Hiding Medical Information of Patient through Image by Recursive Visual Cryptography

Varolia Jesalkumari Sagar
Assistant Professor,
Thakur College of Engineering and Technology
Mumbai, India

ABSTRACT
This paper introduces recursively hiding patient's information using XOR based Recursive Visual Cryptography. The XOR based Visual Cryptography Scheme (VCS) encodes a secret image of data into several shares which are not understood by intruders individually. Here (2, 2) VCS is considered for paper. Its pixel expansion has more columns then original and same number of rows but the image quality is good when it is decoded than traditional VCS. The proposed method is using concept of stereography as many information can be hidden in an image using recursive Visual Cryptography.

Keywords
Visual Cryptography, Image decomposition, superimpose, Pixel Expansion

1. INTRODUCTION
Internet is widely for data transmission which has increased the risk for data safety. Patient information are sensitive and needed to be protect during storage, especially in the cloud, and during transmission. In Visual cryptography mainly visual information is encrypted using encryption algorithm but here there is no need of decryption algorithm to reveal the visual information. But here since XOR based VCS is used the decryption process is done system. The technique was proposed by Moni Naor and Adi Shamir in 1994[1].Visual Cryptography uses two transparent images. They demonstrated a visual secret sharing scheme, where an image was broken up into n shares so that only someone with all n shares could decrypt the image, while any n-1 shares revealed no information about the original image. Each share was printed on a separate transparency, and decryption was performed by overlaying the shares. When all n shares were overlaid, the original image would appear. One image contains random pixels and the other image contains the secret information. It is impossible to retrieve the secret information from one of the images. [1]

The secret image is composed of black and white pixels. The original secret image can be recovered by superimposing the two share images together. The underlying operation of such a scheme is the logical operation OR. Generally, a(k, n)-VCS takes a secret image as input, and outputs share images that satisfy two conditions: First, any k out of n share images can recover the secret image; second, any less than k share images cannot get any information about the secret image. Similar models of visual cryptography with different underlying operations have been proposed, such as the XOR operation introduced in [2]–[3], and the NOT operation introduced in [3], which uses the reversing function of the copy machines.

2. WHY XOR-BASED VISUAL CRYPTOGRAPHY
A (k; n) visual cryptography (VC) scheme [1] is a type of secret sharing scheme with the special property that a secret image can be recovered visually by the human eye and does not require any calculation on a computer. However, the recovered secret image has low quality. In this case, some researchers attempt to consider other different approaches to improve the quality (contrast)of the recovered image. Lee et al. [11] presented a VC scheme using an XOR process to share a binary image.

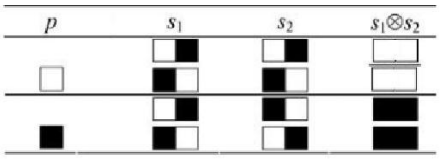
Following the notation from [1,2], a definition of k out of n XOR-based visual cryptography scheme is given.A (k, n) VC scheme S = (C0,C1) consists of two collections of n x m binary matrices C0 and C1.

Traditional Visual Cryptography has almost double pixels in its reconstructed image same as XOR-Based Visual Cryptography. The Reconstructed image in traditional Visual Cryptography had lost its original contrast specially in background but in XOR-Based Scheme the contrast is regained. If the decryption is done by software for stacking shares then both the method gives expected result but if the hard copy of shares are to be stacked then traditional VCS will have same output as softcopy but XOR-Based VCS will not have output as softcopy stacked.

