Enhanced Color Visual Cryptography

S. BOSU BABU, sbb.asp@gmail.com S.S.P KUMAR, balasriram1982@gmail.com
Avanthi College of Engg & Tech, Tamaram, Visakhapatnam, Andhra Pradesh, India.

Abstract-Though researchers has proposed contrastive methods to encrypt images but correlation between pixels RGB value play a imperative part to guess for original image. So, here we introduce a new image encryption method which first rearranges the pixels within image on basis of RGB values and then forward intervening image for encryption. In the field of visual Cryptography to decrypt the image with quality and no pixel expansion has become a challenge. To face these kinds of challenge in this paper has been proposed a new visual cryptography scheme. Encryption process the input image is separate into number of shares using optimization techniques. Once share has been created the splitted shares are compressed by the modified RLE. In the decryption process the reverse process has been taking place to retrieve the original image. Using this proposed method there is no pixel expansion and original quality of image is reconstructed and proved in the experimental result.

Keywords: Optimization Techniques, Modified RLE, Gray Scale Image

I INTRODUCTION

C.blundo says Visual cryptography is a cryptographic paradigm introduced by Naor and Shamir.Some predefined set of participants can decode a secret message without any knowledge of cryptography and without performing any cryptographic computation. In this method we have analyze visual cryptography schemes for grey level images whose pixels have g grey levels ranging from 0 (representing a white pixel) to g -1 (representing a black pixel).A visual cryptography idea for a set r of n participant is a scheme to predetermine a top secret image SI into more number of shadow images called share. Where each member in r receive one share and Certain eligible

qualified set of participants can “visually” recover the top secret image. The advantage of the visual secret sharing scheme is decryption process where not including any combination addition encrypted data is decrypted using Human Visual method. But the encryption plan requirements cryptographic calculation to divide the image into a number of parts. B.w.leung, et al says Visual cryptography is a type of secret sharing techniques for images. The idea of VCS is to divide an image into a group of random share which individually disclose no information about the unique top secret image. The image is relaxing of black and white pixels, and can be recovered by superimpose a threshold number of share with no any operational out mixed up .Within this method also splits a top secret image into more number of shares, the black facade and

the other three shares. It was claim that with no significant the black mask, no information about the secret image can be obtained even if all the other three shares are known. Rezvan dastanian and hadi shahriar shahhoseini says The Information, image and media encryption is a method for preventing misuse of adversaries. Visual cryptography is a method in which decryption is performed with human visual system along with OR operation. In this method one secret image is divided between two shares so that by stacking the two shares secret image appears.With stacking two shares, secret image I appear and with stacking one of the shares with 90 degrees rotation in clockwise on other share appears the secret image Abhishek parakh and subhash kak says a recursive hitting of secret, the user encodes further information about smaller secrets in the shares of a larger secret without an expansion in the size of the latter, thereby increasing the efficiency of secret sharing. The proposed protocol is an application for images as well as text. Thomas month and et al says Visual Cryptography Scheme (VCS) for a set P of n participants is a method to encode a Secret Image (SI) into n shadow images called shares, where each participant in P receives one share Certain qualified subsets of participants can visually recover the SI,but other, forbidden sets of participants have no information on SI.S. Kirkpatrick et al says The method of simulated annealing is a technique that has attracted significant attention as suitable for optimization problems of large scale, especially ones where a desired global extreme is hidden among many, poorer, local extreme. For practical purposes, simulated annealing has effectively “solved” the famous traveling salesman problem of finding the shortest cyclical itinerary for a traveling salesman who must visit each of N cities in turn. The method has also been used successfully for designing complex integrated circuits.Dimitries bertimas et al says simulated annealing algorithm is a probabilistic method proposed in Kirkpatrick and cerny for finding the global minimum of a cost function that may possess several local minima. It works by emulating the physical process whereby a solid is slowly cooled so that when eventually its structure is “frozen,” this happens at a minimum energy configuration.Lin TL et al says The main concept of the original visual secret sharing (VSS) scheme is to encrypt a secret image into n meaningless share images. It cannot leak any information of the shared secret by any combination of the n share images except for all of images. The shared secret image can be revealed by printing the share images on transparencies and stacking the transparencies directly, so that the human visual system can recognize the shared secret image without using any devices.Hiroki koga says The visual secret sharing scheme (VSSS) is a new paradigm of the secret sharing proposed by author. Letting = {1,2; , , , n)be a set of par- tic pants, in the VSSS a black-white secret image is encrypted to n black-white images called shares.Eric r. verheul, henk c.a says Secret sharing techniques belong to the larger area of information hiding that includes watermarking. In secret sharing, random looking shares when brought together recreate the secret. In recursive secret sharing, the shares themselves have components

