Visual Cryptography for Medical Images Including Watermarking

Shanmuga Priya. P, Rengarajan Amirtharajan

Abstract*: *Security has become an indivisible question as Information Technology is ruling the world now. Cryptography is the technique to prove the inconceivable security for the secret data. Visual Cryptography is appropriate for any images, in which k out of n shares are enough to decrypt the clandestine information. It's a method of isolating the secret among a group of contributors and each contributor get a share of the secret. Here sufficient number of shares is combined to expose the secret. Main applications of Visual Cryptography are Bank customer identification, Biometric security and so on. This paper provides such methods to maintain the privacy of an individual's medical image and also embrace watermarking in the medical images, which provides copy right to the medical images of the concerned hospitals. Three Visual cryptography schemes are projected for medical image. Steps related to dividing the secret as shares are needed to be very hard to attack. These schemes mainly focused on decryption method, this act as an imperative utensil for getting efficient results.

Keywords: Medical image, Visual cryptography, secret information, watermarking, decryption.

I. INTRODUCTION

More and more progress in technology needs further security of data. Protecting this data in a safe way is the challenge for the upcoming technologist. For this, technologist provides many securing methods such as Cryptography, Steganography, Visual Cryptography, and Watermarking and so on. Although 'immune to attack', this only defines the strength of algorithm created by many technologist[1,2].

Cryptography is the origin of all securing methods, which begin with the data security[1,3]. Further it is extended to images nothing called Visual Cryptography[5]. The image security can be done using black and white pixels. It is based on vision of the person. It is possible to decrypt the encrypted image visually so it is named as visual cryptography. The first step of this method is half toning, which converts the input image into binary image. The binary image is composed of only black and white pixels. Each pixel is changed into n modified forms, this is termed as shares[8]. It is simple and very efficient in securing the information, because there is no need for key assigning and computational complexity in this. Steganography, which uses cover image to embed the secret data. But in visual cryptography, the images are secured by dividing it into number of shares; there is no need of cover here, share itself speaks. The decryption has to be done by superimposing the required number of shares[6,7].

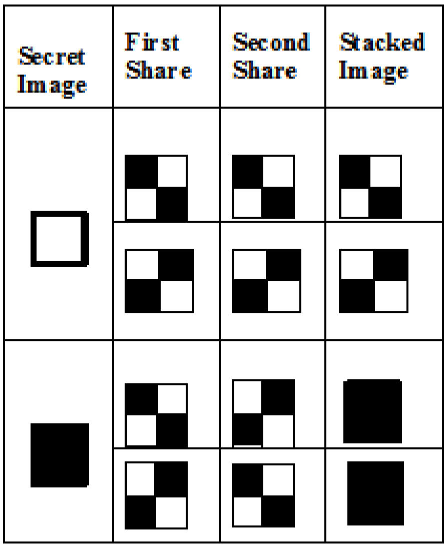


Fig. 1. Visual Cryptography scheme

This paper concentrates on sheltering medical images by using watermarking and visual cryptography techniques[4]. Watermarking which says the name of the service organization[5] and visual cryptography is for providing isolation to the medical images of the peoples. Here multiple medical images can be protected by creating less number of shares. This creates strength to the proposed method.

II. PROPOSED METHOD

The schematic diagram of the proposed method is shown in figure. The main aim of this method has to provide copyright to the service organizations medical image as well as to give the solitude to the people's medical report using visual cryptography. This paper describes three methods of visual cryptography.

The projected methods describes about the encryption of medical images done by shares. Each share is the grouping of black and white pixels. The main advantage of this scheme is that, each share individually cannot give the information about the clandestine image.Decryption does not requires any key or complex algorithm. Hence secret image is obtained by stacking the number of shares.

The general steps involved in this paper are described as follows. The first step has to embed the watermarking in the test

Revised Manuscript Received on November 22, 2019.

* Correspondence Author

Shanmuga priya P, Assistant Professor,ECE, Rajalakshmi Engineering college, Chennai, Tamilnadu. Email: shanmugapriya.p@rajalakshmi.edu.in

Rengarajan Amirtharajan,Professor, School of EEE, SASTRA University, Thanjavur, Tamilnadu. Email: amir@ ece.sastra.edu

inputs[9,10], then these images undergone half toning, that is the input images are converted into binary image. These binary images are encrypted into number of shares as per the prescribed scheme. These steps illustrated the encryption process. The decryption has to be done by superimposing the sufficient number of shares.

