Visual Secret Sharing Provides Security To The Electronic Medical Report

Ierin Babu
Assistant Professor
Information Technology
Adi Shankara Institute of Engineering and technology Kalady

Ajith Pappachan
Student
IT Department
ASIET, Kalady, Kerala ,India

Reshma Murukesh
Student
IT Department
ASIET, Kalady, Kerala ,India

Gayatheri K
Student
IT Department
ASIET, Kalady, Kerala ,India

Abstract

the importance of secret image sharing method is to provide privacy and security, which is an important concern in the medical field. Providing authentication and security to medical data is a challenging task. So as to overcome this challenge the visual secret sharing scheme is proposed. In this method transform the secret pixels into m-array notational system. A threshold value is set in order to reconstruct the original image. The original image is being encrypted and is then shared into proportions .A cover image is being provided to each of these shares. The stego image of high quality is being formed. While reconstructing the image the threshold value along with the minimum number of shares is given. This technique is implemented in the medical field for storing and sharing Electronic Medical Report.

Keywords: Stego Image, Encryption, Steganography, Decryption.

I. INTRODUCTION

Secret image sharing is a mechanism to shelter a secret image among a group of participants by encrypting the secret into shares and decrypting the secret with adequate shares. Conventional schemes generate meaningless shares, which are hard to categorize and lead to suspicion of secret image encryption. To overcome these problems, sharing schemes with steganography were accessible. The meaningless shared data were embedded into the cover image to form stego images. However, distorted stego images cannot be reverted to original. In this effort, a novel secret image sharing scheme with reversible steganography is projected. Main contribution of this work is that two-dimensional reversible cellular automata with memory are consumed to encrypt a secret image into shared data, which are then embedded into cover image for forming stego images. By assembling sufficient stego images, not only the secret image is lossless reconstructed, but also distorted stego image is reverted to original

II. VISUAL SECRET SHARING

Roughly speaking, the problem can be formulated as follows: There is a secret picture to be shared among n participants. The picture is divided into n transparencies (shares) such that if any m transparencies are placed together, the picture becomes visible, but if fewer than m transparencies are placed together, nothing can be seen. Such a scheme is constructed by viewing the secret picture as a set of black and white pixels and handling each pixel separately. The schemes are perfectly secure and easily implemented without any complex cryptographic computation.

III. PROPOSED SYSTEM

In our secret sharing (SS) mechanism it is applied basically to share a secret image. Here each participant has a private shadow; some authorized participants with integrated shadows can cooperate to recover the secret image. The purpose of secret sharing is to recover the secret image while some shadows are lost, distorted, or stolen. Along with the SS mechanism there added a threshold secret sharing system. In this scheme, a dealer can encode and divide secret data into n shadows. Then the dealer distributes the shadows to the involved participants. With any t out of n shadows, authorized participants can cooperate to reveal the secret data accurately.

Here in VSSwe convert each grayscale block into a binary block. First of alleach pixel value in a grayscale block is transformed into binary representation. For example take a grayscale block and transform into binary blocks.

111	159	20
254	10	198
40	215	100

Its corresponding binary blocks are as follows:

[0 1 1 0 1 1 1 1] [1 0 0 1 1 1 1 1] [0 0 0 1 0 1 0 0]

[1 1 1 1 1 1 1 0] [0 0 0 0 1 0 1 0] [1 1 0 0 0 1 1 0]

[0 0 1 0 1 0 0 0] [1 1 0 1 0 1 1 1] [0 1 1 0 0 1 0 0]

Take each binary block and go for different possible combinations of that block, and try to design the block into different shares. For example take a grayscale block and divide the block into shares and apply the above scheme.

A. Two-out-of-Three Scheme using Grayscale Images

Here we design the shares such a way that when combining any two shares will reveal the original bit information, but not the whole share just half of each single share will give the high quality image when reconstructed. We can explain this scheme by taking a value from the grayscale block and divide that value into shares.