defined at a lower recursive level Sandeep katta also says Secret sharing techniques belong to the larger area of information hiding that includes watermarking. In secret sharing, random looking shares when brought together recreate the secret. In recursive secret sharing, the shares themselves have components defined at a lower recursive level. The injection of the random bits in the shares may be done conveniently using d-sequences or other random sequences. Chih-ching thien and ja-chen Lin says a userfriendly image-sharing method for easier management of the shadow images. The sharing of images among several branches using the proposed method has several

characteristics 1.fast transmission among branches 2.fault tolerance 3.a secure storage system 4.reduced chance of pirating of high-quality images and 5.most importantly, the provision to each branch manager an easy-to-manage environment. R.w.eglese says simulated annealing algorithm and the physical analogy on which it is based. Some significant theoretical results are presented before describing how the algorithm may be implemented and some of the choices facing the user of this method. The rest of the paper is organized as follows Proposed method, Encryption process, Decryption process, Experimental result and conclusion.

II PROPOSED METHOD

Visual Cryptography is encryption technique to encrypt an image in such a way. In previous method the encrypted image outcome size is large when compare to input size of the image. Encrypted image is again can be decrypted by stacked together "OR" operation. In visual and pixel expansion. In the above mentioned problem had been solve my proposed method.

First the original secret image is encrypted into n number of shares by Visual cryptography based on optimization techniques with no pixel expansion. Then the shares are compressed by Modified RLE compression. Then the shares again decompressed. Based on this process we can improve the display quality of the recovered image

II(A) ENCRYPTION PROCESS

Cryptography the decryption process finished the reconstructed image has been affect two main problem. The two problems are Image quality of the reconstructed image In visual cryptography two major processes have been involved the Encryption process and decryption process. The encryption only most steps have been involved to encrypt an image. But the decryption process little steps involve to decrypt an image. Below show a proposed diagram for entire process for this method. In the visual cryptography original image is given input to the encryption process, then the image in encrypted by using optimization techniques. Input images are gray level images that pixels have g grey levels ranging from 0(represent a white pixel) to g-1(represent a black pixel).In visual cryptography based optimization techniques split secret images into n number of the shares. In the encryption process image is encrypted based on the black pixel and white pixel, the image is encrypted two shares with black and white pixel (shadow images). Third stage of the encryption process is modified RLE (Run Length Encoding) compression techniques In this compression each and every shares is compressed using this techniques. Each and every image is compressed to binary numbers and send to the end user. Final of the encryption process we get secret information (Shares)

II(B) DECRYPTION PROCESS

In visual cryptography decryption process is a recovering original images in this process little stages involve decrypting a secret image to compare with the encryption process. First stage of the decryption process is recovered binary secret information to shadow image by decompression RLE process. It is a lossless algorithm that only offers decent compression ratios in specific types of data. RLE is probably the easiest compression algorithm there is. It replaces sequences of the same data values within a file by a count number and a single value After finish the decompression shared images are stake together by "OR" operation

