Multimed Tools Appl (2019) 78:1315–1344
https://doi.org/10.1007/s11042-018-6158-3

Deterministic extended visual cryptographic schemes for general access structures with OR-AND and XOR-AND operations

Praveen Kanakkath[1] · Sethumadhavan Madathil[1] · Ramakrishnan Krishnan[1]

Received: 20 October 2017 / Revised: 26 March 2018 / Accepted: 16 May 2018 /
Published online: 20 June 2018

Abstract In Visual Cryptographic Scheme (VCS) shares of the secret image look like random, whereas in Extended Visual Cryptographic Scheme (EVCS) the shares look like meaningful images. In the case of ideal contrast deterministic constructions for VCS, depending upon the access structure, each participant needs to hold one/multiple image shares with same size of the binary secret image and the secret image will be reconstructed without any change in resolution. In this paper, two deterministic constructions for EVCS with a relative contrast of 0.333 are proposed by utilizing the ideal contrast deterministic constructions for VCS as a building block. The proposed schemes are applicable to share secret binary images only. Theoretical analysis and comparison with other related works are given in this paper.

Keywords Visual cryptography · Extended visual cryptography · OR-AND reconstruction · XOR-AND reconstruction · General access structure

1 Introduction

Today, every business, medical and research units of government/private sectors transfer digital images over the Internet and store it in public cloud servers. In order to mitigate

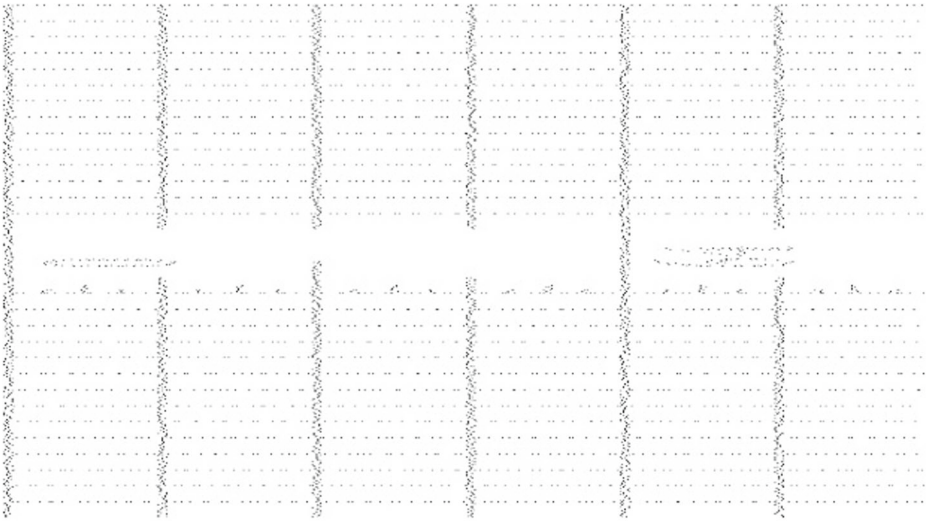
✉ Praveen Kanakkath
k_praveen@cb.amrita.edu

Sethumadhavan Madathil
m_sethu@cb.amrita.edu

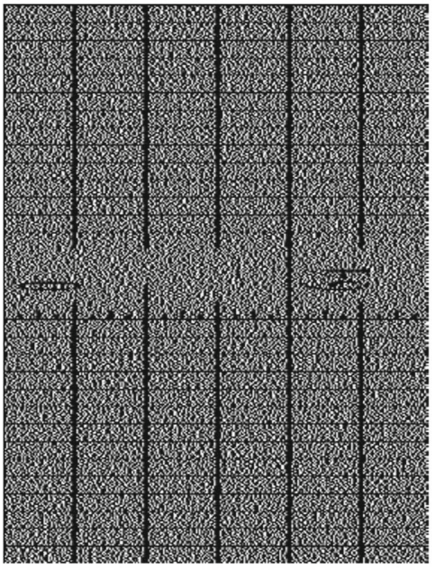
Ramakrishnan Krishnan
drrkdrrk@gmail.com

[1] TIFAC-CORE in Cyber Security, Amrita School of Engineering, Amrita Vishwa Vidyapeetham, Coimbatore, India

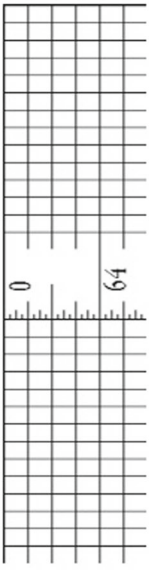
any event of disclosure of secret images to unauthorized persons, there exist various techniques like steganography [23–25] and secret sharing. Secret image sharing is a practice of encoding the secret image into shares and steganography is the practice of hiding a secret information within another file, image or video. Secret images can be encoded into shares



(a) *RI* for Ateniese *et al*. EVCS [13]



(b) *RI* for Our EVCS



(c) *SI*

(d) *RI* for Probabilistic Yang [11]

Fig. 1 Reconstructed images for (2, 3) EVCS

either by complex computations like Lagrange interpolations or using Visual cryptography. In this paper, we focus on the development of Visual cryptographic scheme.

