IMPROVE DISPLAY QUALITY OF SYMMETRIC IMAGE SIZE FOR COMMON ADMISSION STRUCTURES IN VISUAL CRYPTOGRAPHY

[1]S.DEVASENA, [2]S.SUDHA

[1]Cse Department Student (M.E) Sree Sowdambika College of Engineering, Aruppukottai
[2]Cse Department Assistant Professor Sree Sowdambika College of Engineering
Aruppukottai, Email: devasenasuvetha29@gmail.com, sudhajiin@yahoo.co.in

Abstract- In visual cryptography (vc) suffers from a pixel-expansion problem, or an out of control display quality problem for improved images(ii), and lacks a general approach to construct visual secret sharing schemes (vsss) for common admission structures (cass). The propose herein a general and efficient approach to address these issues without difficult blueprint. The efficient approach can be used for binary secret images in non-computer-supported decipher environments. To avoid pixel expansion, design a set of column vectors to encode secret pixels rather than use the vc-based approach. The beginning process is preparing a mathematic model for the vc construction problem to find the column vectors for the best vc construction, after which develop a simulated-annealing-based (sa) algorithm to solve the problem. The display quality of the improved image (ii) is advanced than the previous systems.

Keywords—Visual secret sharing scheme, Pixel expansion, Common admission structures, Controllable display quality

I. INTRODUCTION

VISUAL cryptography (VC), which was proposed by Naor and Shamir,image form all the encryption process are performed. visual secret sharing schemes (VSSs) are used. Two categories of VCSs threshold admission structure(k,n) admission structure is n shares are reveal the information in k shares, common admission structure For example, if there are 4 participants (one president, one vice president, and two managers) sharing a secret, the president may expect to decrypt the secret with any single partner who holds one of the other shares, whereas the vice president is allowed to obtain the secret only with two managers. The two managers are controlled from accessing the secret. Given these flexibilities, we also can set the number of shares as the decrypting condition. Clearly, $(n,)$-and $(k,)$-VCSs are special cases of the CAS. In visual cryptography pixel expansion problem is a major drawback. Problem will increase the storage area and cost and also decrease the contrast in recovered secret image. Decreasing the contrast level is limits the application of VC schemes. Existing system drawbacks are low quality constrains. Quality of the improved image is also affected by blackness. An image that has higher contrast should have better display quality when the blackness is fixed. Contrast and blackness are directly propositional .If the contrast is high the display quality also high. VC construction problem have formulated the threshold VCS for maximizing contrast or minimizing pixel expansion as a linear programming problem. Koga proposed a general formula to both maximize the contrast and minimize the pixel expansion. Lee and Chiu (hereinafter Lee) proposed a generic VC construction method for CAS. Their approach can perfectly recover black secret pixels but the decrease the contrast of improved image in some admission structure. The existing VCS construction algorithms for GASs cannot simultaneously avoid the pixel-expansion problem and guarantee an acceptable blackness These issues forced us to develop a methodical approach to the construction of size symmetric VCSs (SSVCSs or VCSs in short) for CASs subject to the adjustable display quality of improved images. The proposed approach for SSVCSs is applicable to binary secret images and no use of sophisticated code book for the decryption. Using this model, dealers can correct the blackness depending on the personality of the secret images to obtain the best display quality for the improved images. We develop a simulated-annealing-based algorithm to solve the combinatorial optimization problem. Finally, we compare our results with other approaches and present implementation results to evaluate the effectiveness of the proposed algorithm.