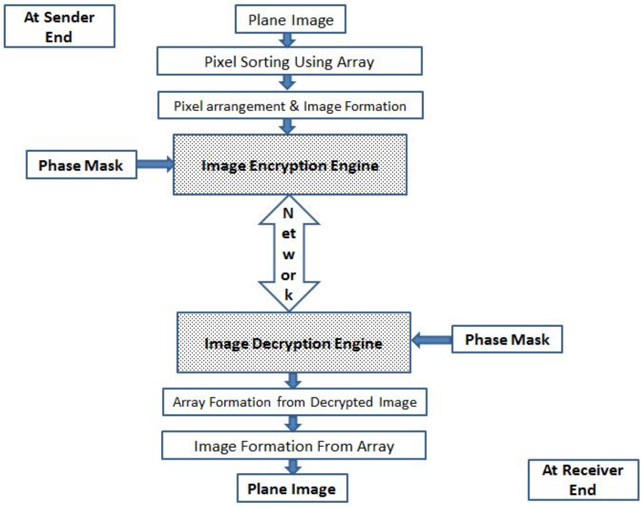

Figure 1 Architecture of proposed method for image encryption.

Architecture shows the image encryption method proposed in this paper. Plain image is first sorted using an array then this array is used to form an intermediate image which is passed for image encryption engine where inter-pixel algorithm is applied to convert a plain image into cipher image. Reverse of this procedure is shown at the receiver end.

II(C) ALGORITHM

Pixel_ReArrangement()

```
1 Start

2 img = input plain image.

3 rows, cols = size of img.
4 create array of (rows*cols , 5)
5 transfer img pixel values into array for complete image
array(,1)=R value
array(,2)=G value
array(,3)=B value
array(,4)=x position
array(,5)= y position
6 sort this array
7 img = form an image using this array
8 Invoke ImageEncryption(img, rows, cols)
9 End
```

Pixel rearrangement algorithm will be responsible for reducing the correlation between pixel values by arranging pixels in a sorted manner within image by using their RGB values and experimental result proves the reduced correlation. To perform this arrangement of pixels, this algorithm filches an image and enumerates its length, width and from its length and width; it calculates the total no of pixels in image. Once we know the number of pixels in image, then an array is created of same length equal to no of pixels in image and then each row of array is assigned with the each pixel of image. When all pixels of image will get shift to array then this array is sorted and this is compound sort which makes further sorting at group-wise; means if 20 pixels starts from 120 value for R then all these pixels will be grouped together and further if these pixels have same value of G and B then groups will made on G and B also.

When these pixels will be get sorted in an array then this array is used for forming image again in sequence starting from first pixel to last and by doing this, 0, 0, 0 pixel value will be occupy first pixel (1, 1) in new image and pixel value 255, 255, 255 will get last pixel location in image (pixel 0, 0, 0 and 255, 255, 255 are subject to available in original image).

```
ImageEncryption (e,x,y)
1 Start
2 Supply PM[ ] array
3 Initialize Counter=1, initJump= Any Arbitrary Integer
4 Loop while PM[counter] is not NULL
    if PM[counter]=0
        Invoke HORIZONTAL_Shift(e,x,y,αr[counter], αg[counter], αb[counter])
        Increment counter by 1.
    Endif
    if PM[counter] = 1
        Invoke VERTICAL_Shift(e,x,y,αr[counter], αg[counter], αb[counter])
        Increment counter by 1.
    Endif
  Endloop
5 End
```

The ImageEncryption() method takes image with its coordinate limits and started performing encryption process by deploying the shifting of R G B components among the pixels. The PM[] array called as Shift pattern mask array consists of binary digits 1's and 0's. The length of this array is the total number of vertical and horizontal shifts done in the encryption process. Each 1 triggers a circular vertical shift and a 0 triggers the invocation of circular horizontal shift. The PM[ ] can be made a part of the key or else supplied separately. With the increase in the length of the mask, the security as well as running time for encryption process increases linearly.

The ImageEncryption() method uses another set of arrays namely αr[counter], αg[counter], αb[counter] which holds in it the different integers for R, G and B component shifts. This ensures that in each successive row, the displacement of a component doesn't remain a constant. Else it will result in the simple circular shift of the entire color component and hence it becomes a favorable condition for the cryptanalyst since guessing the shift of a single row is enough to know by how much are the other rows also shifted. The same entity is also used in the HORIZONTAL_Shift function also to provide a wider scattering of the R G B components from its native pixel position.

