International Journal of Advanced Research in
Computer Science Engineering and Information Technology
Volume: 3 Issue: 1 26-Jun-2014,ISSN_NO: 2321-3337

Visual Cryptography Schemes with Perfect Reconstruction of Black Pixels

S. Anu[1]

IT Student, Department of Information Technology, Sri Krishna Engineering College, India[1].

ABSTRACT—*Conventional visual cryptography (VC) suffers from a pixel-expansion problem, or an uncontrollable display quality problem for recovered images, and lacks a general approach to construct visual secret sharing schemes (VSSs) for general access structures (GASs). We propose here in a general and systematic approach to address these issues without sophisticated codebook design. The approach can be used for binary secret images in non-computer-aided decryption environments. To avoid pixel expansion, we design a set of column vectors to encrypt secret pixels rather than use the conventional VC-based approach. We begin by formulating a mathematic model for the VC construction problem to find the column vectors for the optimal VC construction, after which we develop a simulated-annealing-based algorithm to solve the problem. It indicates that the display quality of the recovered image is superior to that of previous studies.*

1. INTRODUCTION

Visual cryptography (VC), allows the encryption of secret information in image. The existing VC schemes (VCSs) can be divided into two categories: threshold access structure (also known as k-out-of-n VCSs or (k,n)-VCSs) and general access structure (GAS).The GAS concept and also developed a VC-based solution for some GASs. Using the GAS enables dealers to define reasonable combinations of shares as decryption conditions rather than to specify the number of shares. The pixel-expansion problem is a major drawback with most VCSs that use the VC-based approach. The pixel-expansion problem affects the practicability of a VC scheme because it increases the storage and/or transmission costs. Moreover, the pixel-expansion problem usually introduces the side effect that the recovered secret images have less contrast. The contrast of the recovered images decreases in proportion to m, whereas the shares are expanded by a factor of m times. As a result, the decrease in contrast limits the application of these VC schemes are expanded by a factor of m times. As a result, the decrease in contrast limits the application of these VC schemes. The display quality of a recovered image is affected not only by its contrast value but also by its blackness. The degree of blackness represents the probability that black secret pixels will be accurately recovered. An image that has higher contrast should have better display quality when the blackness is fixed. However, a greater blackness value (e.g., 100%) may decrease the contrast value of the recovered image. In this paper, we take blackness as one of the design factors to improve the display quality of recovered images. In decreasing contrast of recovered images in some access structures the existing VCS construction algorithms for GASs cannot simultaneously avoid the pixel-expansion problem and guarantee an acceptable blackness. These issues motivated us to develop a systematic approach to the construction of size invariant VCSs (SIVCSs or VCSs in short) for GASs subject to the adjustable display quality of recovered images. In decreasing contrast of recovered images in some access structures the existing VCS construction algorithms for GASs cannot simultaneously avoid the pixel-expansion problem and guarantee an acceptable blackness. These to develop a systematic approach to the construction of size invariant VCSs (SIVCSs or VCSs in short) for GASs subject to the adjustable display quality of recovered images. The proposed approach for SIVCSs is applicable to binary secret images and no computational devices are needed during the decryption phase. A mathematical optimization model for the problem of the SIVCS for GASs where the objectives are to maximize the worst and average contrast of recovered images simultaneously under a blackness constraint. By adjust the blackness depending on the characteristics of the secret images to obtain the best display quality for the recovered images. Then, we develop a simulated-annealing-based algorithm to solve the combinatorial optimization problem. Finally, the other approaches and present implementation results to evaluate the effectiveness of the proposed algorithm.

2. PROBLEM STATEMENT

The proposed approach for SIVCS is applicable to binary secret images to increase the display quality of stacked image. The approach can be used for binary secret images in non-computer-aided decryption environments. To avoid pixel expansion, we design a set of column vectors to encrypt secret pixels rather than use the conventional VC-based approach. Using this model, dealers can adjust the blackness depending on the characteristics of the secret images to obtain the best display quality for the recovered images. We begin by formulating a mathematic model for the VC construction problem to find the column vectors for the optimal VC construction, after which we develop a simulated-annealing-based algorithm to solve the problem.