Table 1. Comparison(XOR and Traditional VCS)

VCS type	Pixel Expansion	Contrast	Softcopy Decryption	Hardcopy Decryption
Traditional	More	Lost	Same as algorithm	Same as algorithm
XOR Based	More	Retained	Same as algorithm	Not Same

Table 2: (2, 2) XOR-based Visual Cryptography Scheme



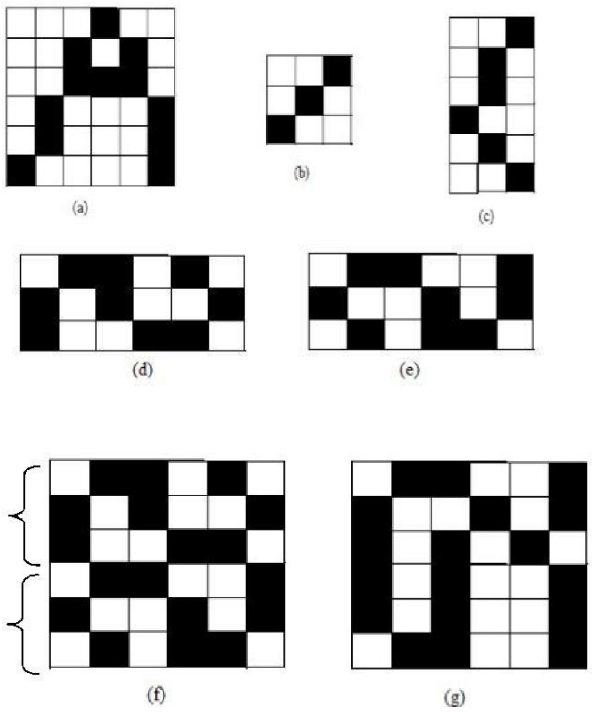
Here it is illustrated with 2-out-of-2 scheme. In the 2-out-of-2scheme, every secret pixel of the image is converted into two

shares and recovered by simply stacking two shares together. This is not equivalent to the OR operation between the shares but have to XOR the pixels. As illustrated in Table2 [4], 4 subpixels are generated from a pixel of the secret image in a way that 2 subpixels are white and2 pixels are black. The pixel selection is a random selection from each pattern. For example, when the corresponding pixel is white, one of the first six rows of Table 2 is randomly selected to encode the pixel into2 shares. It is easy to see that knowing only one share value does not reveal the other share and the secret image pixel. However superimposing all the shares reveals the corresponding binary secret image.

3. RECURSIVE VISUAL CRYPTOGRAPHY

Please use a 9-point Times Roman font, or other Roman font with serifs, as close as possible in appearance to Times Roman in which these guidelines have been set. The goal is to have a 9-point text, as you see here. Please use sans-serif or non-proportional fonts only for special purposes, such as distinguishing source code text. If Times Roman is not available, try the font named Computer Modern Roman. On a Macintosh, use the font named Times. Right margins should be justified, not ragged.

Example is given in Figure 1 to explain the concept. Here three images are considered where in original image (6x6) patient's record is there, Secret message 1(3x3) is about patient's medical details and secret message 2 (6x3)is patient's personal detail. First Visual cryptography is to be applied on secret message 1 image of size 3x3 and two shares are generated of size 3x6.To generated share 1 of secret message 2 image both the shares of secret message 1are concatenated which makes share1 of size 6x6.



