International Journal of Engineering Research and Science & Technology

IJERST

ISSN : 2319-5991
Vol. 4, No. 1
February 2015

www.ijerst.com

Email: editorijerst@gmail.com or editor@ijerst.com

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
Vol. 3, No. 4, November 2014

Research Paper

IMPROVED ALGORITHM FOR VISUAL CRYPTOGRAPHY USING REGION INCREMENTATION

Priyanka Agrawal[1]* and Vijay Kumar Sharma[1]

Corresponding Author: **Priyanka Agrawal ✉ Priyanka_jnit@yahoo.com*

Region incrementing visual cryptography is used to hide multiple secrecy levels in a single image. In n level region incrementing visual cryptography scheme, image is divided in n regions. Each region consists of one level information. For implementing visual cryptography in n levels we need to encode (n+1) shares in such a way so that any single share is not able to show the information and by combining any two shares, first level information would be visible. Similarly by superimposing any three shares, information upto second level could be seen. In similar way, for revealing whole information all the (n+1) shares are superimposed. These n levels are created according to user specification. In proposed scheme, user does not need to address the area of different levels manually and levels are created automatically. User needs only to use a particular level information with a particular size of text. The traditional region incrementing visual cryptography scheme has been modified to address the problem of pixel expansion and poor contrast. In proposed algorithm, problem of pixel expansion and poor contrast has been removed and further it is modified to generate the levels automatically which is named as automatic region incrementing visual cryptography.

Keywords: Visual cryptography

INTRODUCTION

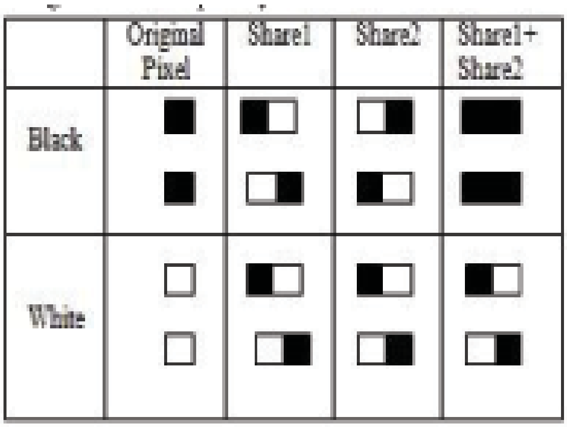
Visual cryptography is an encryption technique which is used to hide information which is present in an image. Visual cryptography scheme was developed by Naor and Shamir in 1994. In this scheme two transparent images called shares are developed. One of the share is made of random pixels in which black and white pixels are of equal number. Second share is made according to first share. When these two shares are superimposed, information is revealed, Some smaller blocks are used in place of single pixel of original image which is needed to be encrypted. If two blocks are used for representing one pixel of original image, one of the block will be white and second one will be black. In the similar way, if four blocks are used in place of one pixel, two of those pixels will be white and remaining will be black.

Now two layers are created. One layer will have all the pixels in random state, one of the six possible states. Share 2 is same as share 1,

[1] Department of Computer Science, Rajasthan Institute of Engineering & Technology, Jaipur.

except for the information pixels. These pixels are in opposite state in share 1. When both shares are superimposed, the pixels identical will be seen as gray and remaining will be completely black.

Figure 1: Black Pixel And White Pixel in Visual Cryptography With Two Sub Pixel Layout



	Original Pixel	Share1	Share2	Share1+ Share2
Black	■	■□	□■	■■
	■	□■	■□	■■
White	□	■□	■□	■□
	□	□■	□■	□■

In the above method we have used four pixels in place of single pixel of secret image. Therefore we got pixel expansion four, i.e., reconstructed image will be four times larger than secret image as shown in Figure 2.