1) Grayscale bits are transformed into Binary bits.

254: [1 1 1 1 1 1 1 0]

	1st half	2nd half
Share1:	0 1 0 1 0 1 0 0	1 1 0 1 1 0 1 0
Share2:	1 0 1 0 1 0 1 0	1 1 1 0 1 1 1 0
Share3:	0 0 1 0 0 1 0 0	1 0 0 1 0 1 0 0

Share1 (1st half): 0 1 0 1 0 1 0 0 Share3 (1st half): 0 0 1 0 0 1 0 0
Share2 (1st half): 1 0 1 0 1 0 1 0 Share1 (2nd half):1 1 0 1 10 1 0

1 1 1 1 1 1 1 0 = 254 1 1 1 1 1 1 1 0 =254

Share2 (2nd half): 1 1 1 0 1 1 1 0
Share3 (2nd half): 1 0 0 1 0 1 0 0

1 1 1 1 1 1 1 0 = 254

Combining any two half shares will give the exact bit and by doing the same procedure for the whole grayscale block gives the perfect high quality image when reconstructed without any loss of contrast.

2) Detailed Study of Proposed system

The significant essential of secret image sharing approaches is that the revealed content of the secret image must be lossless. Moreover, the distorted stego images can be reverted to the original cover image. In order to achieve these purposes, we first transform the secret pixels into them any notational system. Then, the information data used to reconstruct original pixels from camouflaged pixels are calculated. The information data and transformed secret data are shared using the (t, n)-threshold sharing scheme. In this way, we can retrieve the lossless secret image and reverse the stego image to the original image.

3) Understanding of Requirement

- The secret image and cover image is get identified.
- Using the software the secret image and cover image is added from the location.
- The user will set the number of shares and threshold.
- Shares are saved in different location which the user is interested with.
- At the retrieving area the cover image is get added from different locations.
- A key value is also added with the shares in order to provide security.
- When the threshold value is matched then the secret image is obtained from the cover image.

4) Algorithms Used

(1) Start
(2) Obtain the secret and the cover image.
(3) Enter the number of shares required for the image and set the value of i. Also enter the threshold value t
(4) Check whether the number of shares and the value of I assigned are equal
  4.1 Divide the image pixel by pixel among the shareholders.
  4.2 Enter the threshold value.
(5) Check whether the threshold value and the key value are equal
  5.1Retrieve the original image
  5.2Print the image cannot be displayed.