II. BACKGROUND AND RELATED WORK

A) Background of common admission Structures

P={1,2,...n} set of n participants. 2^p denotes the power set of p. The quantity Γ_{qual} denotes the set of subsets of from which we wish to share the secret there $\Gamma_{qual} \in 2^p$. Γ_{qual} is a qualified set. A set not in the Γ_{qual} that is forbidden set. $\Gamma_{qual} \cup \Gamma_{forb} = 2^p$ *and* $\Gamma_{qual} \cap \Gamma_{forb} = \emptyset$. In VCS for an admission structures $(\Gamma_{qual}, \Gamma_{forb})$on p can yield n shares. X is a set of Participants. $X \in \Gamma_{qual}$ can recover the secret image but $X \in \Gamma_{forb}$ cann't recover the secret image. Γ_0 is a

minimal qualified set. $\Gamma_0=\{A \subset \Gamma_{qual} : A' \subset \Gamma_{qual} \forall A' \subset A\}$ Traditional secret shareing schemes, Γ_{qual} increases monotonically and Γ_{forb} decrease monotonically, (Γ_{qual} , Γ_{forb}) admission structure is very strong. Strong admission structure, $\Gamma_{qual} = \{C \subseteq P : B \subseteq C \text{ for some } B \subseteq \Gamma_0\}$ If $\Gamma_{qual} = \Gamma_0$, then the admission structure is very weak. For example,3 participants can share the secret information. Sharing participants p={1,2,3}. $\Gamma_0 = \{(1,2),(1,3)\}$ Qualified set can reveal the secret information. $\Gamma_{forb} = \{(2,3),(1,2,3)\}$ is a forbidden set is not reveal the secret information.

B)Related Works

B.1 Ateniese's Approach

Ateniese first proposed a VC-based approach for VCSs for CASs. They mapped a VCS admission structure to a graph .Form the graph found both the lower and upper bounds on the size of the shares (i.e., the pixel-expansion factor). They gave minimum pixel-expansion factors as well as basis matrices for VCSs for strong admission structures for a maximum of four participants. MacPherson extended Ateniese_s model to include grey-scale images and derive new results on the minimum possible pixel expansion for all possible CASs on at most four participants. constructing the grey-scale VCSs for CASs is a open problem. Drawbacks of Ateniese_s approach is black secret pixels cannot be completely recovered, the aspect ratio of the improved image cannot be maintained, and this approach needs a difficult codebook design.

B.2 Hsu's Approach

Hsu reported the formulation of an unexpanded VCS for a CAS problem. In this method adopts a set of n x 1 column vectors to share a secret pixel to encrypt n participants, thus eliminating the drawbacks of pixel expansion. Based on the model, a probability matrix can be found and used to encrypt a secret for a specific admission structure. Hsu_s objective is to maximize contrast values for all qualified improved images subject to the security constraint. They use the goal-programming technique and also develop a genetic-based algorithm to solve the optimization problem [7-8]. Hsu_s approaches have better maximum and average contrast values for recovered images than Ateniese_s approach. Drawback of hsu approach is poor visual quality of improved images, blackness of the image is low and cannot guarantee an acceptable contrast level.

B.3 Lee's approach

Lee proposed the formulation of a SSVCS for strong common admission structures (Γqual , Γforb),based on the probabilistic (n,n) –VCSs [12]. Lee_s approach is to find a construction set for a given admission structure and quality of basis shares. The basis shares that were yielded by the probabilistic (n,) –VCSs are used to synthesize the shares of (Γqual , Γforb)-VCS according to the construction set. For example: there are 4 participants p={1,2,3,4}. Qualified sets Γqual is {{1,2},{1,2,3},{1,2,4},{3,1,4},{1,2,3,4}}.Three basic shares are shares in 4 participants. Share construction set c={{s1},{s2,s3},{s2},{s3}}. Encryption procedure generates 3 basis shares s1,s2,s3 to 4 participants S1,S2,S3,S4, for the (Γqual , Γforb) – VCS. basis shares s1,s2,s3 shares S1,S3,S4. Stack the qualified set shares and get the secret information. Pixel-expansion-free (n,)-VCS method is used in lee's approach. Lee_s approach has some drawbacks. First, the visual quality of improved images depends on the (n,n)-VCS. Second,In share generation needs two encryption phase.