Figure 2: A 2-out-of-2 VCS with 4-subpixel layout: (a) Secret Image S, (b) First Share S1, (c) Second Share S2, and (d) Reconstructed Image by Superimposing S1 and S2

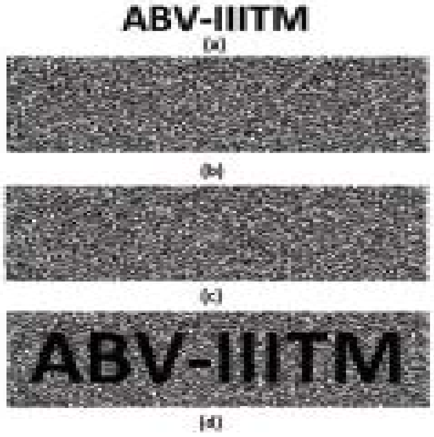
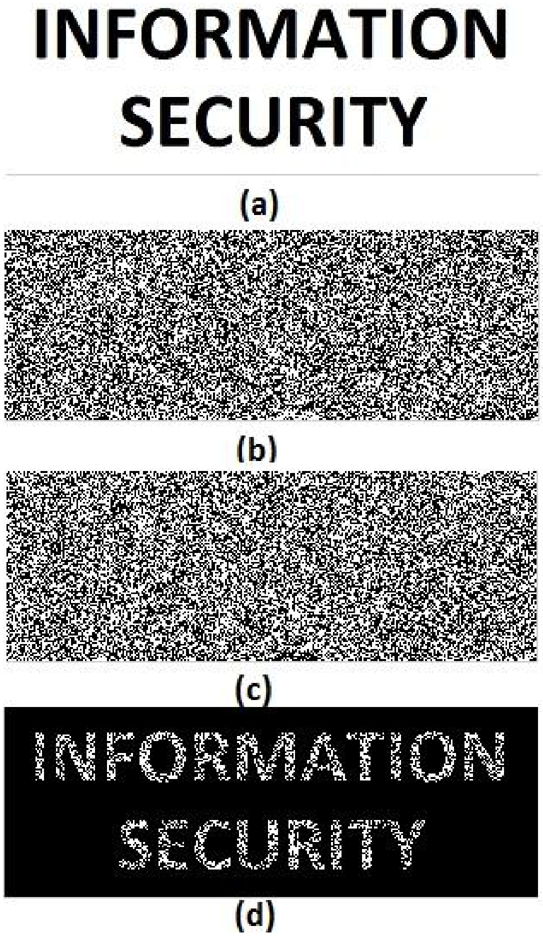


Figure 3: A 2-out-of-2 VCS with inverted colors: (a) Secret Image S, (b) First Share S1, (c) Second Share S2, and (d) Reconstructed Image by Superimposing S1 and S2



LITERATURE REVIEW

Visual Cryptography (VC), invented by Noar and Shamir (1995), is a method for protecting image-based secrets that has a computation-free decoding process. Two transparent images called shares are developed. One of the share is made of random pixels in which black and white pixels are of equal number. Second share is made according to first share. When these two shares are superimposed, information is revealed.

For visual cryptography a smaller pixel expansion and high contrast is desirable because smaller pixel expansion is beneficial for storage and printing out purpose. High contrast is required for easily recognizing the secret image by the unaided eye. On the contrast in visual cryptography schemes by Blundo *et al.* (1999) describes the minimum pixel expansion and maximum contrast.

For increasing the contrast of image additional white pixels are added in Contrast-enhanced visual cryptography schemes based on additional pixel patterns by Monoth and Babu (2010). For removing pixel expansion, shared of secret image were generated from matrices.

Visual cryptography was also used in the form of rotating angles in which we continue rotate the angles of superimposed shares and different reconstructed images are revealed. The ringed shadow image technology of visual cryptography by applying diverse rotating angles to hide the secret sharing by Hsu *et al*. (2004).

Visual cryptography was used for various applications, e.g., scan application. The method to use visual cryptography as scan application has been given by Yan *et al.* (2004). Visual cryptography was also used for biometric representation e.g. finger print application. Visual cryptography was also joined with watermarking by Fu and Au (2004) first time. One more application of visual cryptography is that it can be used in medical images and forgery detection as by Manimurugan and Porkumaran (2011).

METHODOLOGY

Region Incrementing Visual Cryptography generates the shares in such a way when we superimpose any two shares, information belonging to first level should be revealed. As we increase the number of shares, corresponding level information is revealed. Depending on the number of levels RIVC may be of 2-level, 3 level or more.

