A Hybrid Visual Cryptographic Lossless Image Sharing Scheme based on Bit Sharing

B. Reddaiah
Department of Computer Applications,
Yogi Vemana University, Kadapa, India

K. Srinivasa Rao
Department of Computer Applications,
Yogi Vemana University, Kadapa, India

P. V. Gowtham
Department of Computer Applications,
Yogi Vemana University, Kadapa, India

ABSTRACT
Visual cryptography is a technique that is used to share the secret data in the form of images for acquiring data security. This technique involves encryption and decryption processes for securing data. In encryption process the original image is divided into number of shares and then sends to other end. In decryption by using simple computations the subset of shares combined to reconstruct the original image. In the proposed method by using bit sharing method the original image is divided into four shares. These shares are covered with different cover images by using genetic algorithm and mathematical operations along with column transposition.

Keywords
Visual cryptography, lossless, Image sharing, Bit sharing, LSB, Crossover, Column transposition.

1. INTRODUCTION
Today more information is shared through internet only, where there is more possible for the attacks and hacking. So, there is need to secure the data while sharing through internet. Visual cryptography is a technique used to provide security for visual data like images, text and videos. It is a cryptographic method in which the decryption is done by Human Visual System (HVS), that it does not require any computational device. Thus, by this there is no need of hardware and software requirement in decryption process [2]. An example of encryption and decryption of visual cryptography was shown in figure1.

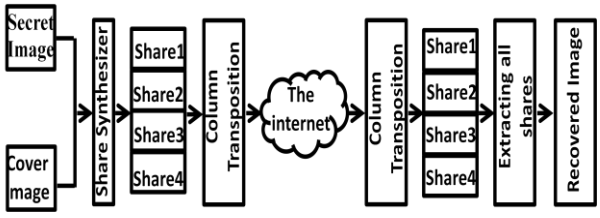

Fig.1: Model of Security Sharing based on Visual Cryptography

For encryption, a secret and cover images are given as inputs to the share synthesizer. Here each share was combined with each cover image. Again from the share synthesizer shares are given as output. For that share column transposition is performed and sends to other end. In decryption to reconstruct the original image, column transposition is used. From that, shares output is derived. Now by extracting all shares the original image is reconstructed by using simple mathematical computation.

2. RELATED WORK
Blakley [9] and Shamir are the two persons, who introduced secret sharing scheme initially. Then many efficient techniques were introduced based on polynomial based scheme, threshold based schemes and Huffman coding schemes [1, 3, 5, 7]. After that Naor proposed a new type of secret sharing scheme called Visual Cryptography (VC). In the same way many other visual cryptographic techniques were proposed based on Latin squares [4], based on blue-noise dithering principles [6], based on optimal pixel expansion, based on embedded random shares, based on position exchange technique [8], based on bit slicing technique. Here visual cryptography is used for grey scale image, but it is not limited to grey scale and binary images and color images too. In this paper, we used bit sharing concept to create the share images from secret image and simple operations to combine the shares with cover images.

3. PROPOSED WORK
In the proposed method, Gray scale secret image can be transmitted securely by using on bit sharing method. If the secret image is a gray scale image, each pixel is represented as set of 8 bits as shown in figure2.

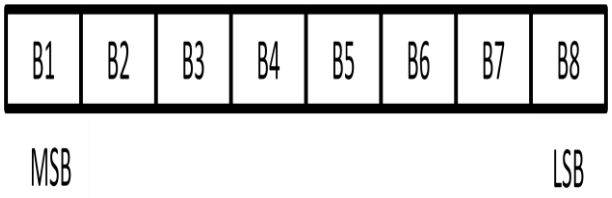

Fig.2: Representation of Pixel – Grey scale image

Secret image is encrypted by dividing the image into shares and each share is combined with each cover image. Initially, one pixel is taken from the secret image and it is divided into four shares. Firstly all pixels of all shares are considered as black, its intensity is 0, and they are known as share1, share2, share3 and share4. The first two bits of the pixel (B1 and B2) are added to the share1 from LSB positions and it is treated as share (1,2), the next two bits of the pixel (B3 and B4) are added to the last two LSB positions of share2 and it is treated as share (3,4). Next two bits of the pixel (B5 and B6) are added to the last two LSB positions of share3 and it is treated as share (5,6) and last two bits of the pixel (B7 and B8) are added to the last two LSB positions of share4 and it is treated as share(7,8). Then four imaginary gray scale images are picked, that are same in size of secret image. To combine the secret shares with cover image we use crossover operation, addition operation and column transposition to get cipher text, as shown in figure3, and the reverse process decryption is shown in figure 4.