III. PROPOSED MODEL

The main idea behind the proposed SSVCS is the probabilistic visual cryptography (ProbVC). To share a black (white) pixel, one of the column vectors in C1 (C0) is randomly chosen and then distributes i-th entry in the column vector to i-th share. For example, the (2,3)-ProbVC scheme is constructed by the following collections of column vectors

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

Encryption of black secret pixel and suppose the chosen column vector is [0 1 0]T, the pixels 0, 1, and 0 are distributed to shares 1, 2, and 3 respectively. image size of shared and stacked images is same as the secret image.

Definition 1. The n-tuple Boolean column vector S = [sj]T with $1 \le j \le n$, is defined as an encoding pattern for each original pixel, where sj=0 (1) denotes that the pixel is encoded as a white (black) sharing pixel in share j.

Definition 2. Suppose P={1,….,n} is a set of n participants and 2P denotes the power set of P. When a set of participants X with X 2 P\ , stack their shares (which were encrypted by vector S) together, the visual effect (i.e., black or white) of a stacked pixel can be obtained by L(VX)=s p1+ sp2+⋯+ spk, where k =| X| and p1 ,…, pk X. The quantity VX is a k-tuple column vector, vxT =[s p1 sp2 ⋯ spk], and the operator —+ ‖ represents the OR operation. If L(vX) = 1 (0), the corresponding pixel will be decoded as black (white) on the stacked image.

Example 1. Suppose 3 participants P = {1,2,3} but two participants stack their shares. Pixel values on their shares black and white and white respectively. Column vector of the participants 1 and 2 is vT{1,2} = [s1 s2] = [1 0] and the stacked pixel is black and it is calculated by the formula L(v{2,3}) = s1 + s2 =1. Column vector of the participants 2 and 3 is vT{2,3} = [s2 s3] = [0 0] and the stacked pixel is black and it is calculated by the formula L(v{2,3}) = s2 + s3 =0. the blackness of a improved image is proportional to the Hamming weight H(V). hamming weight is calculated based on the OR operation. for example share1 = [ ] and share2 = [ ] calculating the hamming weights are H([0 1]) = 1 and H([1 1]) = 2 respectively. OR operation is performed for the corresponding column vector

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

Encryption of black secret pixel and suppose the chosen column vector is $[0\ 1\ 0]^T$, the pixels 0, 1, and 0 are distributed to shares 1, 2, and 3 respectively. image size of shared and stacked images is same as the secret image.

Definition 1. The n-tuple Boolean column vector $S = [s_j]^T$ with $1 \le j \le n$, is defined as an encoding pattern for each original pixel, where sj=0 (1) denotes that the pixel is encoded as a white (black) sharing pixel in share j.

Definition 2. Suppose P={1,….,n} is a set of n participants and 2^P denotes the power set of P. When a set of participants X with $X \in 2^P \backslash \emptyset$, stack their shares (which were encrypted by vector S) together, the visual effect (i.e., black or white) of a stacked pixel can be obtained by $L(VX)=s\,p1+ sp2+\cdots+ spk$, where $k =|X|$ and $p_1, \ldots, pk \in X$. The quantity VX is a k-tuple column vector, $v_x^T = [\, s\,p1\ sp2\ \cdots\ spk\ ]$, and the operator "+" represents the OR operation. If L(vX) = 1 (0), the corresponding pixel will be decoded as black (white) on the stacked image.

