International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 - 5161

Available at http://inpressco.com/category/ijcet

Research Article

Visual Cryptography Scheme for Gray Scale Images based on Intensity Division

Pradeep Kumar Sharma[Á*] and Hari Mohan Singh[Á]

[Á]Department of Computer Science & IT, SHIATS, Allahabad, India

Accepted 10 January 2014, Available online 01 February 2014, **Vol.4, No.1 (February 2014)**

Abstract

Broadly speaking a term Cryptography used to secure & hide the original information of a message from the unauthorised users. First time used to encrypt a plaintext into cipher text where a key was associated at the time of encryption to change original content into some other form i.e. decrypted message. And same key was used to decrypt that message into original form. In the modern communication era, people begin to transmit huge digital and multimedia information through the public network. During the transmission, most important thing is to secure data, for which a different kind of cryptography used, known as Visual Cryptography Scheme (VCS). This paper presents a new VCS approach & its implementation for gray scale images based on Intensity Division. In this approach the intensity of a pixel is divided into MSBs & LSBs. Two shares are generated using MSBs and at the receiver's end stacking of these provide the revealed image. It also improves the quality of shared images even after decryption of the secret image. This is finally compared with the original Host image. Performance of this approach can be measured by calculating MSE & PSNR and Histogram.

Keywords: *VCS, Secret image, Security Keys, Intensity, MSB's, LSB's, MSE & PSNR*

1. Introduction

In the fast growing era, the entire communication channels are Hi-Tech. These are like Internet broadband, Wi-fi & others make it easy to access multimedia or digital data within chunk of seconds. As the growing need of new technology, three most important things are database, network & security of information. Because huge bulk of data transmit from source to destination over to public networks on the daily basis. It is quite difficult to send and receive at other end in the same form, quantity & quality. It may be cause by various attacks like brute force etc. and probability to be hacked by some unauthorised third party in transit. So some challenges came into existence regarding to Information security & Data integrity during transmission. Especially, when this type of data is used for authentication purposes e.g. Biometric devices, Close circuit cameras, Medical diagnosis or e-court evidence. To resolve these problems different researchers have proposed various methods.

Cryptography is a technique used to hide the meaning of a message and is derived from the Greek word kryptos (hidden), where sender and receiver agreed upon a message scrambling protocol & methods for encrypting and decrypting messages. The meaning of a text message is converted into another form i.e. encrypted (encode) and at the receiver end again converted into the original form i.e. decrypted (decode). Some common elements of the cryptography are encryption, decryption, key, secure line & public line. Encryption is the process of locking up information using cryptography. Information that has been locked up this way is said to be encrypted. Decryption is the process of unlocking encrypted information using cryptography. Key is a secret, like a password, which is used to encrypt and decrypt information. There are a few different types of keys used in cryptography. Secure line is a transmission channel which can be used to send information secretly (in other words, nobody can intercept and read that data). Public line is a transmission channel which cannot be used to send information secretly - the information can be "overheard" easily. A public pay phone is an excellent example of this; so is the Internet. In this respect Encryption techniques were categorised into three classes namely, (a) Classical encryption technique, (b) Medieval encryption technique and (c) Modern encryption technique. The Classical encryption technique consist of various distinct models like

- Symmetric cipher model where a secret key is associated with the message to encrypt and the same key is used to decrypt the message.
- Substitution technique, where each letter of the plaintext message is replaced by a different letter.
- Ceaser cipher, where each letter of plaintext are shifted to a certain number of spaces.
- In transposition technique, the letters of message are rearranged in some other form like – dog, odg, dgo etc.

While modern cryptography technique can be describe by two criteria algorithms as

*Corresponding author: **Pradeep Kumar Sharma**

- Symmetric key algorithm (private key cryptography) based on single shared key to encrypt & decrypt the message. Ex. DES, AES
- Asymmetric key algorithm (Public key cryptography) based on two keys, public key & private key. Ex. RSA

