Visual Cryptography Based On Modified RLE Compression without Pixel Expansion

Manimurugan.S, Ramajayam.N

Abstract:-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.

Index Terms: **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. [2] But the encryption plan requirements cryptographic calculation to divide the image into a number of parts.[2] B.w.leung, et al says Visual cryptography is a type of secret sharing techniques for images [3]. 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 [3]. 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 [3]. Within this method also splits a top secret image into [3] more number of shares, the black facade and the other three shares [3]. 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.[3] 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.[4].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 II[4] 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[5]. The proposed protocol is an application for images as well as text[5]. 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.[6].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. [7] 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.[8] 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. [9] Hiroki koga says The visual secret sharing scheme (VSSS) is a new paradigm of the secret sharing proposed by [1] author. Letting $P= \{1,2; , , ,$ n)be a set of partic pants, in the VSSS a black-white secret image is

encrypted to n black-white images called shares.[11] 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[12] 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.[13] Chih-ching thien and ja-chen Lin says a user-friendly 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. [14] 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.[15] 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 cryptography the decryption process finished the reconstructed image has been affect two main problem. The two problems are Image quality of the reconstructed image. 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 as well as the security of the recovered image.

III. ENCRYPTION PROCESS

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).

KARUNYA

Original image

Share.1

Share.2

KARUNYA

Recovered Image
Fig.1 Proposed Method
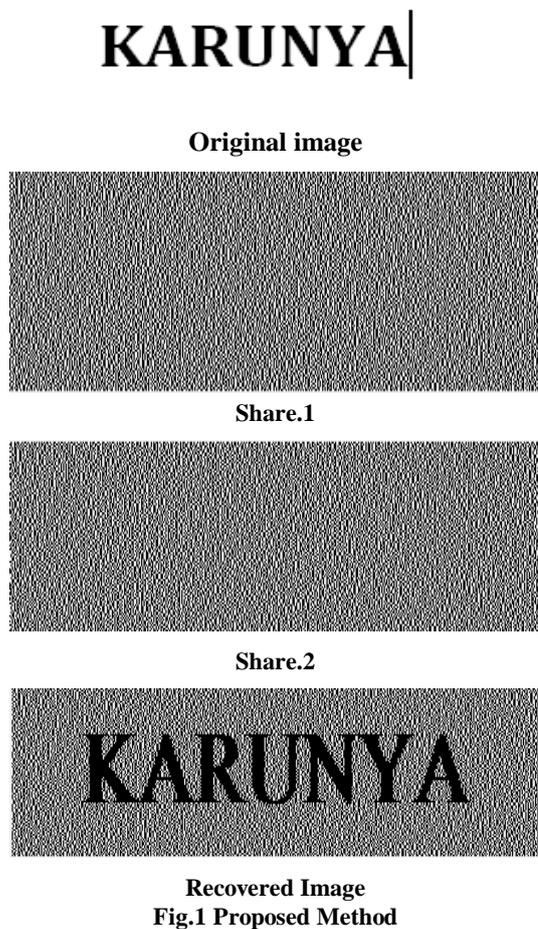
IV.DECRYPTION PROCESS

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.

Table.1 The Details Of Pixel In Secret Image (Share1, Share2, Share3) and Reconstructed Table

Image	Total columns In Image	Total Rows In Image	Total Black pixels In Image	Total white Pixels In Image	Total pixels In Image
Original image	245	50	3928	8322	12250
Share1 Of the image	245	50	5998	6252	12250
Share2 Of the image	245	50	6042	6208	12250
Share3 of the image	245	50	6104	6116	12250
Share1+2+3 of the image	245	50	10116	2134	12250

V. 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.
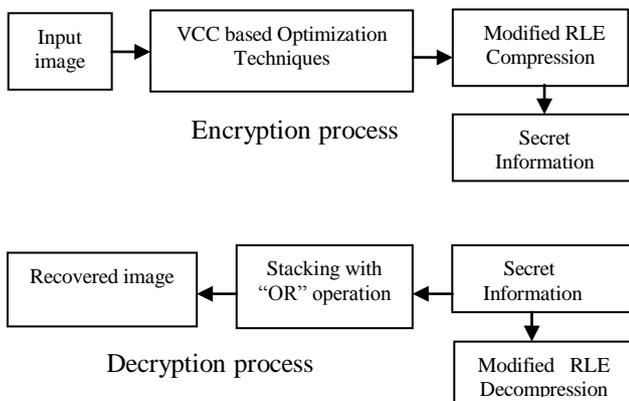

Fig.2 Proposed diagram

VI. CONCLUSION

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. Based on this techniques recovered image quality and also security.

ACKNOWLEDGEMENT

REFERENCES

[1] C. blundo et al"Visual cryptography for grey level images," inf. Process vol.75, no. 6, pp. 255–259, 2000.

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

[3] 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.

[4] 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)

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

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

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

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

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

[10] 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

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

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

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

[14] 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.

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

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

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

AUTHOR'S PROFILE

Dr. S. Manimurugan is an Assistant Professor in the Department of Computer Science and Engineering, Karunya University, Coimbatore, India. A person of great academic calibre, he completed his Bachelor's Degree from Anna University and his Master's Degree from Karunya University both with Ist class division marks. He was highly commended for his work in Image Processing and Information Security, for which he was honoured with a PhD from Anna University. His thesis titled Certain Investigations on Medical Image Encryption and Compression was highly acclaimed by the technical panel and he earned 8.9 CGPA for his course of work. He has over 5.1 years of teaching and research experience which has helped him gain immense knowledge in various fields of Computer Science. His understanding of Image Compression and Visual Cryptography is immense because of his extensive research and experience in these subjects. Apart from this he has largely worked in website development as well. He is a life member of Indian Society for Technical Education.

Ramajayam.N has completed his B.E degree in Computer Science and Engineering at Annamalai University in the year 2011 and is currently doing M.Tech in the Department of Computer Science and Engineering, Karunya University, Coimbatore, India. He is specialized in the area of Computer Science and Engineering and is in his second year of studies. Her research interests include the area of image processing.