Matrix LK_j^0, where j is the level number and 0 represents white pixel. In the similar manner LK_j^1 represents the basis matrix for encoding a black pixel of the jth level. Matrices C_j^0 and C_j^1 for encoding white and black pixels, These matrices are obtained by the permutation of columns of LK_j^0 and LK_j^1.

Traditional RIVC

For each pixel of secret image a matrix is obtained by the permutation of columns of LK_j^0 and LK_j^1. C_k^0 is used to encode a white pixel and C_k^1 is used to encode a black pixel. Now first row of this matrix, according to secret image's pixel is given to first share, second row is given to second share and so on. As there are four columns in any row, four pixel will occupy the place of share corresponding to one pixel of secret image. This will result in pixel expansion four. Wang (2009) provided the basis matrices for the construction of 2-level RIVC scheme.

$$LK_1^0 = LK_2^0 = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$$

$$LK_1^1 = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

$$LK_2^1 = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix}$$

Similarly basis matrices for constructing the 3-level RIVC scheme are given below-

$LK_1^0 = LK_2^0 = LK_3^0 =$

$$LK_1^1 = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

$$LK_2^1 = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \end{bmatrix}$$

$$LK_3^1 = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \end{bmatrix}$$

In this scheme, there are some drawbacks. First drawback is that the address of different levels are given by the user manually everytime. Another drawback is that revealed image bears from pixel expansion m, i.e., the revealed image is m times greater than original image. Also contrast of third level is very low.

We propose the (2, n)-RIVCS in which user does not need to address the area of different levels manually. Levels are created automatically. User needs only to use a particular level information with a particular size of text. A generalized form of traditional region incrementing visual cryptography with extra features added as no pixel expansion and improved contrast is proposed in this scheme.

Proposed Scheme for RIVC with Enhanced Contrast and No Pixel Expansion

In proposed two level and three level RIVC we have selected a column randomly from proposed basis matrices for distributing the values to shares for any particular pixel of image to be decoded. By this concept we use only one pixel in one share corresponding to one pixel of image to be encoded. This method does not increase the pixel expansion, i.e., proposed method generates the reconstructed image of same size as that of original image.

Basis matrices for proposed 2-level scheme are shown below:

$$LK_1^0 = \begin{bmatrix} 0 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix}$$

$$LK_2^0 = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$$

$$LK_1^1 = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$$

$$LK_2^1 = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix}$$

The detailed procedure for proposed 2-level RIVC scheme is presented in ALGORITHM 1.

ALGORITHM 1: Proposed 2-level scheme

1) Select a binary image which needs to be sent secretly.
2) Divide the secret image in two levels according to their significance.
3) Assign level 1 to less significant secret and level 2 to more significant part.
4) For first level white pixel, select one column randomly from LK_1^0.
5) Repeat step 4 through 5 for each pixel of the secret image by selecting appropriate basis matrices.
6) Record the three encoded shares obtained at the end of step 5.

The procedure from Step 1 through 7 will generate three encoded shares. These shares will be sent over the communication medium, At receiver side any 2 out of 3 shares are superimposed to reveal first level information and all 3 shares are superimposed to reveal complete secret image.

Basis matrices for 3-level RIVC scheme are given below:

$$LK_1^0 = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix}$$

$$LK_2^0 = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \end{bmatrix}$$

$$LK_3^0 = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}$$

$$LK_1^1 = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$$

$$LK_2^1 = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}$$

$$LK_3^1 = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}$$

The detailed procedure for proposed 3-level RIVC scheme is presented in ALGORITHM 2.

ALGORITHM 2: Proposed 3-level scheme

1) Select a binary image which needs to be sent secretly.
2) Divide the secret image in three levels according to their significance.
3) Assign level 1 to least significant secret and level 3 to most significant part.
4) For first level white pixel, select one column randomly from LK_1^0.
5) Repeat step 4 through 5 for each pixel of the secret image by selecting appropriate basis matrices.
6) Record the three encoded shares obtained at the end of step 5.

Proposed Automatic RIVC with No Pixel Expansion

In proposed Automatic RIVC user does not need to address the area of different levels manually. Levels are created automatically. User needs only to use a particular level information with a particular size of text. In proposed algorithm we have considered least significant information (level 1) with largest text size and most significant information (level n) with smallest text size. A generalized form of traditional region incrementing visual cryptography with extra features added as no pixel expansion and improved contrast is proposed in this scheme.

