A Presumption Mold of Visual Cryptography Design with Dynamic Groups

Sudhakar Badikala[1], Gowthami Janapatla[2]

Sudhakar Badikala working as an Asst. Professor, Department of Computer Science Engineering at Sindhura College of Engineering and Technology, Affiliated to JNTU, Hyderabad, A.P., India.

Gowthami Janapatla working as an Asst. Professor, Department of Computer Science Engineering at Sindhura College of Engineering and Technology, Affiliated to JNTU, Hyderabad, A.P., India.

***Abstract* - Visual cryptography is a secret sharing scheme where an image is encoded into transparencies. The Secret information can be revealed from the encoded image only when the correct set of images is given as an input and if the input is not matching then the secret information cannot be revealed. We will introduce a scheme which will dynamically add a user to specific group and then based on the information being shared that group related users can retrieve the information. To cut down the overhead of generating and distributing transparencies in user changes, this paper implements a Visual Cryptography scheme. The proposed scheme not provides security to the data but also takes care of discrepancies an extended VC scheme based on basis matrices and a presumption mold is proposed. Apart from the Visual Cryptography scheme we also show the image processing i.e. sending the information for communication along with the image in fact text being written on the image.**

Index Terms— Secret Sharing, Image processing, Visual Cryptography (VC), Presumption Mold.

I. Introduction

Visual Cryptography is one of the Cryptographic techniques where the actual data is embedded in one image and then that image file is encoded. The file that comes as an output is combination of black and white spots which a normal user cannot understand. There are many other ways for providing the security to the data like very famous algorithms which will be used are AES, DES, MD5, Plain cipher encryption and there is one more way with which the security can be provided to the data which is Stegnography. In this technique the data is hidden in any of the files like audio or video or text.

Coming with Visual Cryptography, the user can decrypt the message only when the user is genuine or the one who has got the correct piece of the encoded image. In this project implementation we are encoding the image into n pieces and that group consists of t users, say suppose if the users become t-1 then that data cannot be taken for further more processing because the rule will be violated and can cause damage to that organization. In order to have a correct flow of data the admin need to take care about it. In the VC scheme, a secret image is encoded into transparencies, and data of each piece is noise-like so that the secret information cannot be retrieved from any one transparency via human visual observation or signal analysis techniques. In general, a -threshold VC scheme has the following properties: The stacking of any out of those visual cryptography generated shares can reveal the secret by visual insight, but the combination of fewer number of transparencies cannot retrieve any information other than the size of the secret image. Naor and Shamir proposed a – threshold VC scheme based on basis matrices, and the model had been further studied and extended. The related works include the VC schemes based on presumption models, general access structures, VC over halftone images, VC for color images, cheating in VC, the general formula of VC schemes, and region incrementing VC.

Contrast is one of the important performance metrics for VC schemes. Generally, the stacking revelation of the secret with higher contrast represents the better visual, and hence the stacking secret with high contrast is the goal of pursuit in VC designs. Naor and Shamir define a contrast formula which has been widely used in many implementations. According to the definition of contrast, there are studies attempting to achieve the contrast bound of VC scheme. Moreover, there exist VC related researches using many other approaches. Another important metric is the pixel expansion denoting the number of sub pixels in transparency used to break secret content. The reduction of pixel amplifications has been investigated in previous studies. The presumption model of the VC scheme is based on the basis matrix, and only one column of the matrix is chosen to encode a binary secret pixel, rather than the traditional VC scheme utilizing the whole basis matrices. The size of the generated transparencies is identical to the secret image. Yang also proposed a presumption mold of VC scheme and the two cases and is explicitly constructed to achieve the optimum contrast. Based on this, Yang, Cimato *et al.* has proposed a generalized VC scheme in which the pixel expansion is between the presumption model of VC scheme and the traditional VC scheme.