Example 1. Suppose 3 participants P = {1,2,3} but two participants stack their shares. Pixel values on their shares black and white and white respectively. Column vector of the participants 1 and 2 is $v^T_{\{1,2\}} = [s_1\ \ s_2] = [1\ \ 0]$ and the stacked pixel is black and it is calculated by the formula $L(v_{\{2,3\}}) = s_1 + s_2 = 1$. Column vector of the participants 2 and 3 is $v^T_{\{2,3\}} = [s_2\ \ s_3] = [0\ \ 0]$ and the stacked pixel is black and it is calculated by the formula $L(v_{\{2,3\}}) = s_2 + s_3 = 0$. the blackness of a improved image is proportional to the Hamming weight H(V). hamming weight is calculated based on the OR operation. for example share1 = $\begin{bmatrix}0 & 1\\0 & 1\end{bmatrix}$ and share2 = $\begin{bmatrix}0 & 1\\1 & 0\end{bmatrix}$ calculating the hamming weights are H([0 1]) = 1 and H([1 1]) = 2 respectively. OR operation is performed for the corresponding column vector.

Definition 3. P={1,….,n} is a set of n participants that share an image encoded by an encoding set $C = \{S_i, 1 \le i \le m\}$where Si =[s i,j]- is an n-tuple Boolean column vector. For any subset set X, $\{i_1, i_2, \ldots, iq\}$ is all members of X with $\{i_1, i_2, \ldots, iq\} \subset \{1,2,\ldots,n\}$. Let VC,X denotes the collections of q-tuple vectors that are obtained by restricting each n-tuple vector in C to rows $i_1, i_2, \ldots, iq$. The set $\lambda C,X = \{L(vi,X)\ \forall\ Vi,X \in VC,X,\ X \in 2^P \backslash \emptyset\}$ represents the stacked result of all shares in X . The blackness of this improved image is H(λC,X)/m, where H(λC,X) is the Hamming weight of λC,X.

Definition 4. Suppose an image is stacked from shares held by a set of participants X. These shares hold a portion of a secret image via a VC scheme and two collections C_1 and C_0 of sets, where Ct ={S i,1 ≤ i ≤m}, $t \in \{0,1\}$. The contrast (denoted as α_x) and blackness (denoted as β_x) for the image can be defined as

$$\alpha_X = \frac{H(\lambda_{C_1,X}) - H(\lambda_{C_0,X})}{m} \text{ and } \beta_X = \frac{H(\lambda_{C_1,X})}{m}.$$

Definition 5. Suppose P={1,….,n} is a set of n participants. A solution with non-expandable shares to the VCS for an access structure $(\Gamma_{qual}, \Gamma_{forb})$ on P consists of two collections of sets, C_1 and C_0 of sets, where Ct ={S i,1 ≤ i ≤m}, $t \in \{0,1\}$.

Image difference is calculated using threshold. Following conditions are satisfied:

α_{TH} is denotes threshold.

1. For any $Y \in \Gamma_{forb}$, $VC1,Y = V\,C_{0,}Y$.
2. For any $X \in \Gamma_{qual}$, $H(\lambda C1,X) - H(\lambda C_0,X) > \alpha_{TH}$.

Condition 1 is the security condition on restricting secret accessibility of any forbidden set. The chosen probability is $H(\lambda C1,Y)/m = H(\lambda C_0,Y)/m$ Condition 2 ensures that the blackness of recovered black secret pixels is higher than that of recovered white secret pixels in a qualified recovered image. If $H(\lambda C1,Y) - H(\lambda C_0,Y) > \alpha_{TH}$, a human's visual system can recognize a difference between the recovered secret pixels. If α_{TH} is large enough, a human's visual system can distinguish between the recovered black and white secret pixels to obtain the secret images.Randomly chooses the column vector C_0 (C_1) to encrypt white (black) secret pixels in the encryption phases in SSVCS. Encryption is performed pixel by pixel. This method is easy and low complexity but it is not guarantee that the pixel can be uniformly distributed in a small area in the improved image. Chow et al.'s scheme, the encryption process is performed by taking a multi-pixel block as a unit of encryption. Zhang et al. also worked on the multi-pixel encoding method to improve the quality of the improved image.Their method is similar to Chow et al.'s; however, 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, C_1 and C_0, for SSVCSs upon a given access structure. Hence, we use the single pixel encoding method to generate shares in the following experiments.