Visual cryptography, pioneered by Naor and Shamir [34], is a method in which the dealer generates random-looking shares from a secret image (*SI* Figs. 1, 7 and 11), then distributes these shares to a set of participants and when sufficient shares combine, the reconstructed image (*RI*) will be generated. The quality of a VCS is measured using two parameters: pixel expansion and contrast. The pixel expansion is the number of sub pixels used for encoding a pixel while, contrast is the difference in gray level between black and white pixels of *SI*. One can distinguish the black (1) and white (0) pixel in the *RI* because every m sub pixel in black area will have more black sub pixels than in white area. The Boolean operations used in VCS for reconstruction are: XOR, OR, AND and NOT. In deterministic VCS all the black and white areas of *SI* will be reconstructed in *RI*. Deterministic VCS were introduced in [3, 6, 34]. The perfect black VCS constructions were discussed in [6, 7]. In ideal contrast VCS, the secret *SI* is reconstructed using combined Boolean operations (either OR and NOT [10] or OR and XOR [45] or OR and AND [37]) without loss of resolution. For XOR based ideal contrast step construction [28], participants hold less number of multiple shares when compared with the constructions given in [10, 37, 45]. Deterministic EVCS [5, 20, 27, 31, 32, 44, 46, 48–50, 53, 56, 58, 59, 62, 63] and probabilistic EVCS [8, 9, 12, 15, 16, 18, 22, 35, 36, 39–41, 47, 54, 55] are other types of VCS where the shares of *SI* look like meaningful. The halftone EVCS constructions are discussed in [48–50, 56, 63]. EVCS for (2, 2) [32], (k, k) [18], (k, n) [46] are some of the existing threshold access structure constructions. Progressive EVCS constructions are given in [8, 16]. Apart from some of these schemes [1, 51, 52] as a solution for authentication, Naor and Pinkas [33] proposed a solution based on visual cryptography. Some other applications of visual cryptography are discussed in papers [2, 11, 21, 30, 38, 43, 60, 61].

In ideal contrast VCS constructions [10, 28, 37, 45], each participant needs to carry multiple shares which are of same size of *SI*. For EVCS in general each participant carries a single pixel expanded meaningful image as share. In this paper, we propose constructions (PC1 and PC2) for EVCS having the relative contrast value of *RI* as 0.333, where each participant carries multiple meaningful images as shares. Since each participant holds multiple shares, we consider the average pixel expansion (APE) instead of pixel expansion, where the APE [28] is defined as the average value of the total pixel expansions of the share images that each participant holds. For a good EVCS the APE value needs to be low and relative contrast value of the reconstructed image needs to be high. Our construction shows better results for relative contrast (Fig. 1) and APE values compared with the existing EVCS. The proposed algorithm works when the secret and cover are binary images.

The rest of the paper is organized as follows. Section 2 shows the background and Section 3 shows the proposed EVCS constructions respectively. Conclusions are given in Section 4.

2 Preliminaries

Let $P = \{p_1, p_2, p_3, ..., p_t, ..., p_n\}$ be the set of participants, and 2^P denote the power set of P. Let us define a subset $E = \{p_1, ..., p_t\}$ of P. Denote Γ_{Qual} as qualified set and Γ_{Forb} as forbidden set where, $\Gamma_{Qual} \cap \Gamma_{Forb} = \emptyset$. Any set $A \in \Gamma_{Qual}$ can recover *SI* whereas any set $A \in \Gamma_{Forb}$ cannot recover *SI*. Let $\Gamma_{QM} = \{A \in \Gamma_{Qual}: A' \notin \Gamma_{Qual} \text{ for all } A' \subset A\}$ be the set of minimal qualified subsets of P. Let $\Gamma_{FM} = \{B \in \Gamma_{Forb}: B \cup \{i\} \in \Gamma_{Qual} \text{ for all } i \in P \setminus B\}$ be the set of maximal forbidden subsets of P. The pair $\Gamma = (\Gamma_{Qual}, \Gamma_{Forb})$ is the access structure of the scheme. A VCS with $\Gamma_{QM} = \{A \in \Gamma_{Qual}: A \subseteq P \text{ and } |A| = k\}$ is called (k, n) - VCS. A

VCS with $\Gamma_{QM} = \{A \in \Gamma_{Qual}: A \subseteq P, p_1 \in A \text{ and } |A| = k\}$ is called $(1, k, n)$ - VCS. A VCS with $\Gamma_{QM} = \{A \in \Gamma_{Qual}: A \subseteq P, E \subseteq A \text{ and } |A| = k\}$ is called (t, k, n) - VCS. Let us denote the set $\Gamma_{EM} = \{A_1, A_2, A_3, ..., A_r\}$ which contains r minimal qualified subsets such that $A_1 \cap A_2 \cap A_3, ..., A_{r-1} \cap A_r = E \neq \emptyset$. Let S be an $n \times m$ Boolean matrix and $A \subseteq P$, then the vector obtained by applying the Boolean operations to the rows of S corresponding to the elements of A is denoted by S^A and number of ones in the vector S^A is denoted as $W(S^A)$.