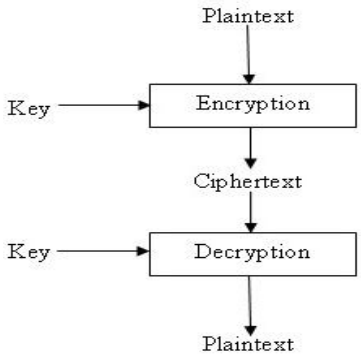

Figure 1 – Text encryption technique

Today it is in the fashion to transmit textual data in visual form in order to increase security. By doing so it is quite possible that the whole or part of the textual data cannot be hacked in transit. But to secure/encrypt the meaning of a visual or multimedia message, a new cryptography technique was introduced by Naor & Shamir in 1995. They proposed the (2, 2) VC scheme, each secret image is divided into two shares such that no information can be reconstructed from any single share. Different researchers have proposed variety of visual cryptography schemes. It uses only human visual system to identify the secret from the stacked image of some authorized set of shares. An example of the (2, 2) –VCS scheme is shown in Figure2 below where the share images are 2 × 2 times larger than the original secret image. The disadvantage of conventional visuals secret sharing schemes is that it applied for binary image only.

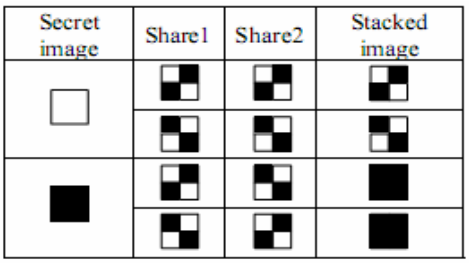

Figure2: Sharing Scheme for black & white

One of the researcher proposed halftone visual cryptography which increases the quality of the meaningful shares based on binary image i.e. black & white. This VCS is limited to binary images only and cannot work on gray scale or color images. Visual Threshold Scheme based on two parameters, pixel expansion and contrast. Simulation results demonstrate that the contrast is close to optimality, and meanwhile the pixel expansion was the minimal. One more approach proposed that the frequency of white pixels to show the contrast of the recovered image. The scheme is non expansible (same in size) and can be easily implemented on a basis of conventional VSS scheme. A new (k, n) ProbVSS schemes with non-expansible shadow size based on the probabilistic method. In the same way a technique was proposed by researcher where 2 out of 3 visual multiple secret sharing method using generalized random grids, visual secret sharing by using generalized random grids is a novel approach for generating nonexpansible shares by artfully utilizing various random variables. Stacking the shares together, secret image can be revealed. An approach was proposed where two new constructions for the secret color images sharing. One is a (n, n) threshold scheme, which can be constructed by using XOR operation. The other is a (2, n) threshold scheme, which can be constructed by using AND & XOR operations. There is a wide scope to research more in this area. We also work on visual cryptography and given a new technique base on intensity division. Two common drawbacks of the visual cryptography scheme (VCS) are the large pixel expansion of each share image and the small contrast of the recovered secret image.

The rest of this paper is organized in the following manner: section 2, the related work is reviewed; the proposed approach is discuss in section 3; in section 4, experimental results are shown, finally the last section gives the conclusion of this paper.

2. Related work

Lin et al. have proposed a technique to improve contrast of the reconstructed secret image. For this purpose they take distribution of black pixels in blocks of the size 2x3. Where, the gray scale secret image is converted into a halftone by using the error diffusion technique. But the main drawback of that approach was slight better contrast of the recovered image. Wang et al. proposed a new visual cryptography technique to improvise Lin et al. approach. This technique was a non-expansion and reversible secret image sharing based on multi-level encoding. Encode the secret image into two meaningless shadow images; therefore, their scheme was a (2,2) secret image sharing scheme. For the security purpose, used a key k to randomly generate an image of the same size of the secret image, which was used to permute *I*, and generate the permuted secret image *P*. After the permutation, divide *P* into non-overlapping 2x2 blocks, and generate the codebook by the following equation:

m = (2 * x + y) mod16

Features of this Approach

- This was based on block wise
- Based on multilevel encoding
- Use of codebook
- Photoshop software used to transform gray scale image G into halftone secret image I
- In the codebook m, x, y are decimal values and P_k, S^1_k & S^2_k are their corresponding secret blocks

- Where white color was shown by '0' bit & black color by '1' bit
- Equation (1) was used to recover permuted secret image *P*
- Key $_k$ was used to calculate inverse permutation & reconstruct the original secret image *I*
- scan the 2x2 blocks of secret image in the order of left to right, up to down.
- Without any distortion on the contrast quality

Resultant of that approach was, it is capable to test two images sized 512x512 as input, easy to use secret key combination with the help of codebook & comparatively low computation.