Example 2. Suppose there are four participants P = {1,2,3,4}, that share a secret image; the minimal qualified set Γ_0 = {{1,2,3},{1,4},{3,4}} and the forbidden set is $\Gamma_{forb} = 2^P \backslash \Gamma_{qual}$. Then, the $(\Gamma_{qual}, \Gamma_{forb})$ -VCS can be constructed using two set of collections

$$C_0 = \{2: E_0, 1: E_6, 1: E_{11}, 1: E_{13}\} = \left\{\begin{bmatrix}0\\0\\0\\0\end{bmatrix}, \begin{bmatrix}0\\0\\0\\0\end{bmatrix}, \begin{bmatrix}0\\1\\1\\0\end{bmatrix}, \begin{bmatrix}1\\0\\1\\1\end{bmatrix}, \begin{bmatrix}1\\1\\0\\1\end{bmatrix}\right\}$$

$$C_1 = \{1: E_1, 1: E_2, 1: E_4, 1: E_8, 1: E_{14}\} = \left\{\begin{bmatrix}0\\0\\0\\1\end{bmatrix}, \begin{bmatrix}0\\0\\1\\0\end{bmatrix}, \begin{bmatrix}0\\1\\0\\1\end{bmatrix}, \begin{bmatrix}1\\0\\0\\0\end{bmatrix}, \begin{bmatrix}1\\1\\1\\0\end{bmatrix}\right\}.$$

Security condition for forbidden sets. Let $Y=\{1,2\} \in \Gamma_{forb}$

$$\lambda_{C_0,Y} = \{L(v_{1,Y}), L(v_{2,Y}), L(v_{3,Y}), L(v_{4,Y}), L(v_{5,Y})\} = \left\{L\left(\begin{bmatrix}0\\0\end{bmatrix}\right), L\left(\begin{bmatrix}0\\0\end{bmatrix}\right), L\left(\begin{bmatrix}0\\1\end{bmatrix}\right), L\left(\begin{bmatrix}1\\0\end{bmatrix}\right), L\left(\begin{bmatrix}1\\1\end{bmatrix}\right)\right\} = \{0,0,1,1,1\},$$

$$\lambda_{C_1,Y} = \left\{L\left(\begin{bmatrix}0\\0\end{bmatrix}\right), L\left(\begin{bmatrix}0\\0\end{bmatrix}\right), L\left(\begin{bmatrix}0\\1\end{bmatrix}\right), L\left(\begin{bmatrix}1\\0\end{bmatrix}\right), L\left(\begin{bmatrix}1\\1\end{bmatrix}\right)\right\} = \{0,0,1,1,1\},$$

And

$$V_{C_1,Y} = V_{C_0,Y} = \left\{\begin{bmatrix}0\\0\end{bmatrix}, \begin{bmatrix}0\\0\end{bmatrix}, \begin{bmatrix}0\\1\end{bmatrix}, \begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}1\\1\end{bmatrix}\right\}$$

the forbidden set Y={1,2} is secure. security condition is easily verified in all forbidden sets.

α_x is calculated based on the below equation

$$\alpha_X = \frac{H(\lambda_{C_1,X}) - H(\lambda_{C_0,X})}{m} = \frac{4-3}{5} = \frac{1}{5}.$$

Observation 1. Each improved images has vary contrast in (Γ_{qual} , Γ_{forb}) -VCS. In this VCS secret can be revaled in qualified set X,X ∈ Γ_{qual}. The relationship between Γ_{qual} , Γ_{forb} and Γ_0.

In figure 1.

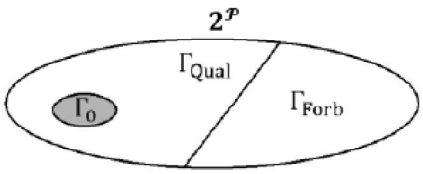


Figure 1 says Γ_{qual} is closure of Γ_0, X,X ∈ Γ_{qual} and X ∈ Γ_0, should be subset of Y,Y ∈ Γ_0. Secret can be revealed by stacked all shares in minimal set Y.