3. BACKGROUND AND RELATED WORK

3.1Background of General Access Structures

Suppose P= {1, , ,n} is a set of n participants, and 2 denotes the power set of . The quantity denotes the set of subsets of from which we wish to share the secret; thus, 2. Each set in is said to be a qualified set, and each set not in is called a forbidden set. Obviously, 2 and. Based on these definitions, a VCS for an access structure on can yield n shares. When we stack together the shares associated with the participants in any set, and then recover the secret image, but any has no information on the stacked image. The quantity consists of all

the minimal qualified sets: $\Gamma_0 = \{A \in \Gamma_{\mathrm{Qual}} \colon A' \notin \Gamma_{\mathrm{Qual}}\ \forall A' \subset A\}$. In traditional secret sharing schemes, increases monotonically and decreases monotonically, the access structure is said to be strong, and is called a basis. In a strong access structure,
$\Gamma_{\mathrm{Qual}} = \{C \subseteq \mathcal{P} \colon B \subseteq C \text{ for some } B \in \Gamma_0\}$, And we say that is the closure of. If, then the access structure is said to be weak. The 3 participants share a secret image (i.e., *, 2, +) and {* ,2+,* , +}, in the strong access structure $(\Gamma_{\mathrm{Qual}}, \Gamma_{\mathrm{Forb}})$VCS, stacking any set of subsets * ,2+, * , +, or * ,2, + can reveal the secret image; otherwise, no information can be displayed. However, in the weak access structure VCS, only stacking sets can reveal the secret image; the image is not guaranteed to be revealed with set {1,2,3}.

4. THE PROPOSED MODEL

The main idea behind the proposed SIVCS is the probabilistic visual cryptography (ProbVC) which was first proposed. Constructed the (k,n)-VCS by using two collections of column vectors, and , which are transformed from basis matrices of the conventional (k,n)-VCS. Suppose the basis matrix contains n m entries, ( ) will contain m n column vectors. To share a black (white) pixel, one of the column vectors in c1 (c0) is randomly chosen and then distributes -th entry in the column vector to -th share. (2,3)-ProbVC scheme is constructed by the following collections of column vectors

$$C_0 = \left\{ \begin{bmatrix}1\\1\\1\end{bmatrix}, \begin{bmatrix}0\\0\\0\end{bmatrix}, \begin{bmatrix}0\\0\\0\end{bmatrix} \right\} \text{ and } C_1 = \left\{ \begin{bmatrix}1\\0\\0\end{bmatrix}, \begin{bmatrix}0\\1\\0\end{bmatrix}, \begin{bmatrix}0\\0\\1\end{bmatrix} \right\}.$$

C1 and c0 are transformed from two basis matrices of the conventional (2,3)-VCS. For encrypting a black secret pixel and suppose the chosen column vector is $[0 \quad 1 \quad 0]^T$the pixels 0, 1, and 0 are distributed to shares 1, 2, and 3, respectively. In this fashion, each secret pixel within a secret image is encrypted in only one pixel in each constituent share. Thus, image size of shared and stacked images is same as the secret image. The approach of Ito et al. has to rely on existing basis matrices of the conventional VCSs. The ProbVC is as secure as the conventional VCSs. Develop a general construction methodology for SIVCSs for GASs

5. FEASIBILE SOLUTION

The solution is considered feasible if the following conditions are satisfied:

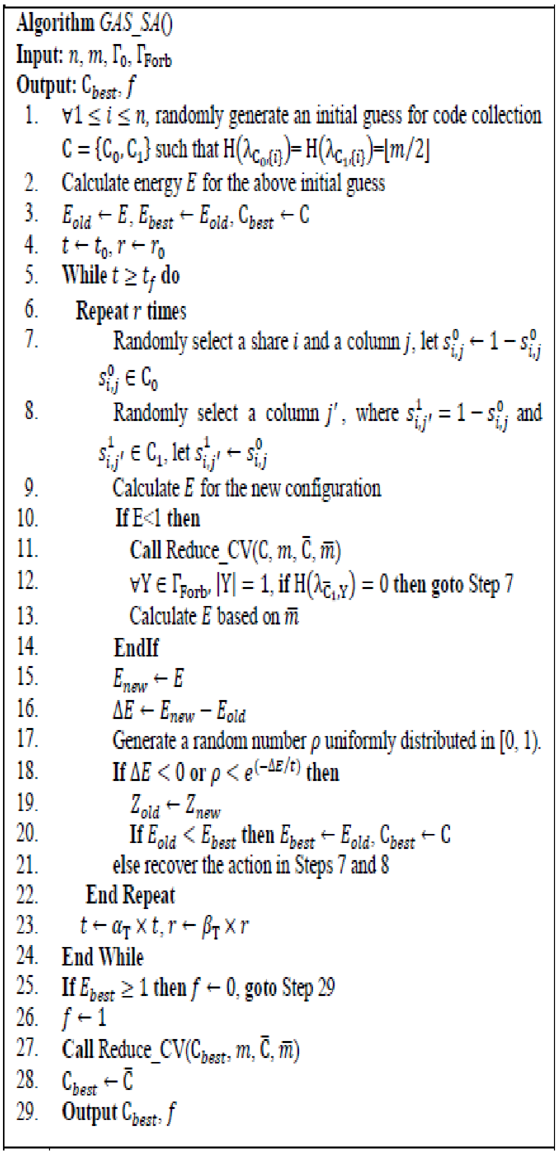
1. For any $Y \in \Gamma_{\mathrm{Forb}}$, $V_{C_1,Y} = V_{C_0,Y}$.
2. For any $X \in \Gamma_{\mathrm{Qual}}$, $H(\lambda_{C_1,X}) - H(\lambda_{C_0,X}) > \alpha_{\mathrm{TH}}$.

The security condition on restricting secret accessibility of any forbidden set. For any forbidden set Y, $\{i_1, i_2, \dots, i_q\}$ is all members of Y and $V_{C_0,Y}$ $(V_{C_1,Y})$ denotes the collection of column vectors that are obtained by restricting each n-tuple vectors in ( ) to rows c1(c0) to row $i_1, i_2, \dots, i_q$. Then $V_{C_0,Y}$ and $V_{C_1,Y}$ have to contain the same collections of q-tuple vectors with the same chosen probabilities. The black and white secret pixels are therefore indistinguishable by human‘s visual system. The property is equivalent to the security condition presented for conventional VCSs. Hence, valid as a security condition of ProbVCSs. It ensures that the blackness of recovered black secret pixels is higher than that of recovered white secret pixels in a qualified recovery image.

If $H(\lambda_{C_1,Y}) - H(\lambda_{C_0,Y}) > \alpha_{TH},$ a human‘s visual system can recognize a difference between the recovered secret pixels. If is large enough, a human‘s visual system can distinguish between the recovered black and white secret pixels to obtain the secret images. Using these definitions, a SIVC scheme for access structure can be constructed as follows: let two collections of sets and be adopted for the SIVCS. In the encryption phase, the dealer randomly chooses one column vector from c1(c0) to encrypt white (black) secret pixels. The above-mentioned method, which is also called the single pixel encoding method, encrypts a secret image pixel by pixel. This method is easy and low in complexity, but it cannot guarantee that the pixel can be uniformly distributed in a small area in the reconstructed image. It may decrease the quality of reconstructed images..Proposed a multi-pixel block size invariant VCS that maintain the relative pixel density in a small area in the reconstructed image to improve the quality of the image. The proposed scheme is built from existing basis matrices of the conventional VCS. However scheme, the encryption process is performed by taking a multi-pixel block as a unit of encryption. They suggest that to use the pixel expansion factor, m, in the conventional VCS as the block size of encryption. It is worked on the multi-pixel encoding method to improve the quality of the reconstructed image. Their method is similar to it collected the pixel block in the secret image by a zigzag scan method in each encoding run. We focus on how to find code collection sets, and , for SIVCSs upon a given access structure. Hence, we use the single pixel encoding method to generate shares.