3. Proposed Approach

By seeing the above given approach, it is clear that this scheme is not much better to resolve visual cryptography problems on various ground like encryption, decryption, contrast & security keys. In this paper we have proposed a new visual cryptography technique which is solely based on intensity division of a pixel selected randomly from the gray scale image. A single gray scale image of the size 256x256 is taken as a Host image. Now calculate decimal values of each pixel. A random pixel is selected from this image and converts its decimal value into binary (8bits). The value of a pixel obtained so is divided into five (5) bit Most Significant Bits (MSB) & three (3) bit Least Significant Bits (LSB). The encryption of the secret image is followed by two authentication keys K_1 & K_2 and generates two shares. After that stacking these two shares & compare with the original Host image, the revealed image will be obtained without the loss of contrast and much pixel expansion. To accomplish this task, we have define two algorithms namely (1) Share Generation and (2) Share combination.

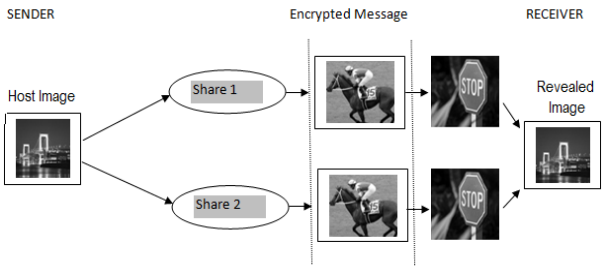

Figure3: Proposed model block diagram of VCS

Consider a gray scale host image I which has dimension $\mathbf{m} \times \mathbf{n}$. Then N represents number of pixels $\boldsymbol{N = m \times n}$. So the gray scale value at each pixel of the image is denoted by $\boldsymbol{P_i}$ where $\boldsymbol{P_i} \in (0..255)$, $i = 1,2,3.....N$. $\boldsymbol{P_i}$ can be denoted by 8 bits. So each single bits of $\boldsymbol{P_i}$ is denoted by $b(\boldsymbol{P_i},7), b(\boldsymbol{P_i},6), b(\boldsymbol{P_i},5)..b(\boldsymbol{P_i}, 0)$.

A. Share Generation Algorithm

Step-1: Convert the intensity values of Pi into 8 bit binary Then individual bit of any pixel $\boldsymbol{P_i}$ can be represented in binary form by following equation

$$\boldsymbol{b(P_i, u) = \left\lfloor \frac{P_i}{2^u} \right\rfloor \ mod\ 2} \quad (1)$$

Step-2: Calculated 8 bits for a particular pixel can be verified by-

$$\boldsymbol{P_i = \sum_{u=0}^{7} b(p_{i,u}).\ 2^u} \quad (2)$$

Where u =0,1,2...7

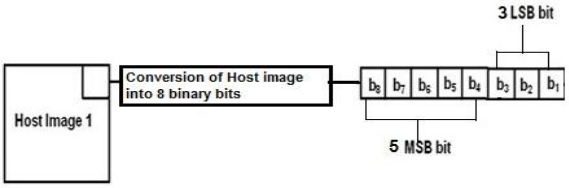

Figure 4: Iintensity conversion of P_i into 8 bit binary

Step-3: Remove 3 LSBs from all pixels to get new intensity range from (0 – 31)

$$\boldsymbol{I_{msb} = I - (3LSBs)} \quad (3)$$

Step-4: Input a secret key K_1 from the sender

$$\boldsymbol{K_{1m} = \frac{K1}{\prod_{i=1}^{no.of\,digit\,(K1)} (10)}} \quad (4)$$

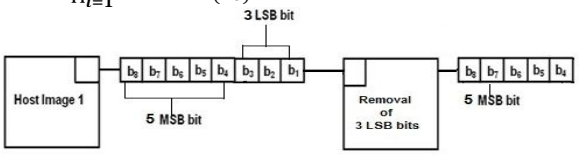

Figure5: Intensity reduction from 8 bits to 5 bits MSBs

Step-5: Divide intensity of each pixel into two different intensities by using K_{1m}

$$\boldsymbol{S_1 = P_i\ (Imsb) * K_{1m}} \quad (5)$$

$$\boldsymbol{S_2 = P_i\ (Imsb) - S_1} \quad (6)$$

$S_{1m} = \lfloor S_1 \rfloor$

$S_{2m} = \lceil S_2 \rceil$

Step-6: Convert the S_1 & S_2 into five bit binary form

Step-7: Take a secret key K_2 from sender

$$\boldsymbol{K_{2m} = K_2\ mod\ 32} \quad (7)$$

$S_{1mf} = Ex\text{-}Or\ (S_{1m}, K_{2m})$

$S_{2mf} = Ex\text{-}Or\ (S_{2m}, K_{2m})$

Step-8: Convert S_{1mf} and S_{2mf} into decimal,

The image obtain from both is called Share1 & Share2 respectively.

