A Novel Method for Securing Medical Image Using Visual Secret Sharing Scheme

G. Elavarasi
Research Scholar, Department of Computer Applications,
Alagappa University, Karaikudi, India.
elavarasig90@gmail.com

Dr. M. Vanitha
Assistant professor, Department of Computer Applications,
Alagappa University, Karaikudi, India.
mvanitharavi@gmail.com

Abstract - The visual mystery sharing (VSS) plot, which starts from the visual cryptography, is an impeccable secure technique that ensures a picture by separating it into many offer pictures. It can be effortlessly remade by the human visual framework without the learning of cryptographic calculations. Security on digital medical images, faced with several security issues in today's healthcare institution. To resolve this issue, a VSS based medical image security scheme is proposed in this paper. Here a new Color Visual Secret Sharing (CVSS)plot is connected to produce shares for input medicinal picture. The offers are made for the safe medicinal picture transmission and the picture data secrecy is kept up. At first the medicinal picture is part into various shadow pictures and the picture is uncovered when every one of these shadows are stacked together.Performance of the proposed method is evaluated by sample test medical images. The experimental results show that the CVSS scheme can provide satisfactory security level.

Keywords: Visual Cryptography,Visual Secret Sharing, Medical Image.

1. Introduction

In the area of medical images, concerning security is more important because of this medical image transmitting to hospitals over unsecured communication channel over open network and unauthorized person can steal and use it of his own benefits so that privileges of patient is suffered. Based on this issue, many researchers have been proposed method using Visual Cryptography method in which original image is split into different shadow images. Naor and Shamir's proposed the visual cryptography [1] which is allowed to secret sharing images without cryptographic computation and this scheme is refer as K-out-of-n VCS. Original image is given and get encrypted form of n images as follows:

$$T = S_{h1} \oplus S_{h2} \oplus S_{h3} \oplus ......S_{hn},$$

where$\oplus$ is a boolean operation, $S_{hn} \in 1, 2, ..., n$ is an image which appears aswhite noise,$k \leq n$, and n isthe number of noisy images. It is difficult to decipher thesecret image T using individual S_{hn}'s [2].

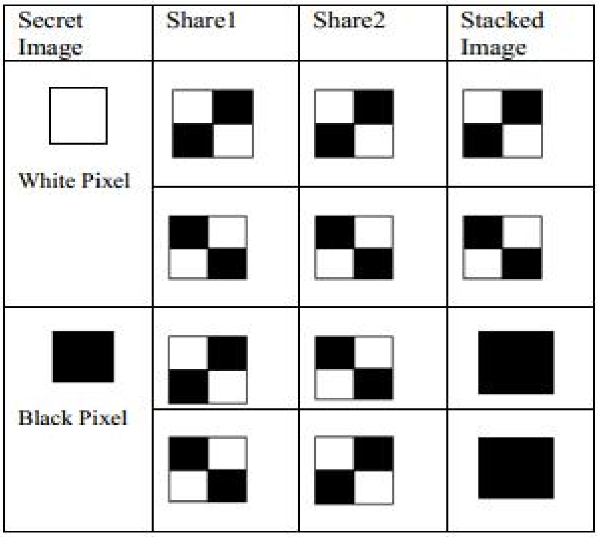


Fig.1.Classical (2,2) VC Scheme construction

The classical (2,2) VC scheme for binary image share construction is illustrated in Fig.1. In this encryption process every pixel of secret image is transformed into two pixels, and each pixel take part in corresponding share image. In the decryption process the two shares are stacked together (OR operation) to recover the secret image. A novel brand of secret offering plan is given the pet name visual secret sharing (VSS) plan [1].

VSS is an inventive procedure in which the imparted images. In this example, the image has been split into two component images. Each component image has a pair of pixels for every pixel in the original image. In visual cryptography, a secret binary image is modified into n shares of arbitrary binary prototypes. It is conceivable to translate the secret image outwardly by superimposing a qualified subset of transparencies [3].

2. Related Work

Researchers extended k out of n secret sharing to apply on color images. They proposed an algorithm to divide a digital color image into n number of shares where minimum k number of shares is sufficient to reconstruct the image. If k number of shares is taken then the remaining shares are (n-k). In an image if certain position of a pixel is 1, then in (n-k)+1 number of shares in that position of that pixel there will be

1. In the remaining shares in that position of the pixel there will be 0. A random number generator is used to identify those (n-k)+1 number of shares[4].