IV. THE EXPERIMENTAL RESULTS

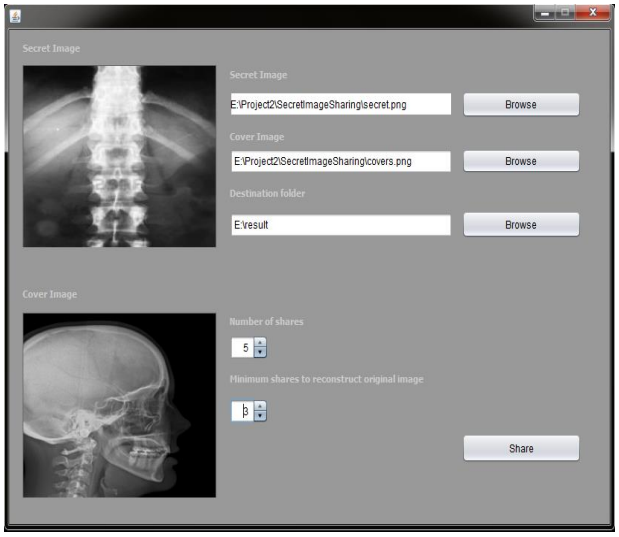

Fig. 1: Selecting The Secret Image, Cover Image, Destination

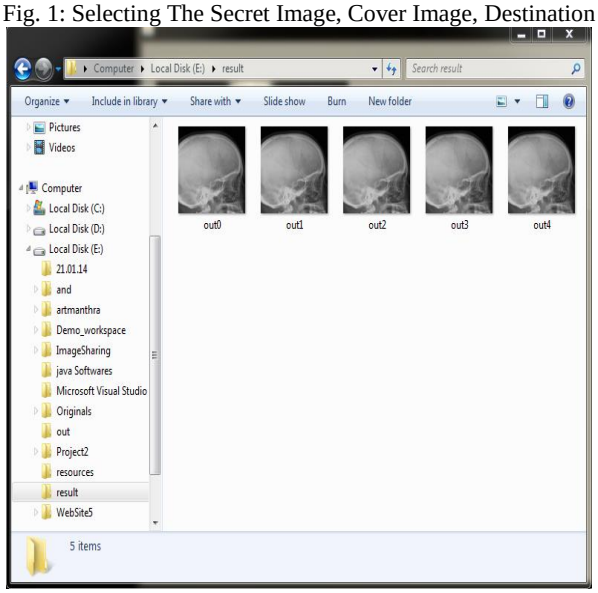

Fig. 2: Resulted Images After Sharing

Fig. 3: Application For Retrieving

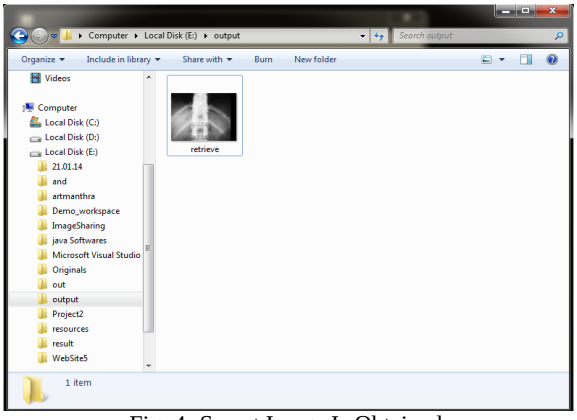

Fig. 4: Secret Image Is Obtained.

V. CONCLUSION

This project is predominantly intended in improving the authentication and the security that is being provided to the medical records. The encryption is the process of encoding the images and only the authorized persons can access the original image. Thus the security of the image can be enriched. Malpractices can be prevented by the method of sharing the images. Using the threshold value that is being set the original image cannot be recovered just by an individual. The access can be attained only with the knowledge and the permission of the users. Thereby the security of the image can be maintained. The cover image is being provided so as to hide the original image.

REFERENCES

[1] A. Shamir, "How to share a secret," Communications of the ACM, vol. 22, no. 11, pp. 612-613, 1979.
[2] C. C. Thien and J. C. Lin, "Secret image sharing," Computer &Graphics, vol. 26, no. 1, pp. 765-770, 2002.
[3] R. Zhao, J. J. Zhao, F. Dai and F. Q. Zhao, "A new image secretsharing scheme to identify cheaters," Computer Standards &Interfaces, doi: 10.1016/j.csi.2007.10.012, 2007.
[4] C. N. Yang, T. S. Chen, K. H. Yu and C. C. Wang, "Improvementsof image sharing with steganography and authentication," TheJournal of Systems and Software, vol. 80, no. 7, pp. 1070-1076,2007.
[5] D. M. Thodi and J. J. Rodriguez, "Expansion embedding techniques for reversible watermarking," *IEEE Transactions onImage Processing*, vol. 16, no. 3, pp. 721-730, 2007.
[6] M. Naor and A. Shamir, "Visual cryptography," *Advances inCryptology: Eurocrypt'94*, Spring-Verlag, Berlin, pp. 1-12, 1995.
[7] D.Stinson, Visual cryptography and thresholdschemes, Potentials, IEEE, 1999, Vol. 18 Issue: 1,pp. 13 -16.
[8] Carlo Blundo, University of Salerno , Alfredo DeSantis and Douglas R Stinson, University of Nebraska-Lincon, On the contrast in visual cryptography scheme, September 1996