Let us define the notations used in this paper.

1) $\bar{x} = \begin{cases} 1 \ if \ x == 0 \\ 0 \ if \ x == 1 \end{cases}$ as NOT operation
2) $\bigotimes$ as OR operation
3) $\bigoplus$ as XOR operation
4) $\bigodot$ as AND operation
5) $\begin{bmatrix} x_1 & x_2 & x_3 \end{bmatrix} \bigotimes \begin{bmatrix} y_1 & y_2 & y_3 \end{bmatrix} = \begin{bmatrix} x_1 \bigotimes y_1 & x_2 \bigotimes y_2 & x_3 \bigotimes y_3 \end{bmatrix}$
6) $\begin{bmatrix} x_1 & x_2 & x_3 \end{bmatrix} \bigoplus \begin{bmatrix} y_1 & y_2 & y_3 \end{bmatrix} = \begin{bmatrix} x_1 \bigoplus y_1 & x_2 \bigoplus y_2 & x_3 \bigoplus y_3 \end{bmatrix}$
7) $\begin{bmatrix} x_1 & x_2 & x_3 \end{bmatrix} \bigodot \begin{bmatrix} y_1 & y_2 & y_3 \end{bmatrix} = \begin{bmatrix} x_1 \bigodot y_1 & x_2 \bigodot y_2 & x_3 \bigodot y_3 \end{bmatrix}$
8) N_i as the number of shares held by participant p_i
9) $Size_i$ as the share size of a single pixel of SI
10) # as the number of Boolean operations done during reconstruction.
11) SPP as Shares hold by each participant.
12) RI as the reconstructed image.
13) OI as the intermediate image generated for reconstructing RI in PC2.
14) $D_{(u,j)}$: The j^{th} share of the u^{th} participant, $Sh_{(u,j)}$ of size $p \times 3q$ is generated using all the $p \times q$ row vectors $D_{(u,j)}$ of size 1×3.

Definition 1 (**OR operation based**) [6]: Let $\Gamma = (\Gamma_{Qual}, \Gamma_{Forb})$ be an access structure on a set of n participants. Two collections of $n \times m$ Boolean matrices C_0 and C_1 constitute a $(\Gamma_{Qual}, \Gamma_{Forb})$-VCS if there exists a positive real number α and the set of thresholds $\{t_A \mid A \in \Gamma_{Qual}\}$ satisfying the following two properties

1. Any qualified set $A = \{i_1, i_2, ..., i_p\} \in \Gamma_{Qual}$ can recover SI by stacking their transparencies. Formally for any S_0 in C_0, $W(S_0^A) \leq t_A - \alpha \times m$ and for any S_1 in C_1, $W(S_1^A) \geq t_A$.
2. Any forbidden set $A = \{i_1, i_2, ..., i_p\} \in \Gamma_{Forb}$ has no information on SI.

Two collections of matrices $C_v, v \in \{0, 1\}$ in Definition 1 are obtained by generating all permutations of the basis matrices $S_v, v \in \{0, 1\}$. In such a case, $|C_0| = |C_1| = m!$ and $r = \log_2 m!$ is called the randomness of the VCS [13, 17]. Formally the two collections of $p \times m$ matrices are obtained by restricting each $n \times m$ matrix in S_v to the rows $i_1, i_2, ..., i_p$ are indistinguishable. The first property is related to contrast $\alpha \times m$ of RI. The number α is called the relative contrast. The second is for the security of the scheme.

2.1 EVCS - Ateniese et al. [5]

In the case of EVCS, the share of the participants belonging to set P is meaningful, and is not random-looking in nature as in conventional VCS. Let $C_{sc}^{c_1,.....,c_n}$ where, $\{c_1, ..., c_n\} \in \{0, 1\}$, be the collection of matrices from which the dealer chooses a matrix to encode a c_i pixel, where $i = 1$ to n in the image COV_i (cover images or meaningful images) associated to participants in set P in order to obtain a sc pixel when the transparencies associated to the participants in the set $A \in \Gamma_{Qual}$ are stacked together. Hence there will be a collection

of 2^n pairs ($C_0^{c_1,\ldots,c_n}$, $C_1^{c_1,\ldots,c_n}$) for all possible combinations of white and black pixels in the n original images. Let $T_0^{c_1,\ldots,c_n} = \left[\, S_0 \,||\, D \,\right] \in C_0^{c_1,\ldots,c_n}$ and $T_1^{c_1,\ldots,c_n} = \left[\, S_1 \,||\, D \,\right] \in C_1^{c_1,\ldots,c_n}$ where, S_0 (resp. S_1) are the basis matrices of perfect black VCS [6, 7] and when stacking the rows of D matrix corresponding to the participants in the qualified set, an all one row vector will obtain. This implies that T_0 (resp. T_1) are basis matrices of a perfect black EVCS for sharing 0 (resp. 1) pixel in *SI*.