Blundo proposed Visual Cryptography schemes for gray level images[5]. Savita Patil used the concept of visual information pixel synchronization and error diffusion to attain a color visual cryptography encryption method that produces color shares [6].

Researchers enhanced the friendliness of VSS scheme by adding a simple and meaningful cover images to noise like share but the problem with this enhancement is that the recovered images are have reduced display quality Several papers investigated meaningful halftone shares [7]-[9] and emphasized the quality of the shares more than the quality of the recovered images. These studies had serious side effects in terms of pixel expansion and poor display quality for the recovered images, although the display quality of the shares was enhanced. Hence, researchers make a tradeoff between the quality of the shares and the quality of the recovered images and the pixel expansion of the image.

Hao-Kuan Tso et al.[10] have been developed Friendly VSS to secure the medical images. In this scheme, random-grid algorithm is used to construct two meaningless shadows and then a friendly pattern is apply on the shares which could make the users manage and identify them easily. Nelmiawati et al.[11] have beenproposed Pixel-Based Dispersal Scheme (PBDS) which is enhanced by combined Rabin's IDA and Shamir's SSA to secure the DICOM digital medical image. BothShamir's SSA and Rabin's IDA have been implemented and tested on multi-provider clouds in securing medical records [12]. In [13] Secret Sharing Scheme**,** a random multi-bit grid *R* with size of *m* by *n* is generated by using a seed and pseudo random number generator. Then, the random multi-bit grid *R* and medical images are used to construct two shared images.

3. Proposed Method

The color visual secret sharing scheme (CVSS) is applied on the medical image which is constructed in to different shares and able to reveal only when all of these shares are aligned together. In this scheme, medical image is read from the dataset and extracting original pixels. Meanwhile, key matrix is randomly generated which holds the values 1 through N number of shares given by user. After that key matrix index has been noted and compared it into the same index of original image, place it into corresponding share images and remaining values of shadow images are filled with 255. Now shares are constructed and impossible to reveal the original medical image with one share.

For example, original image pixels are obtained and user want to create four share images so key matrix are generated with the values from the range 1 to 4 randomly. Suppose if user want to create five share images means key matrix holds the values in the range from 1 to 5. Take the pixel "100" from the index 3 of the original image and comparing it to same index of key matrix and from that key value "4" has been noted. It tells that this value 100 move into index 3 of the fourth share and remaining values are filled 255. The above process is repeated till the pixel values are filled into the share images. Once all these shares are arranged together, there is a chance to reveal the image else no one couldn't retrieve it with single shadow image. Following algorithm is applied to construct a share from the medical image.

Color Visual Secret Sharing Scheme (CVSS) for Medical Images

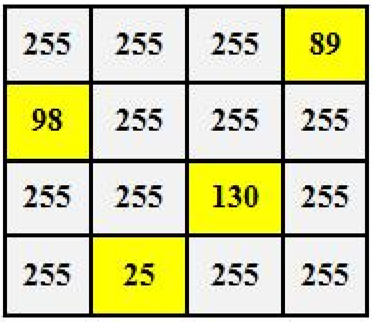
Step 1: Read original medical image (grey-scale format).

100	**45**	**56**	**89**
98	**74**	**12**	**155**
160	**94**	**130**	**147**
64	**25**	**220**	**201**

Step 2: Generate key matrix randomly of same size as original image. Key matrixvalue ranges depends on the number of shadows given by the users.

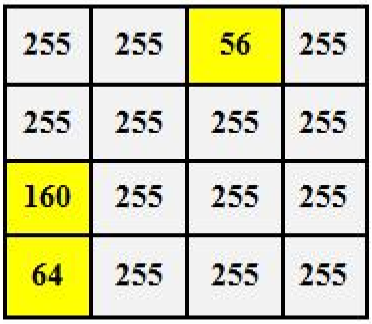
4	**3**	**2**	**1**
1	**4**	**4**	**3**
2	**4**	**1**	**3**
2	**1**	**4**	**3**

Step 3: Get original image index and compare it into same index in the key matrix.Next get the value of that index and then transform into corresponding shadow images. Consecutively remaining shadow image values are set to 255 and the example as shown in fig.