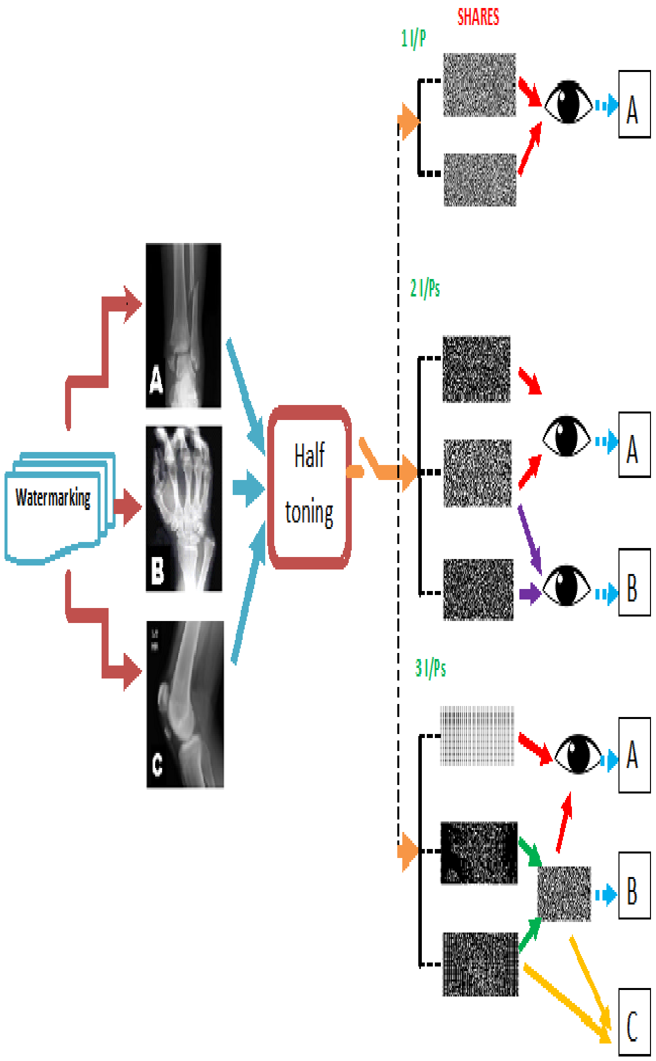
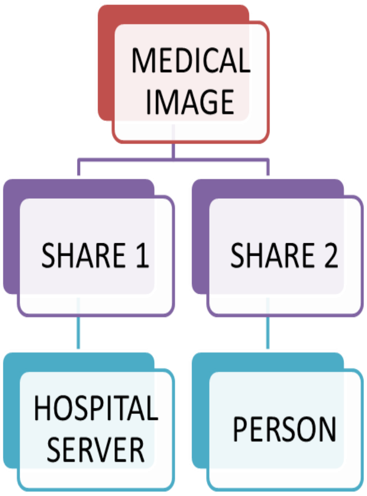
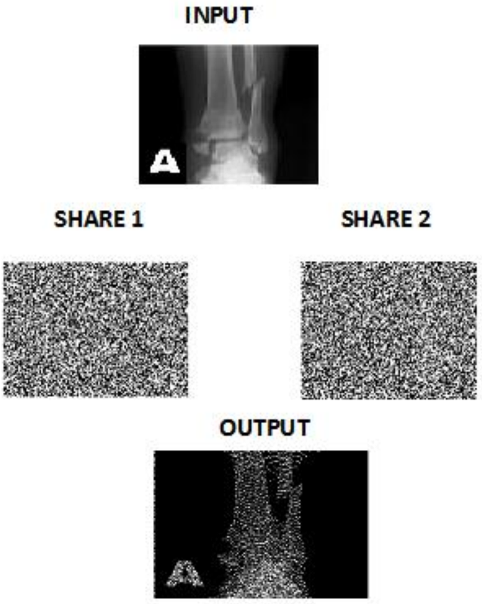


Fig. 2. Schematic Diagram of Proposed Method

A. *Method 1*

Method 1 involves only one watermarked medical image as input.Here '**A**' in the input image, which descrides the hospital A watermarking. This input is separated into 2 shares as per (k,n) threshold scheme.The first share has to be kept in the service organization server and the second share has given to the concerned person(whose image is kept as input).So this isolation provides privacy for the peoples medical report.One cannot visualize anything from single share,that is the medical image can be viewed only if both the shares are place over.Because of watermarking, the hospital can assert that this is my medical report.So this method provides safety to both peoples and service organization.