Definition 6. Suppose P={1,….,n} is a set of n participants. A solution of a (Γ_0 , Γ_{forb}) -VCS on P consists of two collections of sets C_0 and C_1 of sets. Collection C_0 (C_1) is used to encrypt white (black) pixels of secret images. The solution is considered feasible if the security condition can be satisfied for any set Y ∈ Γ_{Forb}. and the secret can be revealed for any set X_1 ∈ Γ_0. The contrast condition can be ignored for the qualified set X_2 ,X_2 ∈ Γ_{qual}, and X_2 ∈ Γ_0. The (Γ_0 , Γ_{forb}) -VCS also is called a weak VCS for GASs.

Observation 2. Instead of applying the (Γ_{qual} , Γ_{forb}) -VCS, the (Γ_0 , Γ_{forb}) -VCS can have a higher opportunity to construct recovered images with better contrast.

Observation 3. Blackness of a recovered image will affect (i.e., increase or decrease) the display quality of the image.

Three observations are indicates the two issues in VCS for CASs.first, the contrast of the images in a qualified set, second, display quality of the recovered images can be improved by adjusting the blackness of the improved images

IV. HE PROPOSED ALGORITHM

A. Formulation

The problem for constructing a (Γ0 , Γforb) -VCS is to find the two collections of sets C0 and C1 subject to the security, contrast, and blackness constraints. From the perspective of the quality of the recovered image, the objectives of the proposed formulation are to maximize the worst and the average contrast for recovered secret images among all minimal qualified sets.

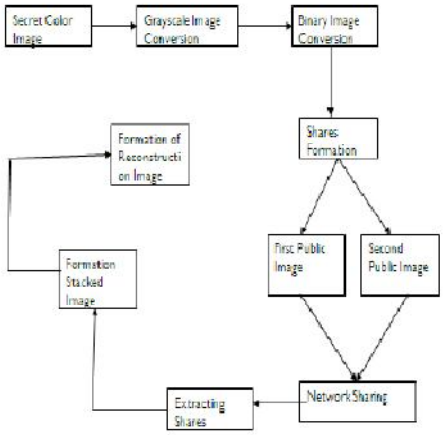
B. SA algorithm

Simulated annealing (SA) based algorithm is a generic probabilistic metaheuristic for global optimization problem. In this algorithm is increase tha display quality and maintain the image ratio and the blackness of the image size is maintain. The pseudocode for the SA algorithm is given below

Algorithm SIMULATED-ANNEALING
Begin
Temp=INIT-temp;
Place=INIT-PLACEMENT;
While(temp)>FINAL-TEMP) do
While(inner_loop_criterion=FALSE) do
New place=PERTURB(place);
ΔC=COST(new_place)-COST(place);
If(ΔC<0)then
Place=new place;
Elseif(RANDOM(0,1)> e-(ΔC/temp))then
Place=new_place;
Temp=SCHEDULE(temp);
END.

SA algorithm starts with a random initial placement in high temperature.the moving of the next pixel is defined move. Calculating the score based on the move made. The probability of the acceptance is based on the current temperature. update the temperature until pixel getting the curect temperature. in this SA algorithm temperature is says about the contrast value of the each pixel

V. ARCHITECTURE DIAGRAM.



In this architecture diagram secret color Image is converted grayscale image. Grayscale image is converted in to binary image because VCSs only applicable in binary images. After applied the VCS secret information is feed in to the shares and binary image is converted into the color image. This image is passed into the network. Receiver will extract the information through the stack the shares. Using the SA algorithm image can be reconstructed.

VI. RESULTS AND COMPARISON

A. Result

The proposed system assess the performance from the quantitative and qualitative view points.the performance of

(Γ0 , Γforb) - VCS is better than the (Γqual , Γforb) – VCS. (Γ0, Γforb) having the better constrast value and high blackness recovery. Experimental is performed based on the

average α_{avg} and minimum α_{min} contrast values.