B. Share Combination Algorithm

The two share images that are transmitted via internet holds the secret image, hence to reveal the secret image both the share images has to be stacked i.e. superimposing first input image with second input image.

Step1 – Take Secret key K_1, K_2 and calculate the following

$S_{1m} = Ex\text{-}Or\ (S_{1mf}, K_{2m})$

$S_{2m} = Ex\text{-}Or\ (S_{2m}, K_{2m})$

Step2 – Convert S1m and S2m into decimal

Step3 – Add S_{1m} and S_{2m}
$P_i\ (I_{msb}) = S_{1m} + S_{2m}$

Step4 – Apply Gray scale contrast stretching

$$P_{im} = \frac{255}{max - min}\ (P_i(I_{msb}) - min)$$

When max is higher value of $Pi_{(msb)}$ and min is lower value of I_{msb}

Step5 - P_{im} is the recovered shared image.

Compare Host image with revealed image

After the conversion, share generation & combination the revealed image is compared with the host image for contrast.

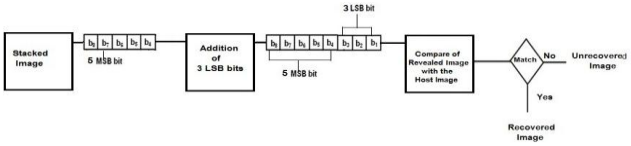

Figure 6: Block diagram of Comparison between Recovered image and Original image

4. Experimental Result

Now, we demonstrate the performance of our proposed technique. We tested gray scale image of 256x256 pixels of baboon. The host image is encrypted using the above algorithms and obtain the revealed image after stacking two share. The performance of the technique is measured by two methods these are PSNR (Peak signal to noise ratio) & Histogram in two ranges (0-31 & 0-255).

Experiment Result of an image of Baboon

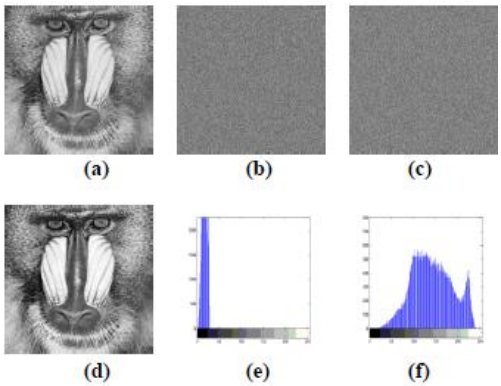

Figure 7: (a) Host image (b) Share 1 (c) Share 2 and (d) Revealed image (e) Histogram in range (0-31) (f) Histogram in range (0-255)

In the above shown figure, first image is the Host image, after encryption two shares are generated in gray scale color & at last the revealed image is obtain by stacking both the shares & comparing with the original one.

Performance Evaluation

The average energy of distribution caused by encrypting on each pixel can be calculated as

$$\mathbf{MSE}=\frac{1}{M.N}\sum_{i=1}^{M}\sum_{j=1}^{N}(X(i,j) - X'(i,j))$$

Where MSE is mean square value which is form two monochrome image *Pi* and *Pim* in which one of the image is original host image and another one is revealed image. Now the PSNR is defined as

$$\mathbf{PSNR\ in\ dB} = 10.\log_{10}\left(\frac{MAX^2}{MSE}\right)\ \mathbf{(dB)}$$

- Image quality can be measure by peak-signal-noise-ratio (PSNR) value measured in decibels (db)
- More PSNR value maintains the quality of image after the host image is encrypted.
- PSNR is also useful to measure for comparing restoration results for the same image.