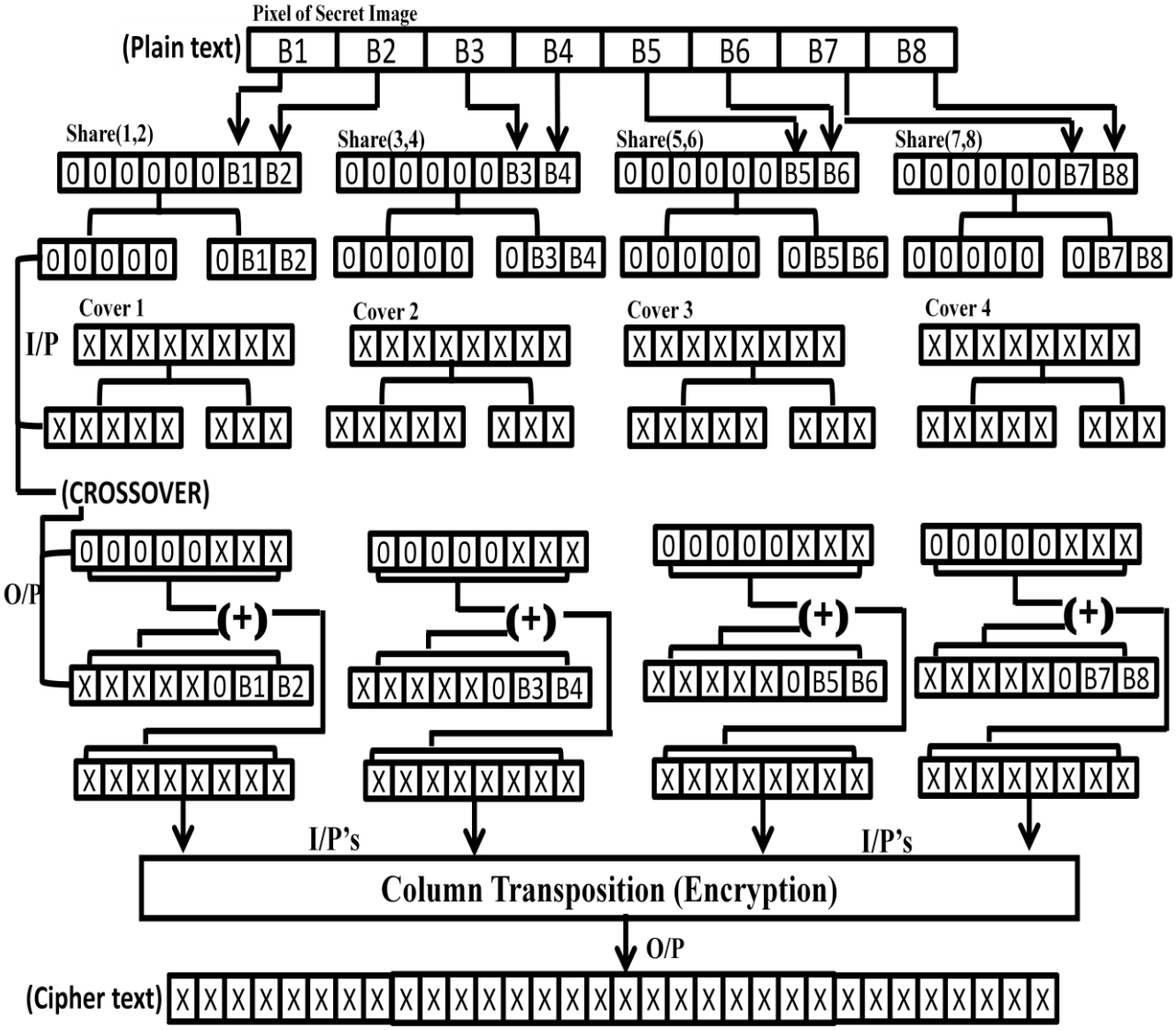

Fig.3: Block Diagram of Proposed Encryption Model for Bit Sharing using Visual Cryptography