Example 1 Let $P = \{p_1, p_2, p_3\}$ be the set of participants, $\Gamma_{QM} = \{\{p_1, p_2\}, \{p_1, p_3\}, \{p_2, p_3\}\}$ and $\Gamma_{FM} = \{\{p_1\}, \{p_2\}, \{p_3\}\}$. Let $SI = \left[\, 1\ 0 \,\right]$. Let the three cover images used in this construction be $COV_1 = \left[\, 0\ 0 \,\right]$, $COV_2 = \left[\, 0\ 1 \,\right]$ and $COV_3 = \left[\, 1\ 1 \,\right]$. Let $S_0 = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix}$ and $S_1 = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{bmatrix}$. Then the Boolean matrices constructed for sharing a 0 pixel is T_0^{011} $= \left[\begin{array}{cccc||ccc} 0 & 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 \end{array}\right]$ and for sharing a 1 pixel is $T_1^{001} = \left[\begin{array}{cccc||ccc} 0 & 1 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 & 1 \end{array}\right]$. So for the access structure (Γ_{QM}, Γ_{FM}) the pixel expansion and relative contrast of Ateniese et al. [5] scheme is 7 and 1/7 respectively.

2.2 Ideal contrast constructions for VCS

Let S_0 (resp. S_1) be the basis matrices of perfect black general access structure scheme ([6] and [7]) for sharing a 0 (resp. 1).

The share generation phase:

In Cimato et al. [10] scheme the m shares for each participant is generated as follows.

$H_{(u,j)}(g,h) = \begin{cases} S_0(u,j) & if SI(g,h) == 0 \\ S_1(u,j) & if SI(g,h) == 1 \end{cases}$; where $j = 1$ to m, $1 \le u \le n$, $0 \le g \le p-1, 0 \le h \le q-1$.

The secret reconstruction phase:

Generate $\Delta_1(g,h) = \bigotimes_{p_u \in \Gamma_{QM}} H_{(u,1)}(g,h)$, $\Delta_2(g,h) = \bigotimes_{p_u \in \Gamma_{QM}} H_{(u,2)}(g,h)$, ...,$\Delta_{m-1}(g,h)$ $= \bigotimes_{p_u \in \Gamma_{QM}} H_{(u,m-1)}(g,h)$, $\Delta_m(g,h) = \bigotimes_{p_u \in \Gamma_{QM}} H_{(u,m)}(g,h)$. Then *RI* is obtained in any of the following three ways when the gray levels of *SI* is 2. Based on Cimato et al. [10] OR-NOT scheme, $RI(g,h) = \overline{\bigotimes_{j=1}^{m} \overline{\Delta_j(g,h)}}$. Based on Wang et al. [45] OR-XOR scheme, $RI(g,h) = \bigoplus_{j=1}^{m} \Delta_j(g,h)$. Based on Praveen et al. [37] OR-AND scheme, $RI(g,h) = \bigodot_{j=1}^{m} \Delta_j(g,h)$. The Wang et al. [45] scheme is also applicable to non perfect black general access structure schemes.

2.3 Ideal contrast Step construction for VCS [28]

In the case of XOR based (2, 2) - VCS, two collections of 2×1 Boolean matrices for sharing a 0 (resp .1) pixel in *SI* are $C_0 = \left\{ \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \end{bmatrix} \right\}$ and $C_1 = \left\{ \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right\}$ respectively. Here

RI is identical to *SI* which implies that the contrast is ideal ($\alpha \times m = 1$) and pixel expansion $m = 1$. By recursively calling XOR based (2, 2)-VCS, Liu et al. [28] in 2010 developed the ideal contrast XOR step construction, where the amount of shares each participant holds is different. The APE and relative contrast of step construction is better when compared to other results and is given in TABLE I of paper [28].

2.3.1 Step construction for (n, n) - VCS (Construction1)

Here initially two shares Sh_1^L and Sh_1^R are generated from *SI* using XOR based (2, 2)-VCS. Then for constructing an (n, n)-VCS select any one of the shares say Sh_1^R as secret image and again generate two shares Sh_2^L and Sh_2^R using XOR based (2, 2)-VCS. This procedure is continued till the shares Sh_{n-1}^L and Sh_{n-1}^R are generated from the share Sh_{n-2}^R using XOR based (2, 2)-VCS. During the share distribution phase, distribute Sh_1^L, Sh_2^L, ..., Sh_{n-1}^L, Sh_{n-1}^R to the n participants in the set P respectively. During the share reconstruction phase, when all the n participants combine their shares, the following procedure will recover the $RI = SI = Sh_1^L \oplus Sh_2^L$, ..., $Sh_{n-1}^L \oplus Sh_{n-1}^R$. Hence the XOR step construction for (n, n) access structure generates a VCS with ideal contrast ($\alpha \times m = 1$) and pixel expansion $m = 1$.

Access structures can be simplified using equivalent participants for effective construction (for achieving small APE). Participants who have the same right can be considered as equivalent participants.

2.3.2 Generation of the simplified qualified set $\widetilde{\Gamma_{QM}}$

Without affecting the security, identical shares are distributed to equivalent participants for simplifying the access structure of VCS. Formally, equivalent participants are defined as follows:

Definition 2 (**Equivalent participants**) [28]: Let Γ_{QM} be the access structure on P. If participant p_i and p_j satisfy that, for all $A \in \Gamma_{FM}, p_i \in A$ hold iff $p_j \in A$ hold, then participant p_i and p_j are considered to be equivalent participants on Γ_{QM}, denoted by $p_i \sim p_j$.