VERTICAL_Shift(e,x,y, αr[counter], αg[counter], αb[counter])

```
1 Start
2 Input image with its coordinate limits x1 to x2, y1 to y2.
3 αr[counter], αg[counter], αb[counter]
4 ΔR= initJump + αr[counter]
5 ΔG= initJump + αg[counter]
6 ΔB= initJump + αb[counter]
7 Loop and Repeat steps for ColC = x1 to ColC= x2
    Do Circular Vertical Shift of R values at ColCth column by ΔR pixels
    Do Circular Vertical Shift of G values at ColCth column by ΔG pixels
    Do Circular Vertical Shift of B values at ColCth column by ΔB pixels
    ΔR = ΔR + αr[counter]
    ΔG = ΔG + αg[counter]
    ΔB = ΔB + αb[counter]
  Endloop
8 Return
```

HORIZONTAL_Shift(e,x,y,αr[counter], αg[counter], αb[counter])

```
1 Start
2 Input image with its coordinate limits x0 to xmax and y0 to ymax.
3 αr[counter], αg[counter], αb[counter]
4 ΔR= initJump + αr[counter]
5 ΔG= initJump+ αg[counter]
6 ΔB= initJump + αb[counter]
7 Loop and Repeat steps for RowC = y1 to RowC= y2
    Do Circular Horizontal Shift of R values at RowCth row by ΔR pixels
    Do Circular Horizontal Shift of G values at RowCth row by ΔG pixels
    Do Circular Horizontal Shift of B values at RowCth row by ΔB pixels
    ΔR = ΔR + αr[counter]
    ΔG = ΔG + αg[counter]
    ΔB = ΔB + αb[counter]
  Endloop
8 Return.
```

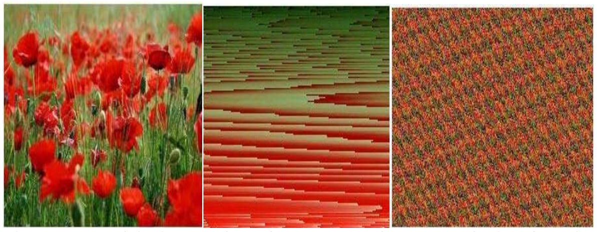

Figure 2 (a) Plain image size of 284 x 117 (b) Image obtain after pixel rearrangement (c) Cipher Image

Proposed algorithm was tested on three different size images of pixels 284 x 117, 1200 x 800 and 320 x 240 and result obtain is shown in figure 2, 3 and 4 respectively. Part (b) of each figure shows the image which is obtained after applying pixel rearrangement which is proposed to reduce the correlation between pixel values such that images should not guess by neighboring pixel. Although image encryption model is based on this methodology that no one other than authorized user can guess about cipher image. So, by looking at part (b) of each figure, this can conclude that correlation is negligible because it is not possible to calculate the neighbor 8 pixel for any pixel. Further histogram of each image is shown which shows the difference in the plain image and cipher image and histogram for plain image and intermediate image is same because there is only pixel rearrangement while in plain image and cipher image there is inter-pixel displacement.