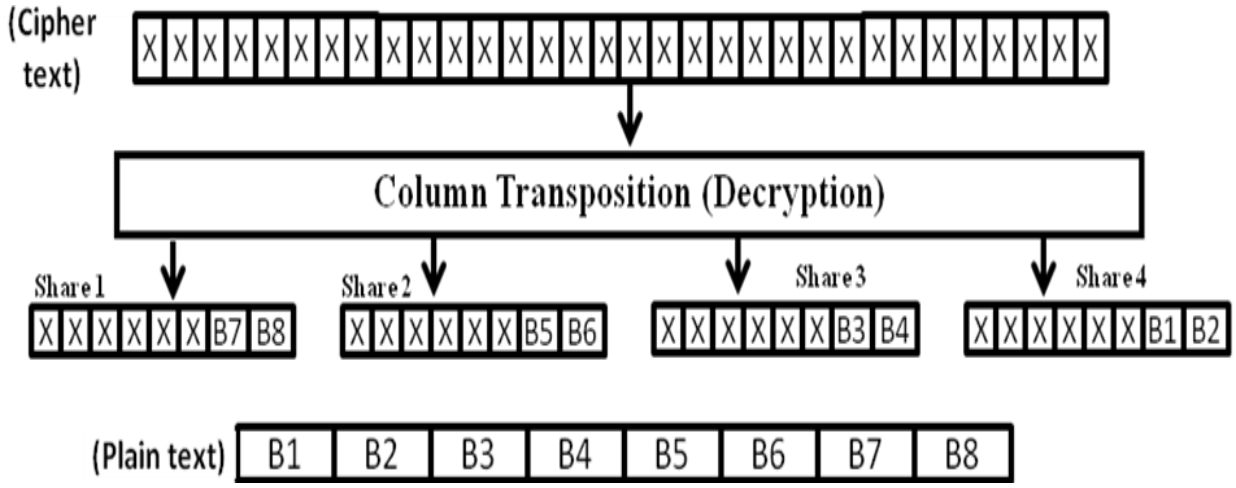

Fig.4: Block Diagram of Proposed Decryption Model for Bit Sharing using Visual Cryptography

3.1 Illustration of Proposed Model with example.

For example, the first pixel of the secret image is assumed to be 25 i.e., 00011001.Since, secret image is dividing into four shares and four different cover images are taken. The pixel values of each cover image (cover1, cover2, cover3 and cover4) are assumed to be 33, 29, 15 and 7 respectively. The process and resulted shares of the encryption and decryption are shown in figure 5 and figure 6 respectively.