Here $\sim$ is an equivalence relation on P. A quotient set is a set derived from another by an equivalence relation. Let $\widetilde{P}$ be the quotient set derived from P based on $\sim$. Following definition shows how to simplify the access structure based on equivalent participants.

Definition 3 (**Simplifying access structure**) : The simplified access structure based on the equivalent participants is $\widetilde{\Gamma_{QM}} = \{\widetilde{A}: A \in \Gamma_{QM}\}$, where the set $\widetilde{A} = \{\widetilde{p_i} \in \widetilde{P}: p_i \in A\}$ is called the corresponding set of A and $\widetilde{p_i}$ is called the equivalence class or corresponding participant of p_i. Γ_{QM} is called the most simplified access structure when $\widetilde{\Gamma_{QM}} = \Gamma_{QM}$.

Theorem 1 [28]*: Let* $\widetilde{\Gamma_{QM}} = \{\widetilde{A}: A \in \Gamma_{QM}\}$. *By distributing the share images of corresponding participants to the equivalent participants, a construction of VCS for the* $\widetilde{\Gamma_{QM}}$ *is also a construction of VCS for the* Γ_{QM}.

Using Definition 3 and Theorem 1, the ideal contrast XOR based step constructions for VCS are given below.

2.3.3 Step construction for Γ_{EM} (Construction2)

Let us denote the set $\Gamma_{EM} = \{A_1, A_2, A_3, ..., A_r\}$ which contains r minimal qualified subsets such that $A_1 \cap A_2 \cap A_3, ..., A_{r-1} \cap A_r = E \neq \emptyset$ where $E = \{p_1, ..., p_t\}$. Let $\Gamma' = \{A \setminus E : A \in \Gamma_{EM}\}$. Method 1 and Method 2 for constructing Γ_{EM} are represented as construction trees of Figs. 2 and 3, respectively. It is given in Theorem 6 of paper [28] that the APE and contrast for both the methods are the same.

Method 1: The shares $Sh_1^L, Sh_2^L, ..., Sh_t^L$ shown in Fig. 2 are distributed to the participants $p_1, p_2, ..., p_t$ respectively. For all $L \in \Gamma'$, if $|L| = 1$, distribute Sh_t^R to the participant in L, else for all L when $|L| = d$ and $g = t+d-1$, take Sh_t^R as secret image and generate share images for participants in L based on the construction shown in the Fig. 2. Then distribute the shares $Sh_{t+1}^L, ..., Sh_g^L, Sh_g^R$ to the participants in L.

Method 2: For all $L \in \Gamma'$, if $|L| = 1$, the dealer distributes Sh_1^R to the participant in the set L, else for all L when $|L| = d$, take Sh_1^R as secret image and generate share images $Sh_2^{RL}, ..., Sh_d^{RL}, Sh_d^{RR}$ and distribute it to the participants in the set L respectively as shown in Fig. 3. When $t = 1$, distribute Sh_1^L to p_1, else generate share images $Sh_2^{LR}, ..., Sh_{t-1}^{LL}$ and Sh_{t-1}^{LR} from Sh_1^L and distribute it to the participants $p_1, p_2, ..., p_t$ respectively.

For both methods 1 and 2, the step construction for the sets $L \in \Gamma'$ are processed independently. Let w=$|L \cup E|$, then the step construction of the set $L \cup E$ forms a step construction of (w, w)-VCS. In the case of $\Gamma_{QM} = \{A_1\}$ and $A_1 = \{p_1, ..., p_t\}$, apply step construction of (t, t)-VCS for the participant set A_1.

