ENHANCEMENT OF AUTOMATIC REGION INCREMENTING VISUAL CRYPTOGRAPHY

JAYA AGRAWAL

Assistant Professor, Rajasthan Institute of Engineering & Technology, Jaipur, Rajasthan., India, Email: agrawal.jaya09@gmail.com

ABSTRACT

For n level region incrementing visual cryptography scheme, image is divided in n regions. Each region consists of one level information. For implementing VC 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. In similar way, for revealing whole information all the (n+1) shares are superimposed. In proposed scheme, levels are created automatically. User needs only to use a particular level information with a particular size of text and it is modified to generate the levels automatically which is named as automatic region incrementing visual cryptography

Keywords—Secret Sharing, Levels, VC (visual cryptography)

1. INTRODUCTION

Visual cryptography scheme was developed by Naor and Shamir in 1994. In this scheme shares are developed. Shares are transparent images developed by the randomization. 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 blocks 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, 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.

Fig 1: Black pixel and White pixel in visual cryptography with two sub-pixel layout.

To avoid the horizontal or vertical distortion of the reconstructed image, a 4-subpixel layout can be used.

Fig 1: Black pixel and White pixel in visual cryptography with two sub-pixel layout.

Fig 2: Black pixel and White pixel in visual cryptography with four sub-pixel layout.

Fig 3. A 2-out-of-2 VCS with 4-subpixel layout: (a) secret
2. TRADITIONAL RIVC

Matrix \( LK^0 \) where \( j \) is the level number and 0 represents white pixel. In the similar manner \( LK^1 \) represents the basis matrix for encoding a black pixel of the \( j \)-th level. Matrices \( C^0 \) and \( C^1 \) for encoding white and black pixels. These matrices are obtained by the permutation of columns of \( LK^0 \) and \( LK^1 \).

For each pixel of secret image a matrix is obtained by the permutation of columns of \( LK^0 \) and \( LK^1 \). \( C^0 \) is used to encode a white pixel and \( C^1 \) 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 provided the basis matrices for the construction of 2-level RIVC scheme.

\[
LK^1 = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ \end{bmatrix}
\]

\[
LK^2 = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ \end{bmatrix}
\]

\[
LK^3 = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ \end{bmatrix}
\]

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

3. PROPOSED MODEL

In proposed two level and three level RIVC a column is selected randomly from proposed basis matrices for distributing the values to shares for any particular pixel of image to be decoded. By using this concept 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.

In traditional RIVC, the permutation matrix of whole
matrix was used, which gives pixel expansion four which results four times larger reconstructed image. This is the first advantage of proposed RIVC over traditional RIVC.

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

\[
\begin{align*}
LK_1^0 &= \begin{bmatrix} 0 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix} \\
LK_2^0 &= \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} \\
LK_1^1 &= \begin{bmatrix} 1 & 0 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 1 \end{bmatrix} \\
LK_2^1 &= \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}
\end{align*}
\]

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 least 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-

\[
\begin{align*}
LK_1^0 &= \begin{bmatrix} 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix} \\
LK_2^0 &= \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix} \\
LK_1^1 &= \begin{bmatrix} 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix} \\
LK_2^1 &= \begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}
\end{align*}
\]

In proposed two level RIVC, for first level a two out of three matrices for black and white pixels and for second level a three out of three matrices is used. By superimposing any two shares, only first level information will be seen because when two out of three matrices for first level is used. Only when by superimposing all three shares, second level information will be seen as used three out of three matrices for second level. This scheme always provides black color for information pixels and thus removes wang’s drawback. This is the another advantage of proposed RIVC over traditional RIVC with 2 levels.

In proposed three level RIVC, for first level a two out of four matrices for black and white pixels and for second level a three out of four matrices and for third level a four out of four matrices. By superimposing any two shares, only first level information will be seen because two out of four matrices for first level is used. By superimposing any three shares, first level and second level information will be seen because two out of four matrices for second levels is used. Only by superimposing all four shares, all level’s information will be seen.

**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, least significant information (level 1) with largest text size and most significant information (level n) with smallest text size is considered. 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 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.

Above algorithm finds the addresses of each level irrespective to the location of levels. After finding the location of levels, Algorithm 4 is used for generating the shares after Algorithm 3.

Algorithm 4: Share Generation

1. Select a binary secret image in which least significant information (level 1) with largest text size and most significant information (level n) with smallest text size.
2. Automatically find the area of levels using ALGORITHM 3.
3. Generate adequate shares using ALGORITHM 1 or 2 according to the number of levels.

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

\[
\begin{align*}
L_{K1}^{0} &= \begin{bmatrix}
0 & 1 & 1 & 1 \\
0 & 1 & 1 & 1 \\
0 & 1 & 1 & 1 \\
0 & 1 & 1 & 1 \\
\end{bmatrix} \\
L_{K2}^{0} &= \begin{bmatrix}
0 & 1 & 1 & 1 & 0 & 0 \\
1 & 0 & 1 & 1 & 0 & 0 \\
1 & 1 & 0 & 1 & 1 & 0 \\
1 & 1 & 1 & 0 & 0 & 0 \\
\end{bmatrix} \\
L_{K1}^{1} &= \begin{bmatrix}
0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\
0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\
0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\
\end{bmatrix} \\
L_{K2}^{1} &= \begin{bmatrix}
0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\
0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\
0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\
\end{bmatrix} \\
L_{K1}^{1+} &= \begin{bmatrix}
1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\
0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\
0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\
\end{bmatrix}
\end{align*}
\]

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

In this research, a brief introduction of traditional RIVC was given and the major drawbacks (pixel expansion and poor contrast) of traditional RIVC were identified and developed the two algorithms for automatic share generation.

5. CONCLUSION

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.

ACKNOWLEDGEMENT

This research paper is made possible through the help and support from everyone, including: parents, teachers, family, friends, and in essence, all sentient beings. Especially, please allow me to dedicate my acknowledgment of gratitude toward the members of J.N.I.T

REFERENCES


X. A Survey on Visual Cryptography Techniques and their Application, M. Tech Scholar Mahakal Institute of Technology Behind Air Strip, Dewas Road, Ujjain(M.P) - 456664, India