Encrypting an image by random grids (RGs) was first introduced by Kafri and Keren in 1987. A binary secret image is encoded into two noise-like transparencies with the same size of the original image, and loading of the two secret shares

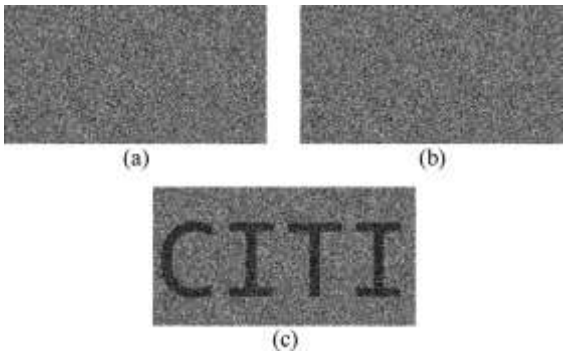
reveals the content of the secret image. On comparing RGs with basis matrix, the major advantage is that the size of generated transparencies is unexpanded. The RG scheme is similar to the presumption mold of the VC scheme, but the RG scheme is not based on the base matrix. The recent studies include RG for color image, RG, and RG schemes.

We consider the scenario of a dynamic user group, where new participants are to join the user group with original participants; and the transparencies need to accommodate the new users. If the transparencies are to be generated with the traditional VC scheme, the original transparencies need to be discarded, and the new transparencies need to be generated with the traditional VC scheme. The regeneration and redistribution of the whole transparencies consume computing and communication resources and may lead to the potential security vulnerability.

Here dynamic group means that people are randomly leaving and adding into the group and if we perform a secret image among a dynamic group then there should be n number of transparencies are required and if any people are added or any people leave that group then again we need to generate new shares for them and if we go for old approach then we are not able to get original image which is secret information so that is the reason why we are going to implement this technique to avoid the regeneration of transparencies and no need to worry about the regeneration of the secret information.

In this paper, we propose a presumption mold of VC scheme for secretly sharing the data. The major contribution is that the proposed scheme accommodates dynamic changes of users in the group sharing a VC secret. The proposed scheme allows changes of users without regeneration and redistribution of VC transparencies, which reduce the computing and communication resources in accommodating user changes. The scheme is capable of generating an arbitrary number of transparencies and the explicit algorithms are proposed to generate the transparencies. For a group with initial users, the proposed algorithm explicitly generates the required transparencies. For newly joining participants, the new transparencies can be explicitly generated without the need to update the original transparencies. The secondary contribution is that this paper designs an implementation of VC based on the presumption mold, and the proposed scheme allows the unlimited number of users. For the conventional VC scheme to implement the case, the mathematical manipulations of infinite size of basis matrices and variables are often required, which is computationally prohibitive. Our approach designs an implementation scheme which is capable of producing a finite subset of the complete infinite transparencies through the proposed Algorithms 1 and 2, with computationally feasible operations. We also derive an optimization problem to solve the maximal contrast of the proposed VC scheme.

Fig 1. Binary Image



II. Proposed Approach Basis Matrix

Basis Matrix:

The basis matrices of VC scheme were first introduced by Naor and Shamir. In this paper, a white-and-black secret image or pixel is also described as a binary image. In the base matrix, to encode a binary secret image, each secret pixel white black will be turned into blocks at the corresponding position of transparencies, respectively. Each block consists of sub-pixels and each part of it is opaque. In the complete paper, we used 0 to indicate a transparent sub-pixel and 1 to indicate an opaque type sub-pixel and if any two sub-pixels are merged on matching positions, the representation of a merged pixel may be visible, when two corresponding pixels are transparent. Else ways, the merged pixel is opaque. Let's denote the manipulation, defined as

$0 \oplus 0 = 0; \quad 0 \oplus 1 = 1; \quad 1 \oplus 0 = 1; \quad 1 \oplus 1 = 1$

Actually, $\oplus$ can be treated as the bitwise operation "OR", and it is to be noted that we use the notation $T_i \oplus T_j$ to indicate the merging of the two transparencies T_i and T_j , since and can be treated as two Boolean matrices.