TABLE VI
A COMPARISON BETWEEN $(\Gamma_0, \Gamma_{Forb})$- AND $(\Gamma_{Qual}, \Gamma_{Forb})$- VCSS

No	$(\Gamma_0, \Gamma_{Forb})$-VCS			$(\Gamma_{Qual}, \Gamma_{Forb})$-VCS		
	m	α_{min}	α_{avg}	m	α_{min}	α_{avg}
1	6	1/3	33.3%	6	1/3	33.3%
2	4	1/4	37.5%	4	1/4	37.5%
3	4	1/4	25.0%	5	1/5	26.7%
4	4	1/4	25.0%	4	1/4	25.0%
5	4	1/4	25.0%	4	1/4	25.0%
6	5	1/5	20.0%	5	1/5	20.0%
7	6	1/6	16.7%	6	1/6	16.7%
8	6	1/6	16.7%	6	1/6	16.7%
9	12	1/12	10.4%	12	1/12	10.4%
10	10	1/10	10.0%	10	1/10	10.0%
11	10	1/10	10.0%	10	1/10	10.0%
12	15	1/15	6.7%	15	1/15	6.7%
13	14	1/14	7.1%	15	1/15	6.7%
14	18	1/18	5.5%	18	1/18	5.6%
15	18	1/18	18.5%	19	1/19	12.8%
16	18	1/18	5.5%	25	1/25	6.0%
17	16	1/16	6.3%	31	1/31	6.0%
18	20	1/20	5.0%	24	1/24	4.2%
19	19	1/19	19.3%	19	1/19	5.3%
20	14	1/14	17.2%	15	1/15	12.0%

m: number of column vectors in code collection C_0 (or C_1)

Performance of $(\Gamma_0, \Gamma_{Forb})$ - VCS is based on the blackness constraints. Performance is based on the three optimum models

- Model A: $(\Gamma_0, \Gamma_{Forb})$-VCS without blackness constraint.
- Model B: $(\Gamma_0, \Gamma_{Forb})$-VCSs under the blackness constraint with blackness control parameter δ=1
- Model C: $(\Gamma_0, \Gamma_{Forb})$-VCSs under the blackness constraint with parameter δ=0

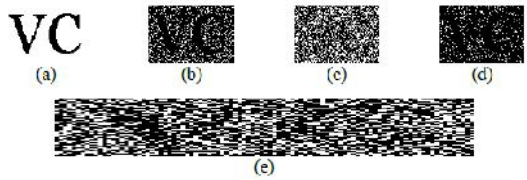
TABLE VII
THE WORST-CASE CONTRAST (α_{min}) OF $(\Gamma_0, \Gamma_{Forb})$-VCSS IN VARIOUS BLACKNESS CONSTRAINTS

No	Optimization models							
	A			B (δ=1)			C (δ=0)	
	m	α_{min}	β	m	α_{min}	β	m	α_{min}
1	6	1/3	5/6	6	1/3	5/6	8	1/4
2	4	1/4	1	4	1/4	1	4	1/4
3	4	1/4	3/4	4	1/4	0	9	2/9
4	4	1/4	1	4	1/4	1	4	1/4
5	4	1/4	1	4	1/4	1	4	1/4
6	5	1/5	3/5	5	1/5	3/5	6	1/6
7	6	1/6	5/6	6	1/6	5/6	6	1/6
8	6	1/6	5/6	6	1/6	5/6	9	1/9
9	12	1/12	5/6	15	1/15	5/6	10	1/10
10	10	1/10	4/5	10	1/10	4/5	12	1/12
11	10	1/10	4/5	10	1/10	4/5	14	1/14
12	15	1/15	13/15	15	1/15	13/15	25	1/25
13	14	1/14	6/7	14	1/14	6/7	18	1/18
14	18	1/18	8/9	18	1/18	8/9	25	1/25
15	18	1/18	7/9	18	1/18	7/9	18	1/18
16	10	1/10	5/6	10	1/10	5/6	10	1/10
17	16	1/16	3/4	16	1/16	3/4	16	1/16
18	20	1/20	17/20	20	1/20	17/20	20	1/20
19	19	1/19	11/19	19	1/19	11/19	19	1/19
20	14	1/14	6//	14	1/14	6//	14	1/14