The generalization of the proposed RIVC scheme for generating the levels automatically is described in Algorithm 3.

ALGORITHM 3: A generalized RIVC scheme

1) Scan the image by starting from (0, 0) pixel position and move with the columns.
2) After scanning all the columns of first row, it scans the second row and so on until the first black pixel is encountered
3) After reaching on first black pixel it stores the row number (say m) and moves to the next row.
4) Repeat procedure until scanning reaches a row (say n) in which all the pixels are white.
5) A text is written between these two rows m-1 and n which can be in any level and the text size is m-n. This helps in getting the addresses of two rows between which a text is embedded and we get the size of text.

6) The scanning is done in the same manner and the text size and first row and last row number of each level is stored.

To automate the process of level identification in Visual Cryptography, the basis matrices are modified as shown below:

$$LK_1^0 = \begin{bmatrix} 0 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix}$$

$$LK_2^0 = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$$

$$LK_1^1 = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$$

$$LK_2^1 = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix}$$

Similarly for 3-level automatic scheme, basis matrices are shown below:

$$LK_1^0 = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix}$$

$$LK_2^0 = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \end{bmatrix}$$

$$LK_3^0 = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}$$

$$LK_1^1 = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$$

$$LK_2^1 = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}$$

$$LK_3^1 = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}$$

Automatic Region Incrementing Visual Cryptography, selects the basis matrices according to number of levels in the image automatically. User does not need to give the number of level details manually.

CONCLUSION

Region Incrementing Visual Cryptography (RIVC) introduced different levels of information in a single secret image first time but it has the problem of pixel expansion in which the number of pixels were getting increased and also the contrast of reconstructed image was very poor. Furthermore it was not able to identify the levels of information itself. User needed to give the address of levels manually. Due to these reasons RIVC was not efficient. In this work, the efforts are made to overcome the above shortcomings of the traditional region incrementing visual cryptography. In the proposed modified RIVC, the numbers of pixels in the reconstructed image are same as those in original image. The algorithms have also been modified in such a way that the resultant reconstructed images do have the better contrast information.

REFERENCES

1. Blundo, De Santis A and Stinson D R (1999), “On the contrast in visual cryptography schemes”, *Journal of Cryptology*, Vol. 12, No. 4, pp. 261-289, 1999.

2. Hsu H S, Chen T S and Lin Y H (2004), “The ringed shadow image technology of visual cryptography by applying diverse rotating angles to hide the secret sharing”, In

Networking, Sensing and Control, 2004 IEEE International Conference on, Vol. 2, pp. 996-1001, IEEE.

3. Fu M S and Au O C (2004), "Joint visual cryptography and watermarking", In Multimedia and Expo, ICME'04. IEEE International Conference on, Vol. 2, pp. 975-978., IEEE.

4. Manimurugan S and Porkumaran K (2011), "A new fast and efficient visual cryptography scheme for medical images with forgery detection", *In Emerging Trends in Electrical and Computer Technology (ICETECT)*, 2011 International Conference on, pp. 594-599, IEEE.

5. Monoth T and Babu A P (2010), "Contrast-enhanced visual cryptography schemes based on additional pixel patterns", In Cyberworlds (CW), 2010 International Conference on, pp. 171-178, IEEE.

6. Naor M and Shamir A (1995), *Visual cryptography*, p. 1.

7. Wang R Z (2009), "Region incrementing visual cryptography", *Signal Processing Letters, IEEE*, Vol. 16, No. 8, pp. 659-662.

8. Yan W Q, Jin D, and Kankanhalli M S (2004), "Visual cryptography for print and scan applications", In Circuits and Systems, 2004. ISCAS'04. Proceedings of the 2004 International Symposium on, Vol. 5, pp. V-572. IEEE.

International Journal of Engineering Research and Science & Technology
Hyderabad, INDIA. Ph: +91-09441351700, 09059645577
E-mail: editorijlerst@gmail.com or editor@ijerst.com
Website: www.ijerst.com

ISSN 2319-5991