Comparative analysis of our approach with the W*ang et al.*

	Wang et al. [3]	**Our proposed scheme**
The Type of Secret Sharing	(2,2) - SIS	(2,2) - SIS
Work on	Halftone(black & white)	Gray Scale Image
Size of input image	512x512	256x256
Pixel expansion	No	Yes(Little bit)
Intensity division	No	Yes
Shares generated on the basis of	Blocks	Pixels
Extra information needed	Yes(the secret key)	Yes (Two level secret key)
Codebook needed	Yes	No
Decoding method	Low computation	Less computation
Contrast Stretchment	No	Yes

Conclusions

This work has illustrated that the pixel intensity division method could be used to effective to improve the performance of an image for transmitting any image through E-mail or through any other medium. In order to reduce the more computation work and improve the quality of image with security a two level authentication scheme has been proposed to avoid different security attacks and threats. This scheme is much secure and safe than the other traditional schemes. The major advantages of the proposed scheme is to reduce computation, increase security, improve the image quality by contrast stretchment & pixel expansion, performance evaluated by calculating PSNR and Histograms. In future this dissertation can be extent to develop various color images of different intensity like Scheme for RGB & CMY, Histogram for 3D gray scale images etc.

References

Floyd R.W., Steinberg L. (1976) An adaptive algorithm for spatial grey scale. Proceedings of the Society of Information Display 17, pp 75–77.

Shamir A. (1979), How to Share a Secret, Communications of the Association for Computing Machinery, Vol. 22, No. 11, pp. 612-613.

Blakley G.R.(1979), Safeguarding Cryptographic Keys, in Proceedings of the National Computer Conference, American Federation of Information Processing Societies, pp. 313 317.

Kafri, O. and Keren, E. (1987) Encryption of pictures and shapes by random grids, Optics Letters, 12, (6), pp. 377-379

Naor M. and Shamir A. (1995), Visual Cryptography, Lecture Notes in Computer Science, Vol. 950, pp. 1-12

Tompa Martin and Woll Heather, How to Share a Secret with cheater, Springer-Verlag

Metaxas P. (1999), Optimal Parallel Error-Diffusion Dithering. Color Imaging: Device-Indep. Color, Color Hardcopy, and Graphic Arts IV, Proc. SPIE 3648, 485–494.

Ito R., Kuwakado H., Tanaka H. (1999), Image Size Invariant Visual Cryptography, IEICE Transactions on Fundamentals, Vol. E82-A, No. 10, pp. 2172-2177.Sun Hung-Min and Shieh Shiuh-Pyng (1999), Recursive

Constructions for the perfect secret sharing schemes, PERGAMON, Computers and Mathematics with Applications 37, pp 87 96.

Thien C.C. and Lin J.C. (2000), Secret Image Sharing, Computers and Graphics, Vol. 26, pp. 765-770.

Tzeng Wen-Guey and Hu Chi-Ming (2002), Designs, Codes & Cryptography Volume 27 Issue 3, pp 207 – 227.

Wu Y.S., Thien C.C., Lin J.C. (2000), Sharing and Hiding Secret Images with Size Constraint, Pattern Recognition, Vol. 37, No. 7, pp. 1377-1385.

Yang Ching-Nung (2000), New visual secret sharing schemes using probabilistic method, Elsevier Computer Science, Pattern recognition letters 25, pp 481-494.

Wang R. Z. and Su C. H. (2002), Secret Image Sharing with Smaller Shadow Images, Elsevier, Pattern Recognition Letters, Vol. 27, No. 6, pp. 551-555.

Wang Daoshun, Zhang Lei, Ma Ning and Li Xiaobo (2001), Two secret sharing schemes based on Boolean operations, Elsevier Computer Science, Pattern recognition 40, pp 2776-2785.

Wang Ran-Zan and Lee Yao-Ting,(2010) Visual cryptography by Random Grids with identifiable shares, World Academy of Science, Engineering and Technology 41.

Revenkar P. S., Anjum Anisa and Gandhare W. Z. (2010), Survey of Visual Cryptography schemes, International Journal of Security and Its Applications, Vol. 4, No. 2.

Wang Zhi-Hui, Chang Chin-Chen and Pizzolatti Marcos Segalla (2011), A New Reversible Secret Image Sharing Scheme Based on Multi-Level Encoding International Conference on Internet Computing and Information Services, IEEE Computer Society.

Hu Chunqiang, Liao Xiaofeng, and Cheng Xiuzhen (2012), Verifiable multi-secret sharing based on LFSR sequences, Elsevier, Theoretical Computer Science 445, pp 52–62.

Deepa G. (2013), The comparative study on visual cryptography and random grid cryptography, IOSR Journal of Computer Engineering (IOSR-JCE), vol 12, issue 2, PP 04 -14.