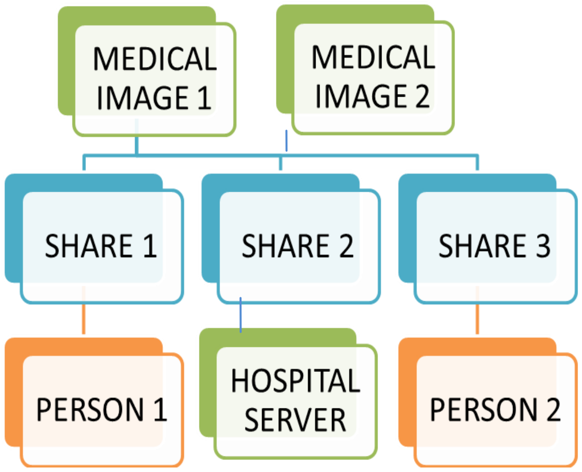


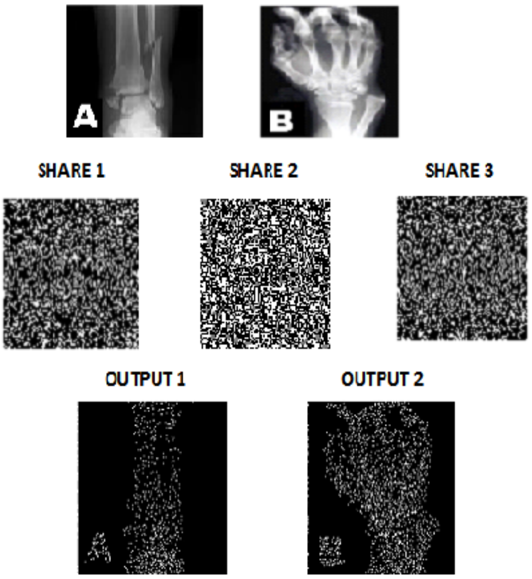


A Sample Result for Method 1

B. *Method 2*

In this method, three shares are created by getting two persons medical image as input. If we combine share1 and share 2, it reveals first persons medical image. One can visualize the second medical image by uniting share 2 and share 3. Hence share 2 is common for exposing both the outputs, this share2 should remain in the hospital server. Then share1 is given to first person and the share 3 is given to second person. This method uses only less memory to secure the medical images of many persons in the data base of the organization. Hence to secure two medical images, only one share is enough to be in the server.