III DISCUSSION

VIPs are assigned freely to carry the visual information of original images in each subpixels.Visual quality of the encrypted shares and of the decrypted share, denoted as and, respectively, mostly depends upon the size of pixel expansion, and , the number of VIPs and , the number of 1 s in each . We assume that the in is , meaning all elements of the "OR"-ed row vector of the matrix are 1. The has the same value as contrast difference in the Algorithm For the , smaller and larger , indicating more number of VIPs in a small pixel expansion, produce better visual quality shares. On the contrary, for the , larger and smaller and are desirable for the reconstructed share with high contrast. Consequently, there exists a tradeoff relationship between and for encryption shares and the decryption share and the decision of parameters is up to the purpose of applications. For a scheme with parameters , , and one with the and of the former are 1/6 and 2/6, and those for the latter are 2/6 and 1/6. The higher contrast of encryption shares, the lower contrast of the decryption share, and vice versa. The error filter employed in the error diffusion also affects the share quality. An error filter with longer weight leads to high contrast of encryption shares .Since Floyd and Steinberg's filter was first introduced, many modifications to the original error diffusion algorithm have been introduced that address the unwanted artifacts of the original algorithm. A typical problem that occurs is spectral whitening where the variation in average separation distance between minority pixels becomes so great that the pattern starts to resemble the halftone pattern created by white noise. In an effort to break up worm patterns in error diffusion, Jarvis and Stucki introduced 12-element error filters and it is apparent that both filters break up worms at extreme gray levels.Another factor that affects the quality is the position-dependent threshold in the error diffusion stage. To produce better quality shares, output-dependent threshold modulation can be used in the error diffusion to suppress unwanted textures

IV EXPERIMENTAL RESULT

In threshold visual cryptography reconstructed image quality have affect two problem, reconstructed image quality and security. That problem solved by my proposed Run Length Encoding (RLE) Compression method. RLE Compression method to compressing the n number of shadow images and decompress. To show the table.1, black and white pixels based quality improvement. In the table.1 the black pixel is appear little more when compare to the white pixel. The white pixel appears half percentage of the image so the quality of the image is improved.

V CONCLUSION AND FUTURE SCOPE

In this paper we presented new algorithm for image encryption by using sorting of pixels as per their RGB values and arranging them group-wise which helped to reduce the correlation between pixels and increased entropy value. Experimental results were taken out on Matlab 6.0.1 and this is a lossless image encryption algorithm with results. Histogram of plain image and cipher image is also carried out. Further inter pixel algorithm can be used with another confusing property to result in better image encryption technique. This work can be further extended by using the pyramidal block scheme for image encryption with inter pixel scheme.

VI REFERENCES

[1] Information available via www at htpp://en.wikipedia.org/wiki/Open_communication.

[2] Jakimoski, G. and L. Kocarev. 2001. ―Chaos and Cryptography: Block Encryption Ciphers Based on Chaotic Maps. IEEE Transactions on Circuits and Systems□—I: Fundamental Theory and Applications. 48(2): 163-169.

[3] Jayant Kushwaha and Bhola Nath Roy, "Secure Image Data by Double encryption", International Journal of Computer Applications (0975 – 8887), Volume 5– No.10, August 2010.

[4] Mohammad Ali Bani Younes and Aman Jantan, "Image Encryption Using Block – Based Transformation Algorithm" IAENG, 35:1, IJCS_35_1_03, February 2008.

[5] Mohammad Ali Bani Younes and Aman Jantan, "An Encryption Approach Using a Combination of Permutation Technique Followed by Encryption" IJCSNS, vol 3 no 4, April 2008.

[6] Aditee Gautam, Meenakshi Panwar and Dr.P.R Gupta, "A New Image Encryption Approach Using Block Based Transformation Algorithm", (IJAEST) International Journal Of Advanced Engineering Sciences And Technologies, Vol No. 8, Issue No. 1, 090 - 096 @ 2011, ISSN: 2230-7818.

[7] Amnesh Goel, Reji Mathews & Nidhi Chandra, "Image Encryption based on Inter Pixel Displacement of RGB Values inside Custom Slices", International Journal of Computer Applications (0975 – 8887), Volume 36– No.3, December 2011.

[8] Socek, D., Shujun Li, Magliveras, S.S. and Furht, B, "Enhanced 1-D Chaotic Key-Based Algorithm for Image Encryption", First International Conference on Security and Privacy for Emerging Areas in Communications Networks, 2005:406-406.

[9] Deergha Rao and K. Gangadhar, "Modified Chaotic Key- Based Algorithm for Image Encryption And Its VLSI Realization", International Conference on Digital Signal Processing, 2006.

