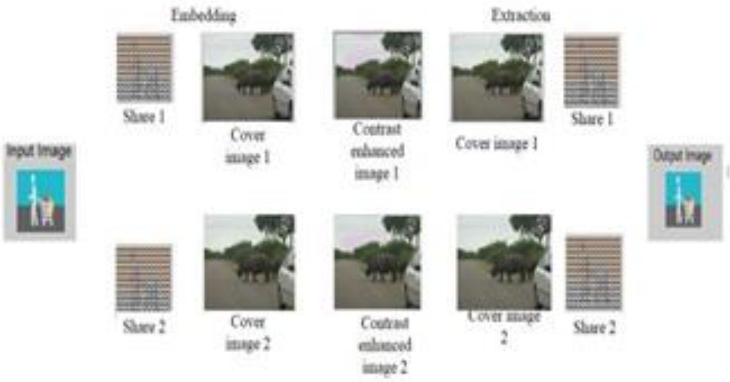

Fig. 3.Expirimental results

V. CONCLUSION

We established a Region Based Visual Cryptography Scheme with RDH algorithm for Color Images. The objective function is secret sharing of information. In this paper, a Visual secret sharing scheme with no pixel expansion has been proposed. It can be used to create multiple shares without any pixel expansion. The shares are embedded in to cover images by RDH algorithm with the property of contrast enhancement. To reveal the secret image, n share images were just stacked and the recovery images could be recognized by the Human Visual System, no other devices were needed to reveal the secret image. If the receiver has all the shares and key then only he can decrypt. Otherwise he can't get any details about original image. Thus our proposed scheme achieved the purpose of the visual secret scheme is solving the critical problem of pixel expansion. The column permutation operation, secret key and RDH algorithm is also concentrated on the security of the secret information.

VII. ACKNOWLEDGMENT

I am thankful to my project guide Asst.Prof Mrs.Ramya N and Head of the Department Mrs. Nishidha.T. for their support, remarks and suggestions, which were essential to carry out the survey. I am also grateful to all the staff members of Electronics & Communication Engineering Department of KMCT College of Engineering, Calicut for their assistance and support in improving the review paper significantly. I also thank my family and friends for all the support given by them.

REFERENCES

[1] Vol. 2, Issue 3, March 2013 Copyright to IJARCCE www.ijarcce.com "Region Based Visual Cryptography Scheme for Color Images "D. R. Denslin Brabin1, Divya Venkatesan2, Divyalakshmi Singaravelan3, Lekha Sri Rajendran4 Associate Professor, IT Department, Jaya Engineering College, Chennai, India1 Students, IT Department, Jaya Engineering College, Chennai, India 2, 3, 4.

[2] IEEE signal processing letters, VOL.22, NO.1, JANUARY 201581"Reversible Image Data Hiding with Contrast Enhancement "Hao-Tian Wu, Member, IEEE, Jean-Luc Dugelay, Fellow, IEEE, and Yun-Qing Shi, Fellow, IEEE.

[3] M.Naor and A.Shamir, "Visual Cryptography" Proc. Adv. Cryptography: Eurtocrypt, LNCS 95, 1995

[4] S J Shyu , Shi-Jinn Horng a, Kai-Hui Lee , Pei- Ling Chiu, Tzong-Wann Kao,secret sharing scheme for multiple Secrets without pixel expansion",Pattern Recognition,2000.

[5] Tzung-Her Chen, Kai-Hsiang Tsao, and Kuo-Chen Wei,"Multi-Secrets Visual Secret Sharing", Proceedings of APCC 2008, IEICE, 2008

[6] Bert W. Leung, Felix Y. Ng, Duncan S. Wong, "On the security of a visual cryptography scheme for color images", Pattern2009.

[7] C.W. Honsinger, P. Jones, M. Rabbani, and J. C. Stoffel, "Lossless Recovery of an Original Image Containing Embedded Data," U.S. Patent6 278 791 B1, Aug. 21, 2001.

[8] M.-Z.Gao,Z.-G.Wu,andL.Wang,"Comprehensive evaluation for Hbased contrast enhancement techniques," Adv. Intell.Syst. Applicat., vol. 2, pp. 331-338, 2013.