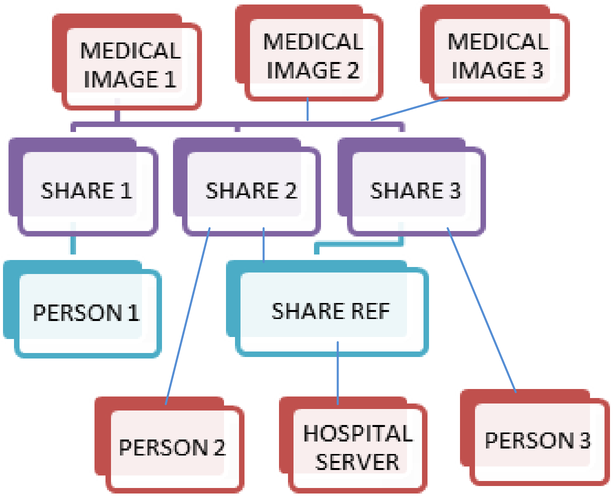


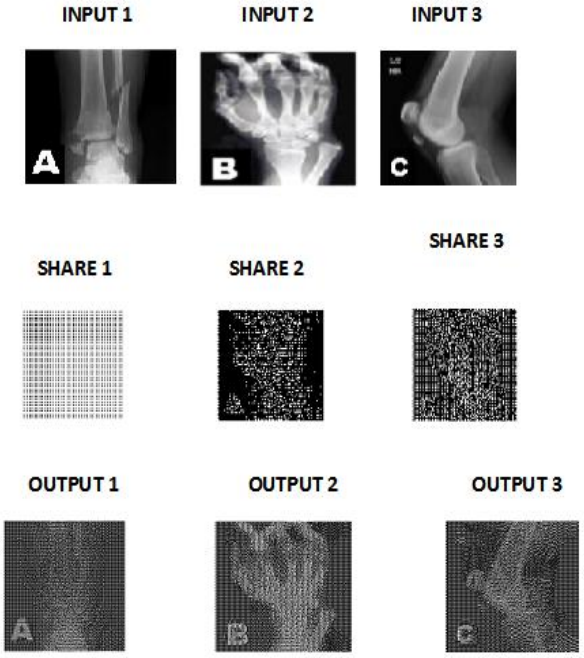


A Sample Result for Method 2

C. *METHOD 3:*

This method produces three shares for three input medical images. Here share 2 and share 3 are combined to give the share reference. With the help of share reference; one can decrypt three outputs.Share1 and share reference exposé the first person's medical image, share 2 and clockwise rotated share reference provides second medical image, share 3 and anticlockwise rotated share reference reveals third medical image. Hence the share reference (common share) has stored in the hospital data base, share1,share 2 and share 3 are given to person1, person 2 and person 3 respectively.





A Sample Result for Method 3

The first method which produces two shares by using one secret image. The second one creates two shares,which has two input medical image. With the reference of three images, three shares and all formed in third method.The share rotation is implemented in method 3 to get three images by combining different combinations of the encrypted shares.

III. CONCLUSION

Visual understanding is better than anything, because this is apart from any language. Many fields are available for securing confidential data/image. This paper describes visual cryptography with watermarking. Watermarking is the unique identity for service organization; this avoids any disputes regarding ownership of the image. Here the image to be protected is divided into shares. In order to reveal the protected image, these shares have to come together. This explains the extent to which data/image protection can be made. In case of multiple images to be protected, it is enough to create less number of shared images. One shared image is enough to protect multiple images. Thus these proposed techniques prove that less storage space is enough for protecting multiple images.

REFERENCES

1. Shaik, A., Thanikaiselvan, V., Amitharajan, R.2017. Data security through data hiding in images.A review. Journalof Artificial Intelligence, 10 (1), pp. 1-2
2. Iacovazzi, A., Elovici, Y 2017.Network Flow Watermarking: A Survey. IEEE Communications Surveys and Tutorials, 19 (1), art. no. 7570208, pp. 512-530.
3. Verma, V.S., Jha, R.K.2015. An Overview of Robust Digital Image Watermarking. IETE Technical Review (Institution of Electronics and Telecommunication Engineers, India), 32 (6), pp. 479-496
4. Mousavi,S.M.,Naghsh,A.,Abu-Bakar,S.A.R.2014. Watermarking Techniques used in Medical Images: A survey. Journal of Digital Imaging, 27 (6), pp. 714-729
5. Rani,M.M.S.,Mary,G.G.2017.Particle swarm optimization based image enhancement of visual cryptography shares. Studies in Computational Intelligence, 672, pp. 31-49.
6. Chao,H.C.,Fan,T.Y.2017.Generating random grid based visual secret sharing with multi-level encoding .Signal Processing: Image Communication, 57, pp. 60-67.
7. Ren,Y.,Liu,F.,Guo,T.,Feng,R.,Lin,D.2017. Cheating prevention visual cryptography scheme using latin square. IET Information Security, 11 (4), pp. 211-219.
8. Naor, M. and Shamir, A. (1995) Visual Cryptography. In: Proceedings of the Advances in Cryptology-EUROCRYPT'94, Lecture Notes in Computer Science (Volume 950), 1-12.
9. N. Mahesh Kumar and T. Manikandan, 'Non blind watermarking using contourlet transform,' in Indian Journal of Computer Science and Engineering,E-ISSN: 0976- 5166, P-ISSN: 2231-3850, vol.2, no. 1, pp. 31-38, 2011.
10. N. Mahesh Kumar, T. Manikandan and V. Sapthagirivasan 'Non blind image watermarking based similarity in contourlet domain,' in International Conference on Recent Trends in Information Technology at MIT, June 3-5,2011.

AUTHORS PROFILE

P. Shanmuga Priya is working as an Assistant professor in the department of ECE, Rajalakshmi Engineering College, Chennai India .She received her Master Degree from SASTRA University, Thanjavur,India in 2013. She obtained her bachelor's degree in Electronics and Communication Engineering from Kings College of Engineering, Thanjavur. She. Her research interests include Information security and Image processing.

Dr. Rengarajan Amirtharajan received the B.E. degree from the PSG College of Technology, Bharathiyar University, Coimbatore, India, in 1997. He received the M.Tech. and Ph.D. degrees from SASTRA University, Thanjavur, India, in 2007 and 2012, respectively. He is currently Professor with SEEE, SASTRA University. He has patented a novel embedding scheme USPTO in 2015. He has also published over 170 research articles in national and international journals