For the basis matrices, two collections of Boolean n by m matrices C_0 and C_1 are constructed to encode the binary pixel , respectively. Each row of the matrix in C_0 and C_1 corresponds to an encoded block, and the elements represent the sub pixels. Before describing the definitions of C_0 and C_1, we first explain how to encode *s*. *s* For being white, the dealer

randomly chooses a matrix from with uniform distribution and then sends all the rows to each, respectively. Being black, the dealer at random chooses a matrix from C_0 with uniform distribution and then sends all the rows to each T_i, respectively.

For *s* being black, the dealer randomly chooses a matrix from C_1 with uniform distribution and then sends all the rows to each, respectively. The C_0 and are required to meet the conditions described in

Definition1. Let denote H(υ) the hamming weight of (0-1) a υ–vector (i.e., the number of ones in υ).

Definition 1: A (t, n) VC scheme with m sub pixels and contrast α>0 can be represented as two collections of n × m Boolean matrices C_0 and C_1. Let be a constant integer. A valid VC scheme is required to meet the following conditions:

1) For any matrix in C_0, the stacked υ of any out of the *n* rows in the matrix satisfies .

2) For any matrix in , the stacked υ of any t out of the *n* rows in the matrix satisfies .

3) For any *k* -element subset $\{i_1,i_2,\ldots\ldots i_n\}$ subset $\{1,2,\ldots.n\}$ and , $k<t$ the two collections of k × m matrices obtained by restricting each matrix in C_0 and C_1 , to rows $i_1,i_{2,\ldots\ldots},i_k$ are indistinguishable in the sense that they contain the same matrices with the same frequencies.

The first and the second conditions represent the contrast requirements. In general, with larger α, the stacking result is more visually differentiable. Third condition presents the security requirement. A valid VC must be able to prevent the secret pixels from being revealed by analyzing the patterns or probability distributions from *k* transparencies for $k<t$.

If we find n × m an Boolean matrix B_0 € C_0 and an n × m Boolean matrix B_1 € C_1 , we can construct C_0 and C_1 by permuting all columns of B_0 and B_1, expressed as

C_0= {All the matrices obtained by permuting all columns of B_0}

C_1= {All the matrices obtained by permuting all columns of B_1}

If two n × m Boolean matrices B_i and B_i` can be adjusted to become the same matrix with reordering columns, and are equivalent in terms of generating .Therefore, the orders of columns of and are technically insignificant.

$$m^n = \sum_{j=0}^{n} \binom{n}{j} hj, i$$

Example 1: An example of a (3, 4) VC scheme is,

$$B_0= \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & o & 1 & 1 & 1 & o \end{pmatrix}$$

$$\text{And } B_1= \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & o & 1 & O & 1 & 1 \\ o & 0 & 1 & 1 & 0 & 1 \\ 0 & O & 1 & 1 & 1 & 0 \end{pmatrix}$$

The $A_{j,n}$ are

$$A_{0,4} = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} \quad A_{1,4=} \begin{pmatrix} 0 & 1 & 1 & l \\ 1 & 0 & 1 & l \\ 1 & 1 & 0 & 1 \\ l & 1 & l & 0 \end{pmatrix}$$

$$A_{2,4=} \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & l & 0 & 1 & o & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 \end{pmatrix}$$

$$A_{3,4} - \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & o \\ o & 0 & 1 & 0 \\ o & 0 & 0 & l \end{pmatrix} \quad A_{4,4} - \begin{pmatrix} o \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

Thus, B_0 is represented as H_0=(0,1,0,0,2), and B_1 is shown as H_1=(2,0,o,l,0)

III. Presumption Mold

For a given value of t, the transparencies can be continuously generated with the (t, ∞) Opt Pr VC scheme. However, practical applications require the algorithm to terminate within limited number of steps and to meet the requirement; we have to specify the number of transparencies in the algorithm. The algorithm requires (x, y), obtained by solving from Table I. The outcomes of Algorithm 1 are seen and an index table, where is the index of the used memory less sequence to encode the secret pixel.