6. SA-BASED ALGORITHM

The SA-based algorithm is developed for solving model IP2. The proposed approach treats decision variable m as a given variable and tries to find the best solution with a given access structure c1 (c0) based on m. Step 1 randomly guesses an initial value for and subject to the security constraint on each share. Step 2 calculates energy value for the first solution. Given that the optimization problem in IP2 is a minimization problem, the energy function in the SA-based algorithm is directly defined as c1 (c0). Steps 3 and 4 initialize related parameters for the SA procedure. Steps 5–24 are the main SA loop, which will be terminated when the frozen temperature, tf, is reached. Steps 6–22 are executed r times to refine solutions in a state of equilibrium. Steps 7 and 8 randomly explore a next solution by altering the current solution state of its neighbourhood. The step size in Step 7 is very small; the algorithm selects column vector j in, and then alters the encoding of share. The altered encoding is denoted by si,j . Step 7 indicates that share violates the security condition, which is corrected in Step 8. Step 8 selects a column vector in in which the encoding of share i,j , differs from si,j and then alter si,j . In such a way, the encoding of share can be altered and the security condition of share can be preserved. Steps 10–14 deal with Constraint (7) in model IP2 only while the current solution receives no penalty (i.e., <). Step 11 reduces the current code collection and then Step 12 checks whether or not the code collection meets Constraint (7). If the constraint can be satisfied, the energy of the feasible solution is re-evaluated based on the actual quantity of vectors in the solution (i.e., $\bar{m}$) in Step 13; if the constraint cannot be satisfied, then it aborts the solution. Steps 15–21 evaluate the value of the energy function for the new state and decide whether or not the current state will be replaced by the new state. The objective value with the minimum energy value should be saved as the best solution in Step 20. After r solution iterations, parameters t and r are modified in Step 23.



```
Algorithm GAS_SA()
Input: $n, m, \Gamma_0, \Gamma_{\mathrm{Forb}}$
Output: $C_{best}, f$
1.  $\forall 1 \le i \le n$, randomly generate an initial guess for code collection
    $C = \{C_0, C_1\}$ such that $H(\lambda_{C_0\{i\}}) = H(\lambda_{C_1\{i\}}) = \lfloor m/2 \rfloor$
2.  Calculate energy $E$ for the above initial guess
3.  $E_{old} \leftarrow E$, $E_{best} \leftarrow E_{old}$, $C_{best} \leftarrow C$
4.  $t \leftarrow t_0$, $r \leftarrow r_0$
5.  While $t \ge t_f$ do
6.    Repeat $r$ times
7.        Randomly select a share $i$ and a column $j$, let $s_{i,j}^0 \leftarrow 1 - s_{i,j}^0$
        $s_{i,j}^0 \in C_0$
8.        Randomly select a column $j'$, where $s_{i,j'}^1 = 1 - s_{i,j}^0$ and
        $s_{i,j'}^1 \in C_1$, let $s_{i,j'}^1 \leftarrow s_{i,j}^0$
9.        Calculate $E$ for the new configuration
10.       If E<1 then
11.         Call Reduce_CV($C, m, \bar{C}, \bar{m}$)
12.         $\forall Y \in \Gamma_{\mathrm{Forb}}, |Y| = 1$, if $H(\lambda_{\bar{C}_1,Y}) = 0$ then goto Step 7
13.         Calculate $E$ based on $\bar{m}$
14.       EndIf
15.       $E_{new} \leftarrow E$
16.       $\Delta E \leftarrow E_{new} - E_{old}$
17.       Generate a random number $\rho$ uniformly distributed in [0, 1).
18.       If $\Delta E < 0$ or $\rho < e^{(-\Delta E/t)}$ then
19.         $Z_{old} \leftarrow Z_{new}$
20.         If $E_{old} < E_{best}$ then $E_{best} \leftarrow E_{old}$, $C_{best} \leftarrow C$
21.       else recover the action in Steps 7 and 8
22.     End Repeat
23.    $t \leftarrow \alpha_T \times t$, $r \leftarrow \beta_T \times r$
24. End While
25. If $E_{best} \ge 1$ then $f \leftarrow 0$, goto Step 29
26. $f \leftarrow 1$
27. Call Reduce_CV($C_{best}, m, \bar{C}, \bar{m}$)
28. $C_{best} \leftarrow \bar{C}$
29. Output $C_{best}, f$
```

Table-I SA-based algorithm for access structure

7. DEMONSTRATION

The contrast value of Fig. 5(d) is lower than that of the others; the display quality of Fig. 5(d) is superior to that of Fig. 5(b) and (c) because all of the black secret pixels can be recovered. Because a cipher-text can be made in smaller (or thin) fonts the secret image can have higher capacity in a given area or a dealer can write the cipher-text in a smaller area. The above example proves the effectiveness of the blackness constraint in the proposed optimization model. These results also indicate that the blackness can be more important than contrast in the visual quality of a VC scheme.