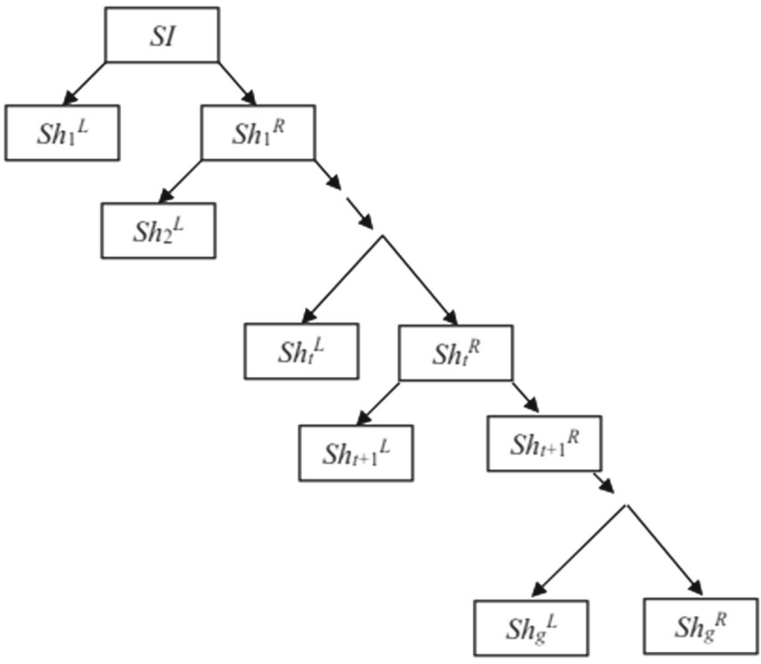


Fig. 2 Step construction Method 1

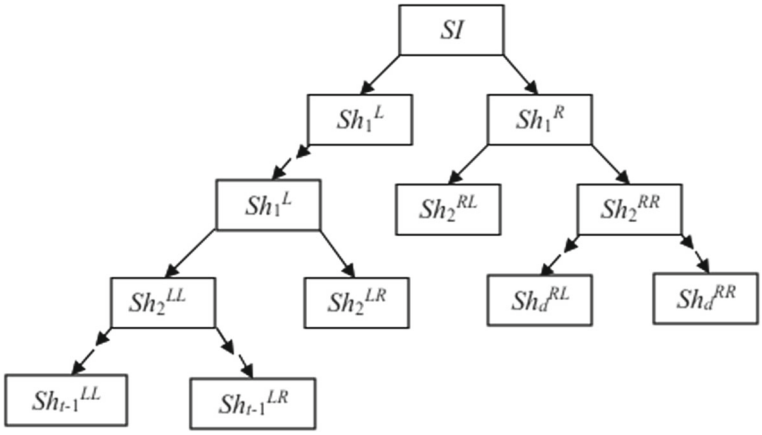


Fig. 3 Step construction Method 2

2.3.4 Step construction of VCS for general access structure(Construction 3)

Following are the steps performed by the dealer for generating shares for $\Gamma = (\Gamma_{QM}, \Gamma_{FM})$.

Step 1) Simplify Γ_{QM} to $\widetilde{\Gamma_{QM}}$ according to Theorem 1.
Step 2) Then divide $\widetilde{\Gamma_{QM}}$ into several parts, say $\Gamma_i = \{A_1, A_2, A_3, ..., A_{ri}\}$ such that $A_1 \cap A_2 \cap A_3, ..., A_{ri} = E_i \neq \emptyset$.
Step 3) For each part Γ_i, let $\Gamma_i' = \{A \setminus E_i : A \in \Gamma_i\}$ and $\Gamma_i'' = \{L \in \Gamma_i' : |L| \neq 1\}$. If $\Gamma_i'' = \emptyset$ then apply Construction 2 directly on Γ_i'. Else treat Γ_i'' as virtual participant E_i' in $\Gamma_i = \{E_i, E_i'\}$. Then apply Construction 2 (Method 1 or Method 2) on Γ_i i.e., apply the (2, 2)-VCS and denote the share image distributed to E_i' as Sh_i'. Then go to Step 1 and apply a new step construction of VCS, which takes Sh_i' as the secret image for the access structure Γ_i''.
Step 4) Repeat Step 1, 2 and 3 until all the participants receive their share images for all the qualified sets in Γ_{QM}.

Theorem 1 simplifies the access structure Γ_{QM}. Step 1 reduces the number of qualified sets in Γ_{QM}. There always exist partitions for a general access structure where each part satisfies the condition of Construction 2 [28]. A simple example for partitioning $\widetilde{\Gamma_{QM}}$ is explained as follows. Assume $\widetilde{\Gamma_{QM}} = \{A_1, A_2, A_3, ..., A_r\}$, then let $\Gamma_1 = \{A_1, A_2, A_3, ..., A_f\}$ be the set of qualified sets which contain p_1, i.e., $A_1 \cap A_2 \cap A_3, ..., A_{f-1} \cap A_f = \{p_1\}$. Let Γ_2 be generated from $\Gamma_1' = \widetilde{\Gamma_{QM}} \setminus \Gamma_1$. Similarly Γ_i is generated from $\Gamma_{i-1}' = \Gamma_{i-2}' \setminus \Gamma_{i-1}$, where all the minimal qualified sets in Γ_i contain participant p_i. Suppose when there are n partitions in total, $\widetilde{\Gamma_{QM}} = \Gamma_1 \cup \Gamma_2 \cup ... \cup \Gamma_n$ and each Γ_i satisfies the condition of Construction 2. APE of VCS will vary based on the partition methods and it is quite complicated to find a general partition method to obtain minimal APE [28]. Suppose for example when $\widetilde{\Gamma_{QM}} = \{\{p_1, p_2, p_3\}, \{p_1, p_2, p_4\}, \{p_1, p_3, p_4\}, \{p_2, p_3, p_4\}\}$. Then we can generate two partitions from Γ_{QM} as $\Gamma_1 = \{\{p_1, p_2, p_3\}, \{p_1, p_2, p_4\}\}$ where $\{p_1, p_2, p_3\} \cap \{p_1, p_2, p_4\} = \{p_1, p_2\}$ and $\Gamma_2 = \{\{p_1, p_3, p_4\}, \{p_2, p_3, p_4\}\}$ where $\{p_1, p_3, p_4\} \cap \{p_2, p_3, p_4\} = \{p_3, p_4\}$. Even though in Step 2, when each part of Γ_{QM} satisfies the condition of Construction 2, in order to obtain a smaller APE, the dealer needs to further divide Γ_i'' by

recursively applying Construction 3. Example 2 shows a ($t = 1, k = 3, n = 4$) access structure where, participant p_1 is an essential participant and is present in all the qualified sets.