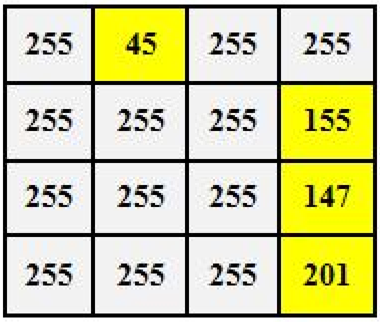
255	255	255	89
98	255	255	255
255	255	130	255
255	25	255	255

Shadow 1



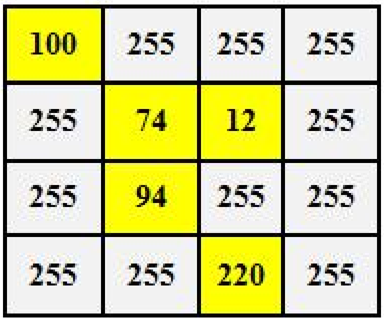
255	255	56	255
255	255	255	255
160	255	255	255
64	255	255	255

Shadow 2



255	45	255	255
255	255	255	155
255	255	255	147
255	255	255	201

Shadow 3



100	255	255	255
255	74	12	255
255	94	255	255
255	255	220	255

Shadow 4

Now, comparing pixel index and key matrix index. Pixel 100 is placed into the same index of 4th share because in key matrix, the value 4 is generated in the same index. Pixel 45, 56, 89 move into 3rd, 2nd, 1st shares by noted the values of key matrix are 3, 2, 1.

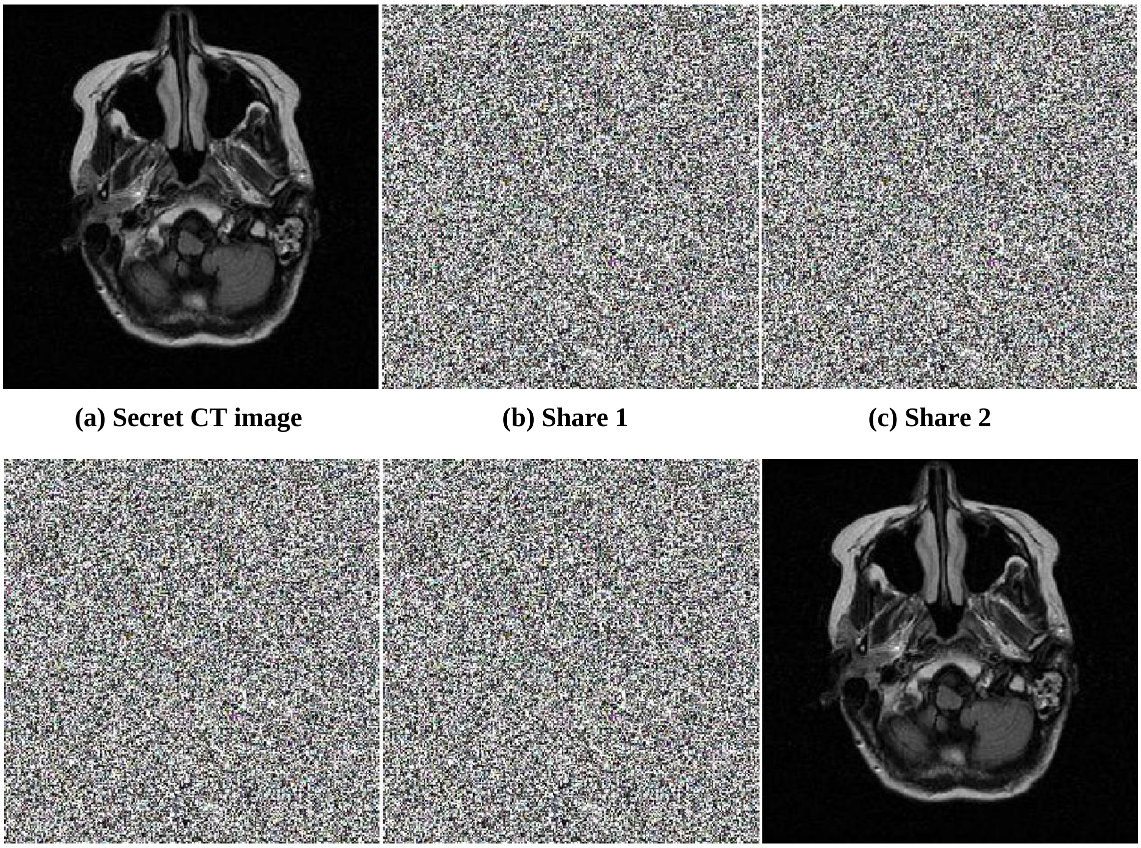
Step 4: The same process repeated until last pixel values are reached. Then obtainedthe noise like 4 different shadow images.