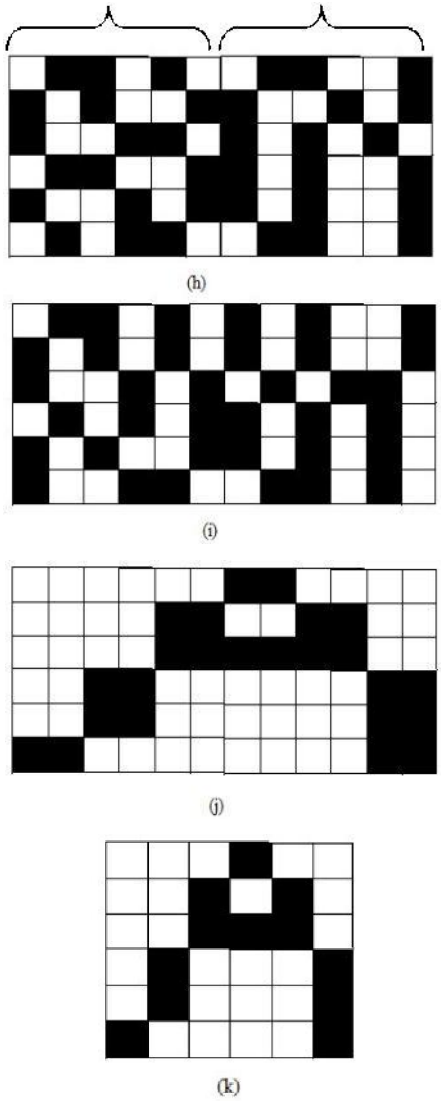


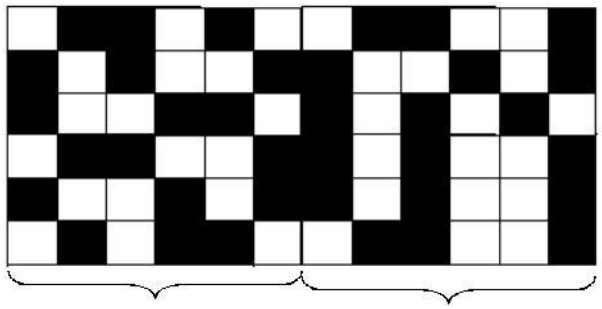
Figure 1 (a)Original Message (6x6) (b) Secret Message 1(3x3) (c) Secret Message 2 (6x3) (d) Share 1 of Secret Message 1(3x6) (e) Share 2 of Secret Message 1(3x6) (f) Share 1 of Secret Message 2 (6x6) (g) Share 2 of Secret Message 2 (6x6) (h) Share 1 of Original Message (6x12) (i) Share 2 of Original Message(6x12) (j) Decoded Original Image (6x12) (k) Reconstructed Original Message(6x6)

Share 2 is generated of size 6x6 with respect to share 1 such that by decoding shares using XOR based VC Secret message 2 is to be decoded. Now using these two shares of secret image 2 , share 1 of Original secret is generated. For that both the shares are combined and share1 of size 6x12 is generated and XOR based VC. To decode the original message of same size as its original size which is 6x6 here ,size reduction algorithm is used ,which is mentioned below, reconstructed image is achieved.

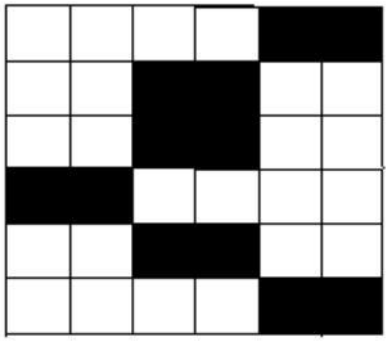
Size reduction algorithm.

1. Consider decoded image and one image with the size of original message with all pixels white.
2. Color the ith pixel with black color if 2i-1 and 2i both pixels is black for same row (because number of rows are same) in decoded image.

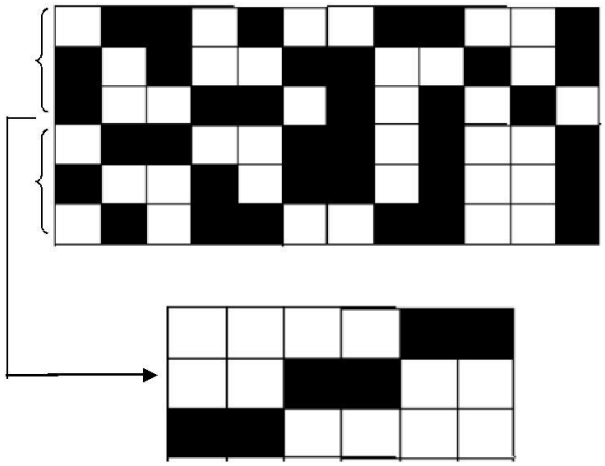
3. Repeat the steps for all the pixels.