Based on some access structures mentioned in Table 1 it is evident that APE for XOR based step construction by Liu et al. [28] VCS is less when compared with VCS by Ateniese et al. [6], Adhikari et al. [3], Shyu et al. [42], Cimato et al. [10], Wang et al. [45] and Praveen et al.[37]. Also constructions [10, 28, 37, 45] will provide ideal contrast, but we cannot obtain ideal contrast for constructions [3, 6, 42]. The disadvantage of constructions [10, 28, 37, 45] is each participant needs to carry multiple shares which is of the same size of secret image, but in the case of constructions [3, 6, 42] each participant needs to carry a single pixel expanded share.

Example 2 Let $P = \{p_1, p_2, p_3, p_4\}$ be the set of participants, the secret image is denoted as *SI* and shares generated using XOR step construction are of same size of *SI*. Let $\Gamma_{EM} = \{\{p_1, p_2, p_3\}, \{p_1, p_2, p_4\}, \{p_1, p_3, p_4\}\}$ and $\Gamma_{FM} = \{\{p_2, p_3\}, \{p_2, p_4\}, \{p_3, p_4\}, \{p_1, p_2\}, \{p_1, p_3\}, \{p_1, p_4\}\}$.

As per the scheme, Γ_{EM} is already in the most simplified form and also satisfies the condition of Construction 2, so $\widetilde{\Gamma_{QM}} = \Gamma_{QM}$. Let Γ_1 be the partition obtained from $\widetilde{\Gamma_{QM}}$. Then apply Construction 2 on Γ_1 to generate $\Gamma_1' = \Gamma_1'' = \{\{p_2, p_3\}, \{p_2, p_4\}, \{p_3, p_4\}\}$.

Let the virtual participant be $E_1' = \Gamma_1''$ then $\Gamma_1 = \{p_1, E_1'\}$. Apply (2, 2)-VCS on the set Γ_1 which generate shares Sh_1^L and Sh_1' from *SI*. Distribute Sh_1^L to p_1 and Sh_1' to virtual participant E_1'. Take Sh_1' as the secret image and apply step construction on Γ_1''. As per the scheme it is possible to divide Γ_1'' into two parts say, $\{\{p_2, p_3\}, \{p_2, p_4\}\}$ and $\{\{p_3, p_4\}\}$.In the case of set $\{\{p_2, p_3\}, \{p_2, p_4\}\}, \{p_3, p_4\} \in \Gamma_{FM}$. So $p_3 \sim p_4$. Apply (2, 2)-VCS on Sh_1' to generate shares Sh_2^{L1} and Sh_2^{R1}. Based on Definition 2, 3 and Theorem 1, distribute Sh_2^{L1} to p_2 and Sh_2^{R1} to p_3 and p_4.In the case of set $\{\{p_3, p_4\}\}$, apply (2, 2)-VCS on Sh_1' to generate shares Sh_2^{L2} and Sh_2^{R2}. Distribute Sh_2^{L2} to p_3 and Sh_2^{R2} to p_4.

So p_1 holds share $H_{(1,1)} = Sh_1^L$ which implies $N_1 = 1$. p_2 holds share $H_{(2,1)} = Sh_2^{L1}$ which implies $N_2 = 1$. p_3 holds shares $H_{(3,1)} = Sh_2^{R1}$ and $H_{(3,2)} = Sh_2^{L2}$ which implies $N_3 = 2$. p_4 holds shares $H_{(4,1)} = Sh_2^{R1}$ and $H_{(4,2)} = Sh_2^{R2}$ which implies $N_4 = 2$. So APE = (1 + 1 + 2 + 2)/4.

3 Main results

3.1 Proposed Construction (PC1)

Initially generate $H_{(u,j)}(g, h)$ for *SI* as given in share generation phase of Section 2.2. As given in Definition 1, in order to provide randomness [13, 17] while encoding each pixel in

Table 1 APE of VCS for some access structures

Γ_{QM}	[28]	[6, 10, 37, 45]	[3]	[42]
$\{p_1, p_2\}$,$\{p_1, p_3\}$	1	2	2	2
$\{p_1, p_2\}$,$\{p_1, p_3\}$,$\{p_2, p_3\}$	1.6	4	3	3
$\{p_1, p_2, p_3\}$,$\{p_1, p_2, p_4\}$,$\{p_1, p_3, p_4\}$	1.5	8	6	6
$\{p_1, p_2, p_3\}$,$\{p_1, p_2, p_4\}$,$\{p_1, p_3, p_4\}$,$\{p_2, p_3, p_4\}$	2	32	6	6
$\{p_1, p_2, p_3, p_4\}$	1	8	8	8

SI, S_0 or S_1 are updated with a column permutation operation. The algorithm to generate $n \times m$ meaningful shares $Sh_{(u,j)}(g, h)$ from the $n \times (m-2)$ distinct cover images $COV_{(u,j)}(g, h)$ and a pair of complementary cover images (CV, IV) for the secret image SI is given below.