Step 5: To reconstruct the original image, remove 255 value and remaining originalpixel values and also get their corresponding indexes of all the shadow images.

4. Results and Discussion

4.1 Experimental Results

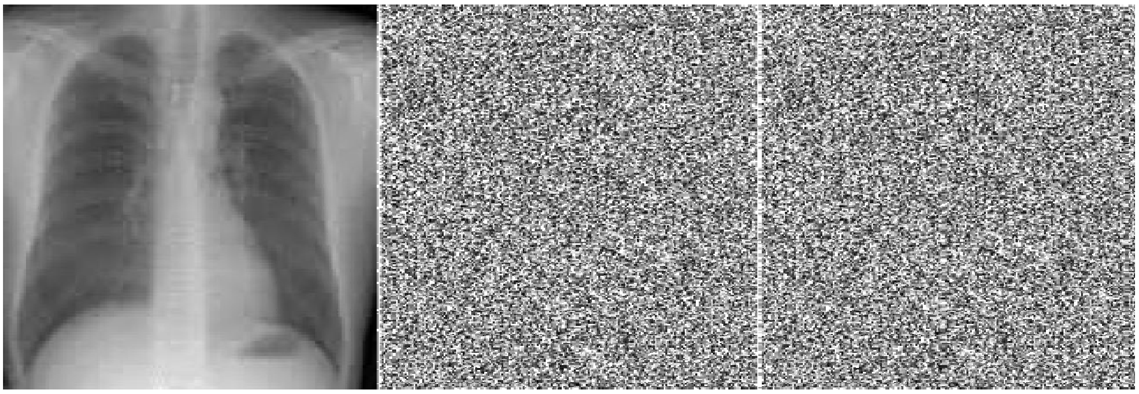
A novel CVSS algorithm, implemented in visual studio environment (C# language) is used and applied on CR and CT medical images, the results as shown in Fig. 2 and Fig.3. It includes original medical image, individual shares and reconstructed original images.



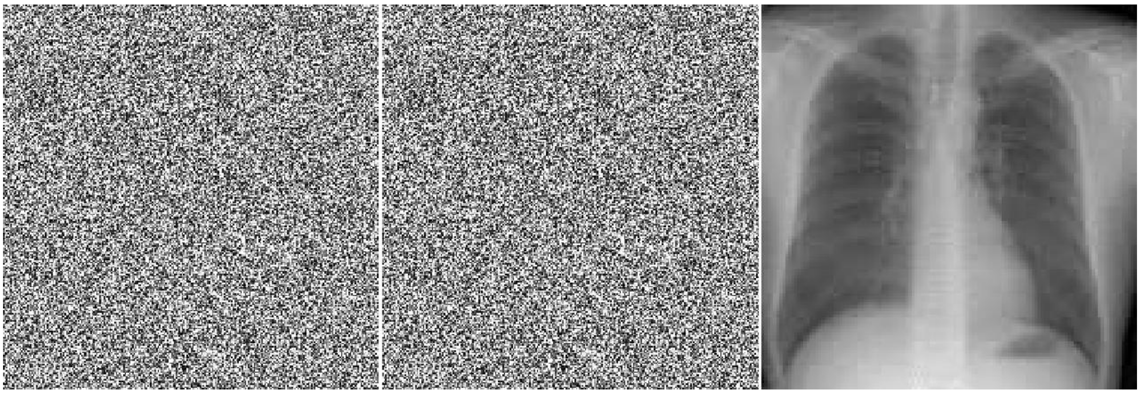
(a) Secret CT image **(b) Share 1** **(c) Share 2**

(d) Share 3 **(e) Share 4** **(f) Reconstructed Iris image**

Figure 2. Experimental Results of CT images



(a) Secret CR image **(b) Share 1** **(c) Share 2**



(d) Share 3 **(e) Share 4** **(f) Reconstructed CR image**

Figure 3. Experimental Results of CR images

4.2 Performance Analysis

4.2.1 NPCR and UACI Analysis

NPCR is the change rate of the number of pixels in the encrypted image. The unified average changing intensity (UACI) is the measurement of the average intensity of differences between the secret image and encrypted image. It shows the high NPCR values which represents the encrypted image pixels indexes are completely changed compared with original image. Experimental results shows the estimated expectations and variance of NPCR and UACI values are very close to the theoretical values, which justify the validity of theoretical values. Hence the proposed encryption scheme is resistant against differential attacks [15].