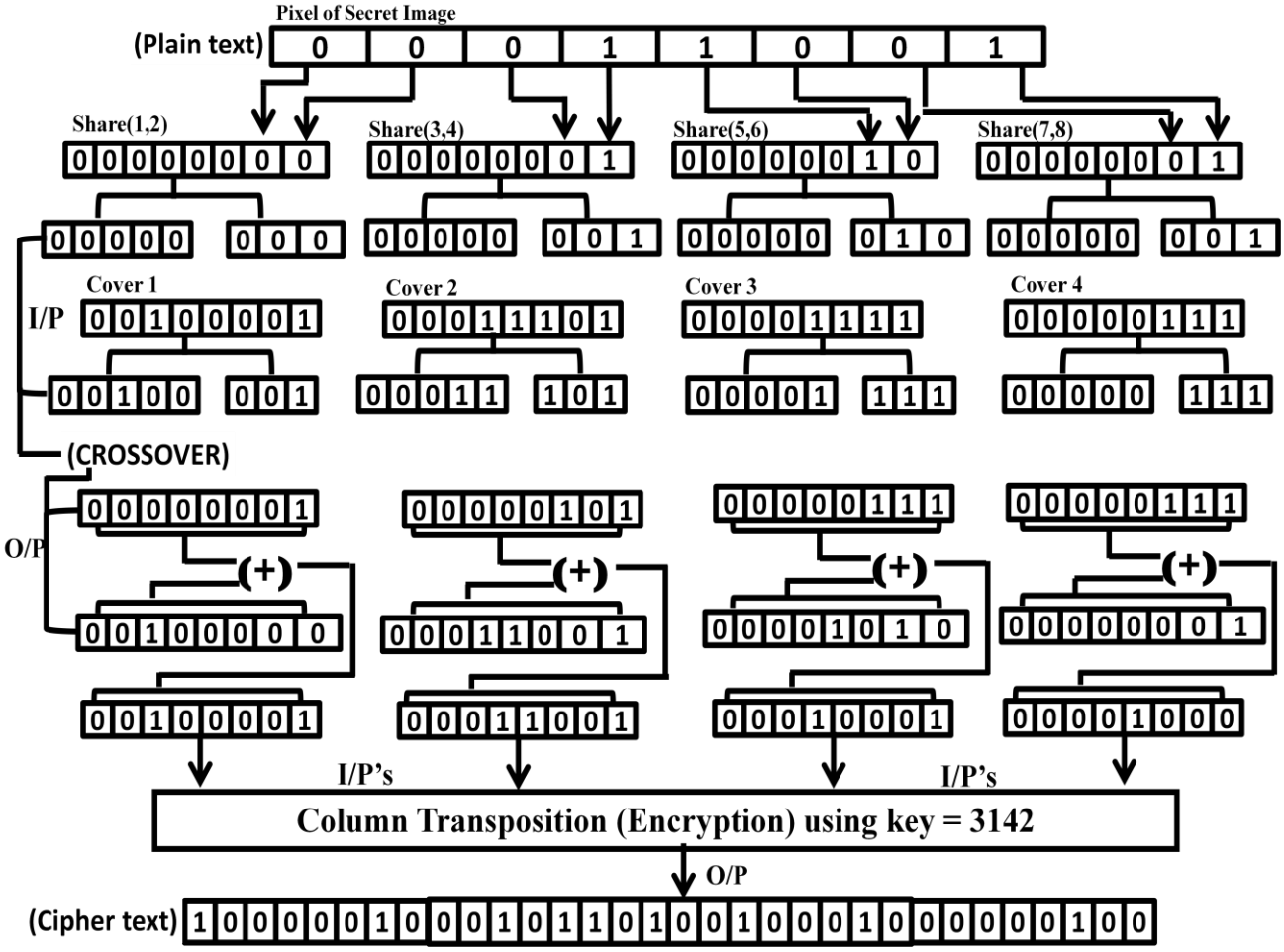

Fig.5: Example of Proposed Encryption Model for Bit Sharing using Visual Cryptography

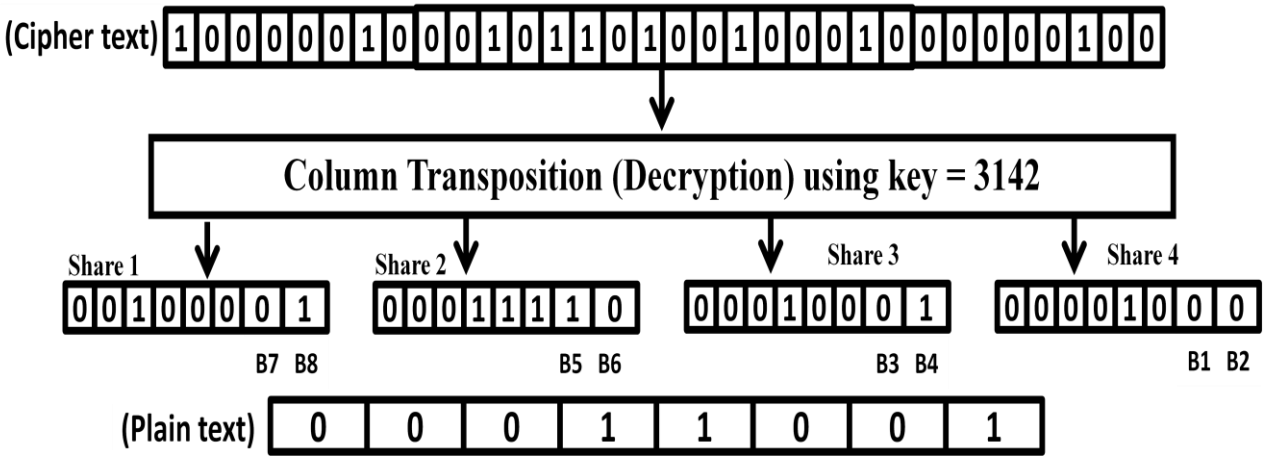

Fig.6: Example of Proposed Decryption Model for Bit Sharing using Visual Cryptography

4. IMPLEMENTATION AND RESULTS

The proposed approach uses bit sharing method of visual cryptography on gray scale images. It is implemented to encrypt the gray scale images and results are presented in table 1 and table 2.