[10] Jui-Cheng Yen, and Jiun-In Guo, "A New Chaotic Key-Based Design for Image Encryption and Decryption", IEEE International Symposium on ISCAS 2000, Geneva, pp. IV-49-IV-52, May. 2000.

[11] Reji Mathews, Amnesh Goel, PrachurSaxena & Ved Prakash Mishra, "Image Encryption Based on Explosive Inter-pixel Displacement of the RGB Attributes of a PIXEL", Proceedings of the World Congress on Engineering and Computer Science 2011 Vol I WCECS 2011, October 19-21, 2011, San Francisco, USA. ISBN: 978-988-18210-9-6.

[12]. Shyamalendu kandar et al, "k-n secret sharing visual cryptographyscheme for color image using random number," International journal of engineering science and technology vol. 3 no. 3 mar 2011.

[13] B.W.leung et al"On the security of a visual cryptography scheme for color images," Pattern recogn, vol. 42, no. 5, pp. 929–940, 2009.

[14] Rezvan dastanian et al"Multi secret sharing scheme for encrypting Two secret images into two shares" 2011 International conference on information and electronics engineering" IPCSIT vol.6 (2011)

[15] Abhishek parakh and subhash kak "A recursive threshold visual cryptography scheme" Stillwater, ok 74078.

[16] Thomas month and babu anto p "Achieving optimal contrast in visual cryptography schemes without pixel expansion" International journal of recent trends in engineering, vol. 1, no. 1, may 2009.

[17] S.Kirkpatrick et al "Optimization by simulated annealing" Science, 13 May 1983, volume 220, number 4598.

[18] Dimitries bertimas and john tsitkils "Simulated annealing"Statistical science, 1993, vol.8. No. 1, 10-15.

[19] Lin TL et al "A novel visual secret sharing scheme for multiple secrets without pixel expansion" Expert systems with applications, 37 (2010) 7858–7869.

[20] Thomas month and babu anto p "Achieving optimal contrast in visual cryptography schemes without pixel expansion" International journal of recent trends in engineering, vol. 1, no. 1, may 2009

[21] Hiroki koga "A general formula of the (t; n)-threshold visual secret sharing scheme," University of tsukuba.

[22] Eric r. verheul et al"Constructions and properties of k out of n visual secret sharing schemes" Design and cryptography.

[23] Sandeep katta "Visual secret sharing scheme using grayscale images" Stillwater, ok 74078

[24] Chih-ching thien and ja-chen Lin "An image-sharing method with user-friendly shadow images," IEEE transactions on circuits and systems for video technology, vol.13, no. 12, December 2003

[25] R.w.eglese "Simulated annealing: a tool for operational research," European journal of operational research (1990) 271-181.

[26] Zhongmin Wang et al "Halftone visual cryptography via direct binary search"14th European Signal Processing Conference (EUSIPCO 2006), Florence, Italy, September 4-8, 2006.

[27] Carlo Blundo et al," Visual Cryptography Schemes with Optimal Pixel Expansion" Universit`a degli Studi di Milano, 26013 Crema, Italy.

AUTHORS BIOGRAPHY

S.BosuBabu, born on 15th August 1984 in Visakhapatnam, A.P., India.

Dr. C. P. V. N. J. Mohan Rao, is working as Professor & Principal of Avanthi College of Engineering & Technology, Tamaram, Makavarapalem, Narsipatnam (RD), Visakhapatnam, Andhra Pradesh, INDIA. He obtained PhD from Andhra University and having 15 years experience. He published more than 18 papers in reputed Journals.

Somayajula Satya Pavan Kumar is working as Assistant Professor, in CSE Department, , Avanthi College of Engineering & Technology, Tamaram, Visakhapatnam, A.P., India. He has received his M.Sc(Physics) from Andhra University, Visakhapatnam and M.Tech (CST) from Gandhi Institute of Technology And Management University (GITAM), Visakhapatnam, Andhra Pradesh, INDIA. His research areas include Software Engineering and network security.