In the first round, we use Algorithm 1 to generate n` transparencies and Z. If we need not to generate more transparencies in the future, Z is not required and discarded. Otherwise, Z has to be stored safely, and therefore we can generate more transparencies $T_1, T_2, \ldots, T_n$ by utilizing Z.

The result of the algorithm 1 you can see in fig(i) and a)T_1 b) T_2 c)$T_1 \oplus T_2$

Algorithm 1.The algorithm of(t,∞) optPrVC scheme

Input :A binary secret image S,two positive integers t,n',

and two vectors(X,Y).

Output: n' transparencies $T1, T2, \ldots, Tn'$; an index table Z.

1 for each pixel $s[w,h]$ in S do

2 if $s[w,h]$=white then

3 Generate an integer $z \in \{t-2k \mid k = 0,1, \ldots\ldots, t/2\}$

and $P(z = t-2k) = y_{t-2k}$.

4 else

5 Generate an integer $z \in \{t-1-2k \mid k = 0,1, \ldots,$

$(t-1)/2$ And $P(z = t-1-2k) = -y_{t-1-2k}$.

6 end if

7-$Z[w,h] = z$

8 for k=1 to n' do

9 Assign randomly $T_k[w,h]$ to 0 or 1 where $P[T_k[w,h] = 0] = x_z$

10 end for

11 end for

Algorithm 2: The Algorithm of (t,∞) ptPrVC scheme by the index table *Z*

Input : An index table Z, a positive integer n'', and a vector X.

Output : n`` transparencies $T'_1, T'_2, \ldots\ldots\ldots, T'_{n''}$

For each z[*w*,*h*] in Z do

For k=1 to n'' do

Assign randomly $T'_k[w,h]$ *to 0 or 1* where $P(T'_k[w,h] = 0) = x_z$.

End for

End for each

IV. Conclusion

We have proposed a Visual Cryptography scheme with Dynamic group considerations where secret information can be shared among the users of a specific group in a precise manner. Our System provides security to data in more effective manner say like when there are three users in a group and even if a single user is not present in the group at the time of decrypting the code then the information cannot be revealed from the current source and thereby providing good security to data from going it to the non genuine users. Finally in this proposed model we are providing a solution for the existing one about the dynamic group if a user leave that group or if the user is added in to the group it is not possible to regenerate the secret information by the proposed approach we overcome this problem by simply generating the transparencies to the new users and removed user's transparencies based up on the Basis Matrix.

References

M.Naor and A. Shamir, "Visual cryptography," in *Proc. Advances in Cryptography (EUROCRYPT'94)*, 1995, vol. 950, LNCS, pp. 1–12.

R. Ito, H. Kuwakado, and H. Tanaka, "Image size invariant visual cryptography," *IEICE Trans. Fundam. Electron., Commun., Comput. Sci.*,vol. 82, pp. 2172–2177, Oct. 1999.

C. N. Yang, "New visual secret sharing schemes using presumption method," *Pattern Recognit. Lett.*, vol. 25, pp. 481–494, Mar. 2004.

S. J. Lin, S. K. Chen, and J. C. Lin, "Flip visual cryptography (FVC) with perfect security, conditionally-optimal contrast, and no expansion,"*J. Vis. Commun. Image Represent.*, vol. 21, pp. 900–916, Nov.2010.

G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, "Visual cryptography for general access structures," *Inf. Computat.*, vol. 129, no. 2, pp. 86–106, Sep. 1996.

F. Liu, C. Wu, and X. Lin, "Step onstruction of visual cryptography schemes," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 1, pp. 27–38, Mar. 2010.

Z. Zhou, G. R. Arce, and G. Di Crescenzo, "Halftone visual cryptography," *IEEE Trans. Image Process.*, vol. 15, no. 8, pp. 2441–2453, Aug. 2006.

Authors Profile

Sudhakar Badikala working as an Asst. Professor at Sindhura College of Engineering and Technology, Affiliated to JNTU-Hyderabad, A.P., India.

Gowthami Janapatla working as an Asst. Professor at Sindhura College of Engineering and Technology, Affiliated to JNTU-Hyderabad, A.P., India.