Table 1: Values of NPCR and UACI

Medical Images	NPCR (%)	UACI (%)
CT	99.59	32.08
CR	99.62	33.46

Fully uniform image with 256 gray levels which the probability of all pixels are the same, the entropy would have its maximum value, i.e. 8, which means the most irregularities among image pixels. The proximity of the image entropy to 8 means the efficiency of proposed method in image encryption [14].

Table 2: Entropy for Original and Encrypted Images

Medical Images	Original Image	Share Image
CT	7.7721	7.2209
CR	7.8143	7.2273

5. Conclusion

In this paper a novel medical image security method is proposed by using color visual secret sharing scheme. In this algorithm the pixel position is shuffled based on random matrix with traditional VSS procedure.It is very useful to enhance the medical image security by encrypting original images. The CVSS method is not only applicable for medical images and also exists for other digital images. The experimental results show that the proposed CVSS scheme gives the image confidentiality, integrity and reliability. Performance analysis proves the security, effectiveness and robustness of the proposed VSS algorithm.

References

[1] M. Naor and A. Shamir, “Visual cryptography,” in EUROCRYPT, pp. 1–12, 1994.

[2] Ching-nung yang and Chi-SungLaih, “New Colored Visual Secret Sharing Schemes”, Journal of Designs, Codes and Cryptography, Vol.20, pp.325–335, 2000.

[3] Shankar, K., and P. Eswaran. “RGB-Based Secure Share Creation in Visual Cryptography Using Optimal Elliptic Curve Cryptography Technique”, Journal of Circuits, Systems and Computers 25.11 (2016): 1650138.

[4] Shashikala Channalli, Ajay Jadhav, “Steganography an art of hiding data,” International journal on Computer Science and Engineering Vol.1(3), pp.137-141,2009.

[5] C. Blundo, A. D. Santis, and M. Naor, “Visual cryptography for grey level images,” Inf. Process. Lett., vol. 75, no. 6, pp. 255–259, 2000.

[6] Savita Patil and Jyoti Rao,”Extended Visual Crptography for Color Shares using Random Number Generator,” International Journal of Advanced Research in Computer and Communication Engineering Vol. 1, pp 399-410 Issue 6, August 2012.

[7] Z.Zhou, G.R.Arce, and G.D. Crescenzo,“Halftone visual Cryptography,” IEEE Trans. Image Process, vol.15,no.8,pp.2441-2453,Aug.2006.

[8] Z.Wang, , G.R.Arce, and G.D. Crescenzo,“Halftone visual Cryptography via error diffusion,” IEEE Trans. Inf. Forensics Security, vol.4, no.3,pp. 383-396, Sep.2009.

[9] I.kang,G.R.Arce,and H.K.Lee, “Color extended visual cryptography using error diffusion,” IEEE Trans. Image Process., vol. 20, no.1, pp. 132-145, Jan. 2011.

[10] Hao-Kuan Tso, Tsung-Ming Lo, Wei-Kuei Chen, “Friendly Medical Image Sharing Scheme”, Journal of Information Hiding and Multimedia Signal Processing, Volume 5, Number 3, July 2014.

[11] Nelmiawati, Mazleena Salleh, and Subariah Ibrahim, “Medical Image Dispersal using Enhanced Secret Sharing Threshold Scheme”, Int'l Conf. Health Informatics and Medical Systems | HIMS'15 |.

[12] T. Ermakova and B. Fabian, “Secret Sharing for Health Data in Multi-Provider Clouds”, in Conference on Business Informatics (CBI), Vienna, 2013.

[13] Tso, Hao-Kuan, and Der-Chyuan Lou. “Medical image protection using secret sharing scheme”, Proceedings of the 6th International Conference on Ubiquitous Information Management and Communication. ACM, 2012.

[14] Hooman Kashanian, Masoud Davoudi and Hamed Khorramfar, “Image Encryption using chaos functions and fractal key”, International Journal of Computer Science and Network Security, vol.16, no.10, page(s): 87-92, 2016.

[15] Shankar, K., and P. Eswaran. "A new k out of n secret image sharing scheme in visual cryptography." Intelligent Systems and Control (ISCO), 2016 10th International Conference on. IEEE, 2016.