4.1 Encryption

Table1: Results of encryption

Binary representation of first pixel	By using Two-bit sharing method				Pixels from imaginary Cover Images			
	Share1	Share2	Share3	Share4	First pixel from Cover image1	First pixel from Cover image2	First pixel from Cover image3	First pixel from Cover image4
0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0
0	0	0	0	0	1	0	0	0
1	0	0	0	0	0	1	0	0
1	0	0	0	0	0	1	1	0
0	0	0	0	0	0	1	1	1
0	0	0	1	0	0	0	1	1
1	0	1	0	1	1	1	1	1

Here crossover operation is performed for all shares and pixels of cover images.

Table2: Results of encryption continued

Output of Crossover1		Output of Crossover2		Output of Crossover3		Output of Crossover4		Addition operation for all crossover outputs			
o/p1	o/p2	o/p1	o/p2	o/p1	o/p2	o/p1	o/p2	Output1	Output2	Output3	Output4
0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0
0	1	0	0	0	0	0	0	1	0	0	0
0	0	0	1	0	0	0	0	0	1	1	0
0	0	0	1	0	1	0	0	0	1	0	1
0	0	1	0	1	0	1	0	0	1	0	0
0	0	0	0	1	1	1	0	0	1	0	0
1	0	1	1	1	0	1	1	1	0	1	0

4.2 Decryption

After using the column transposition in reverse, table 3 shows the recovered secret image without any loss and its resolution remains the same as previous.

Table3: Results of encryption continued

Share1	Share2	Share3	Share4	Original recovered image pixel
0	0	0	0	0
0	0	0	0	0
1	0	0	0	0
0	1	1	0	1
0	1	0	1	1
0	1	0	0	0
0	1	0	0	0
1	0	1	0	1

5. CONCLUSION

This proposed system from visual cryptography is based on bit sharing and on grey scale level images. Four shares are created to encrypt an image, based on position of bit. These shares are merged with cover images. To make the system complex crossover method from Genetic algorithms is used. Along with that column transposition is also used that makes the system more complex. While decrypting to recover secret image from shares data is integrated without any loss. The practical implementation of proposed system is low cost and time saving.

6. REFERENCES

[1] J. Benaloh, J. Leichter.: Generalized secret sharing and monotone functions, In S. Goldwasser, CRYPTO-88, Springer LNCS 403, pp. 27-35. Springer-Verlag, 1990, DOI: 10.1007/0-387-34799-2-3.

[2] M. Naor, A. Shamir.: Visual Cryptography. In: EUROCRYPT 1994, Springer LNCS, vol. 950, pp. 1-12. Springer, doi: 10.1007/BFb0053419.

[3] M. Bertilsson, I. Ingemarsson.: A construction of practical secret sharing schemes using linear block codes, In J. Seberry and Y. Zheng, editors, AUSCRYPT-92, volume 718 of Lecture Notes in Computer Science, pp. 67-79. Springer-Verlag, 1993, doi: 10.1007-3-540-48969-X.

[4] A. Adhikari, M. Bose.: A new visual cryptographic scheme using Latin squares, IEICE Transactions on Fundamentals, Springer AISC249, pp:1998-2002, 2004, doi: 10.1007/078-3-319-03095-1-x.

[5] Ran-Zan Wang, Chin-Hui Su.: Secret image sharing smaller shadow images, Pattern Recognition Letters 27, Elsevier, 2006, pp: 551-555, 0.1016/j.patree.2005, 09.021.

[6] Zhou, Z., Arce, G.R., Crescenzo, G.D.: Halftone Visual Cryptography, IEEE Transactions on Image Processing, 2006, pp: 2441-2453, doi: 10.1109/TIP.2006.875249.

[7] Ch. Ratna Babu, M. Sridhar, Dr. B. Raveendra Babu.: Information Hiding in Gray Scale Images using Pscudo-Randomized Visual Cryptography Algorithm for Visual Information Security, ICISCON-2013, IEEExplorer 2013, pp: 195-199, doi: 10.1109/ICISCON.2013.6524202.

[8] A. Dutta, D. K. Kole.: An Efficient Secret Image Sharing Scheme Using an Effectual Position Exchange Technique., ICT and Critical Infrastructure: Proceedings of the 48th Annual Convention of Computer Society of India - vol II. Springer – AISC, vol 249, 2014, doi: 10.1007/978-3-319-0-03095-1-25.

[9] G. R Blakley, Safeguarding cryptographic keys, AFIPS Conference Proceedings, vol. 48, 1979, pp: 313-317.