β: the blackness of the recovered image which has the worst contrast value α_{min}

B. Comparison:

Compare our results with the other results of Ateniese,Hsu,Lee.



These results verify the effectiveness of the proposed optimization model in improving the contrast for the image in the worst case. Figure 4 is represent the fig 4(a) is our original secret information. Fig4(b) is represent the recovered images of this study (contrast α_{min}=2/9, blackness β=1).Fig4(c) is represent the recovered image of Lee's study (α_{min}=1/8, blackness β=1).
fig4(e) is represent the recovered image of ateniese's approach (pixel expansion factor=5, α_{min}=1/5, blackness β=0.8).

CONCLUSION

In this approach, weak visual cryptography scheme for CASs. The proposed model for SSVCSs eliminates the disadvantages of the pixel-expansion problem. Our method guarantees the blackness of black secret pixels for VCSs and improves the display quality of the worst-case image. It is better than the previous results. It increase the display quality of the improved 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 SSVCS for CASs subject to controllable blackness of black secret pixels. Second, we formulate the construction problem of the SSVCS for CASs 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.

REFERENCES

[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.

[9] F. Liu, C. Wu, and X. Lin, —Step Construction of Visual Cryptography Schemes, ‖ *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 1, pp. 27–38, 2010.

[10] A. Adhikari, T. K. Dutta, and B. Roy, —A New Black and White Visual Cryptographic Scheme for General Access Structures, ‖ *Indocrypt'04, LNCS*, vol. 3348, pp.399–413, 2004.

[11] L. A. MacPherson, —Grey Level Visual Cryptography for General Access Structures, ‖ *M.S. thesis, Univ. Waterloo*, Waterloo, ON, Canada, 2002.

[12] K. H. Lee and P. L. Chiu, —An Extended Visual Cryptography Algorithm for General Access Structures, ‖ *IEEE Transactions on Information Forensics and Security*, vol.7, no.1, pp.219-229, 2012.

[13] F. Liu, C. K. Wu, and X. J. Lin, —A New Definition of the Contrast of Visual Cryptography Scheme, ‖ *Information Processing Letters*, vol. 110, no, 7, pp. 241-246, 2010.

[14] C. Blundo, and A. De Santis, —Visual cryptography schemes with perfect reconstruction of black pixels, ‖ *Computers & Graphics*, vol. 22, no. 4, pp. 449–455, 1998.

[15] T. Hofmeister, M. Krause, and H. U. Simon, —Contrast-optimal k out of n Secret Sharing Schemes in Visual Cryptography, ‖ *Theoretical Computer Science*, vol. 240, no. 2, pp. 471–485, 2000.

[16] H. Koga, —A General Formula of the (t,n)-threshold Visual Secret Sharing Scheme, ‖ in *Advances in Cryptology*, Asiacrypt, 2002, pp. 328–345.

[17] Y. W. Chow, W. Susilo and D. S. Wong, ―Enhancing the Perceived Visual Quality of a Size Invariant Visual Cryptography Scheme,□ *Lecture Notes in Computer Science*, vol. 7618, pp. 10-21, 2012.

[18] H. B. Zhang, X. F. Wang, W. H. Cao, and Y. P. Huang, ―Visual Cryptography for General Access Structure using Pixel-Block Aware Encoding,□ *Journal of Computers*, vol. 3, no. 12, pp. 68–75, 2008

★★★