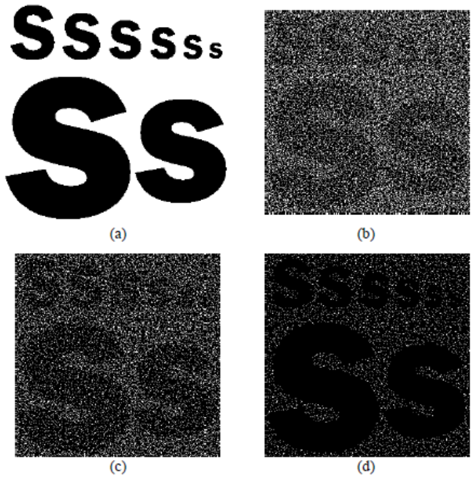


Fig. 7. A part of implementation results for access structure 10, (a) the secret image (320x320 pixels, 192DPI), (b) the recovered image for set {2,3,5} (Model A, contrast =1/10, blackness =4/5), (c) the recovered image for set {2,3,5} (Model B, =1/10, =9/10), (d) the recovered image for set {1,3,4,5} (Model C, =1/12, =1)

8. CONCLUSION AND FUTUREWORK

A weak visual cryptography scheme for GASs using the optimization technique. The proposed model for SIVCSs eliminates the disadvantages of the pixel-expansion problem from which conventional VC scenarios suffer. Our method guarantees the blackness of black secret pixels for VCSs and improves the display quality of the worst-case image. Our approach performs better than those previously proposed in terms of the display quality of the recovered image, which includes the controllable blackness for black secret pixels and maintenance of the same aspect ratio as that of the original secret image. The major contributions of this work include the following three: First, this is the first solution for weak SIVCS for GASs subject to controllable blackness of black secret pixels. Second, we formulate the construction problem of the SIVCS for GASs as a mathematical optimization problem such that the problem can be solved by using optimization techniques. Third, the proposed method is a general and systematic approach that can be applied to any VC schemes without individually redesigning codebooks or basis matrices.

REFERENCE

[1] M. Naor and A. Shamir, ―Visual Cryptography,‖ *Advances in Cryptology: Eurprocrypt'94*, vol. 950, pp. 1–12, 1995.

[2] J. Weir and W. Yan, ―A Comprehensive Study of Visual Cryptography,‖ *Transactions on Data Hiding and Multimedia Security V , LNCS*, vol. 6010, pp. 70—105, 2010.

[3] C. N. Yang, ―New Visual Secret Sharing Schemes using Probabilistic Method,‖ *Pattern Recognition Letters*, vol. 25, no. 4, pp. 481–494, 2004.

[4] R. Ito, H. Kuwakado, and H. Tanaka, ―Image Size Invariant Visual Cryptography,‖ *IEICE Transactions on Fundamentals*, vol. E82-A, no. 10, pp. 2172–2177, 1999.

[5] P. L. Chiu and K. H. Lee, ―A Simulated Annealing Algorithm for General Threshold Visual Cryptography Schemes,‖ *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, 2011.

[6] G. Ateniese, C. Blundo, A. D. Santis *et al.*, ―Visual Cryptography for General Access Structures,‖ *Information and Computation*, vol. 129, no. 2, pp. 86–106, 1996.

[7] C. S. Hsu and Y. C. Hou, ―Goal-Programming-Assisted Visual Cryptography Method with Unexpanded Shadow Images for General Access Structures,‖ *Optical Engineering*, vol. 45, no. 9, pp. 097001-1 (10 pages), 2006.

[8] C. S. Hsu, S. F. Tu, and Y. C. Hou, ―An Optimization Model for Visual Cryptography Schemes with Unexpanded Shares,‖ *Foundations of Intelligent Systems, LNAI*, vol. 4203, pp. 58–67, 2006.

BIOGRAPHY

Ms. S.Anu, B.Tech., IT Student and she pursued B.Tech in Department of Information Technology at Sri Krishna Engineering College. She has presented her paper in 2 National level Conferences at various Engineering College.