(a)



(b)



(d)

Figure 2. (a) Share 1of Original Message (6x12) (b) Decoded Secret Message 2(6x6) (c) Share 1of Original Message (6x12) (d) Decoded Secret Message 1(3x6)

In this method, first share of original image acts as Cipher (which contains hidden message) and second share acts as a key to decode original message. Shown in figure 2 that share 1 can reveal secret message 1 and secret message 2 by alone but to decode original message share 2 is needed. Share 1 can be horizontally then one can reveal secret image 1 using XOR based VCS.

It means in our medical consideration patient's sensitive details can be safely stored on cloud or can be transmitted over network because the share does not reveal any information until and unless key share is available.

4. ADVANTAGES

The proposed method is good in securing sensitive data of patient as it is storing it in random image format which reveals no information and for the data which is not so sensitive but has to be hidden, can be stored in share 1 so that every time share 2 is not required for verification. The best part is three information pieces are stored in two shares without any indication to intruders.XOR based VCS decodes original image with far better quality mostly for binary images.

5. CONCLUSION

The implementation of this method requires training as patient's information is not stored in image format today but VCS hides information in image format only because it plays with pixels so all data has to be stored in image format first and then encrypted. Comparing traditional VCS with XOR based visual cryptography; XOR based visual Cryptography gives better visual quality. Generated shares are random dots so it doesn't reveal secret information. In future, it can be extended for Colored image. One can store more then one information in shares which makes our algorithm efficient and no pixel expansion is there because of size reduction algorithm with less complexity.

Recursive Visual Cryptography is an excellent option for applications where more data to be hidden stored . It can be built for less number of participants to greater number of participants. The advantages of such type of Recursive Visual cryptographic scheme are: Original image security is provided. Secure Authentication is provided. Chance of fake share creation is not possible. More than one image be kept as secret. This work is an attempt to make a secured transfer of valuable images between trusted parties. The confidentiality is maintained and the authentication can be checked by digital signatures. The proposed method can be considered as a good candidate for secure visual data transmission in systems with limited bandwidth.

6. REFERENCES

[1] Naor, M. and Shamir, A. 1995. Visual Cryptography. Advances in Cryptography-Eurocrypt, 950: 1-12.

[2] Gnanaguruparan, M. and Kak, S. 2002. Recursive Hiding of Secrets in Visual Cryptography. Cryptologia 26: 68-76.

[3] D. Q. Viet and K. Kurosawa, "Almost ideal contrast visual cryptography with reversing," Topics in Cryptology—CT-RSA,pp. 353–365, 2004.

[4] E. Biham and A. Itzkovitz, "Visual cryptography with polarization," in RUMP Session of CRYPTO'98, 1997.

[5] G. Ateniese, C. Blundo, A. De Santis and D. R. Stinson, "Visual cryptography for general access structures", Information and Computation 129 (1996), 86-106.

[6] M. Naor and A. Shamir, "Visual cryptography II: improving the constrast via the cover base, in Security Protocols", M. Lomas, ed., Lecture Notes in Computer Science 1189 (1997), 197-202.

[7] M. Naor and A. Shamir, Visual cryptography, in "Advances in Cryptology { EUROCRYPT '94", A.De Santis, ed., Lecture Notes in Computer Science 950 (1995), 1-12.

[8] P.S.Revenkar, Anisa Anjum, W .Z.GandhareGovernment College of Engineering, Aurangabad, M.S., India"Survey

of Visual Cryptography Schemes" International Journal of Security and Its Applications Vol. 4, No. 2, April, 2010.

[9] W. Hawkes, A. Yasinsac, C. Cline, An Application of Visual Cryptography to Financial Documents, technical report TR001001, Florida State University (2000).

[10] R. Gonzalez and R. Woods, Digital Image Processing using MATLAB, Fourth Impression, 2008.

[11] Kai-Hui Lee and Pei-Ling Chiu "An Extended Visual Cryptography Algorithm for General Access Structures" - IEEE transactions on information forensics and security, vol. 7, no. 1, february 2012.