3.1.1 Share generation and distribution phase

Input :

1. Secret image SI which is of size $p \times q$
2. Set of $n \times (m-2)$ distinct cover images $\{COV_{(u,j)}(g, h) : 1 \leq u \leq n, 1 \leq j \leq (m-2), 1 \leq g \leq p, 1 \leq h \leq q\}$
3. A pair of complementary cover images (CV, IV), where $IV(g, h) = \overline{CV(g, h)}$
4. S_0 (resp. S_1) are the basis matrices of size $n \times m$ constructed from a perfect black general access structure scheme([6,7]) for sharing a 0 (resp. 1)

Algorithm :

For g = 1 to p
  For h = 1 to q
    For j = 1 to (m - 2)
      For u = 1 to n
        $D_{(u,j)} = \left[COV_{(u,j)}(g, h) \;\; H_{(u,j)}(g, h) \;\; COV_{(u,j)}(g, h) \right]$
      End
    End
  For u= 1 to n
    Set $D_{(u,m-1)} = \left[CV(g, h) \;\; H_{(u,m-1)}(g, h) \;\; CV(g, h) \right]$
    Set $D_{(u,m)} = \left[IV(g, h) \;\; H_{(u,m)}(g, h) \;\; IV(g, h) \right]$
  End
  Apply same column permutation, to all the $n \times m$, D matrices which is of size 1×3.
    For j = 1 to m
      For u = 1 to n
        For t = 1 to 3
          $Sh_{(u,j)}(g, h, t) = D_{(u,j)}(t)$
        End
      End
    End
  End
End

Output :

Set of $n \times m$ meaningful shares $\{Sh_{(u,j)} : 1 \leq u \leq n, 1 \leq j \leq m\}$ of size $p \times 3q$. The m meaningful shares $Sh_{(u,j)}$ are given to u^{th} participant.

3.1.2 Secret reconstruction phase

Using Praveen et al. [37] reconstruction algorithm generate the secret $RI(g, h) = \bigodot_{j=1}^{m} \bigotimes_{p_u \in A} Sh_{(u,j)}(g, h)$.

3.1.3 Analysis on the APE, contrast and security

This construction is based on the proper arrangement of first, second and third bit in the blocks $D_{(u,j)}$ which is of size 1×3. In the construction, same column permutation is applied for all D matrices corresponding to a secret pixel s in SI. Let us assume r_1, r_2, r_3 as random bits either 0 or 1 and $COV_{(u,j)}$, $CV(g,h)$, $IV(g,h)$ (inverted $CV(g,h)$) as meaningful cover images. Assign the second bit of all $D_{(u,j)}$ as $H_{(u,j)}$, the first and third bit are same as that of corresponding meaningful image. If m is the pixel expansion of a VCS, according to the algorithm m - 2 shares of u^{th} participant are generated using $COV_{(u,j)}$. During reconstruction phase corresponding to s, all the j^{th} $(D_{(u,j)})$ block of the qualified participants stacked(OR) together to generate j^{th} ($\begin{bmatrix} r_1 & r_2 & r_3 \end{bmatrix}$) block and when AND-ing all the j blocks, $\begin{bmatrix} 0 & s & 0 \end{bmatrix}$ is obtained corresponding to s in RI. The design rationale is $(m-1)^{th}$ meaningful share and m^{th} meaningful share of u^{th} participant are constructed using $CV(g,h)$ and $IV(g,h)$ respectively. In this construction all the n participants hold m shares and the pixel expansion in each share is 3. So **APE** for this EVCS is $\frac{3\times n\times m}{n}$, where m is the pixel expansion of a perfect black general access structure VCS. It is possible to construct a (t, k, n) - EVCS based on our PC1, when the inputs S_0 (resp. S_1) are basis matrices of size $n \times 2^t m_1$ constructed from a perfect black Guo et al. [19] - VCS, where m_1 is the pixel expansion of a perfect black (k - t, n - t) VCS. It is also possible to construct a $(1, k, n)$ - EVCS, when the inputs S_0 (resp. S_1) are basis matrices of size $n \times 2m_2$ constructed from a perfect black scheme of Arumugam et al. [4] - VCS, where m_2 is the pixel expansion of a perfect black (k - 1, n - 1) VCS. Arumugam et al. [4] - VCS is a special case of Guo et al. [19] - VCS. The APE for our (t, k, n) - EVCS constructed by using Guo et al. [19] - VCS is $\frac{3\times n\times (2^t\times m_1)}{n}$. The APE for our $(1, k, n)$ - EVCS constructed by using Arumugam et al. [4] - VCS is $\frac{3\times n\times (2\times m_2)}{n}$. Step construction based ($t = 1$, $k = 3$, $n = 4$) - VCS using XOR operation is shown in Example 2. In the construction same permutation is applied for all D matrices corresponding to a secret pixel in SI. For proving contrast and security we have not considered permutation of D matrices.

Proof of Contrast :

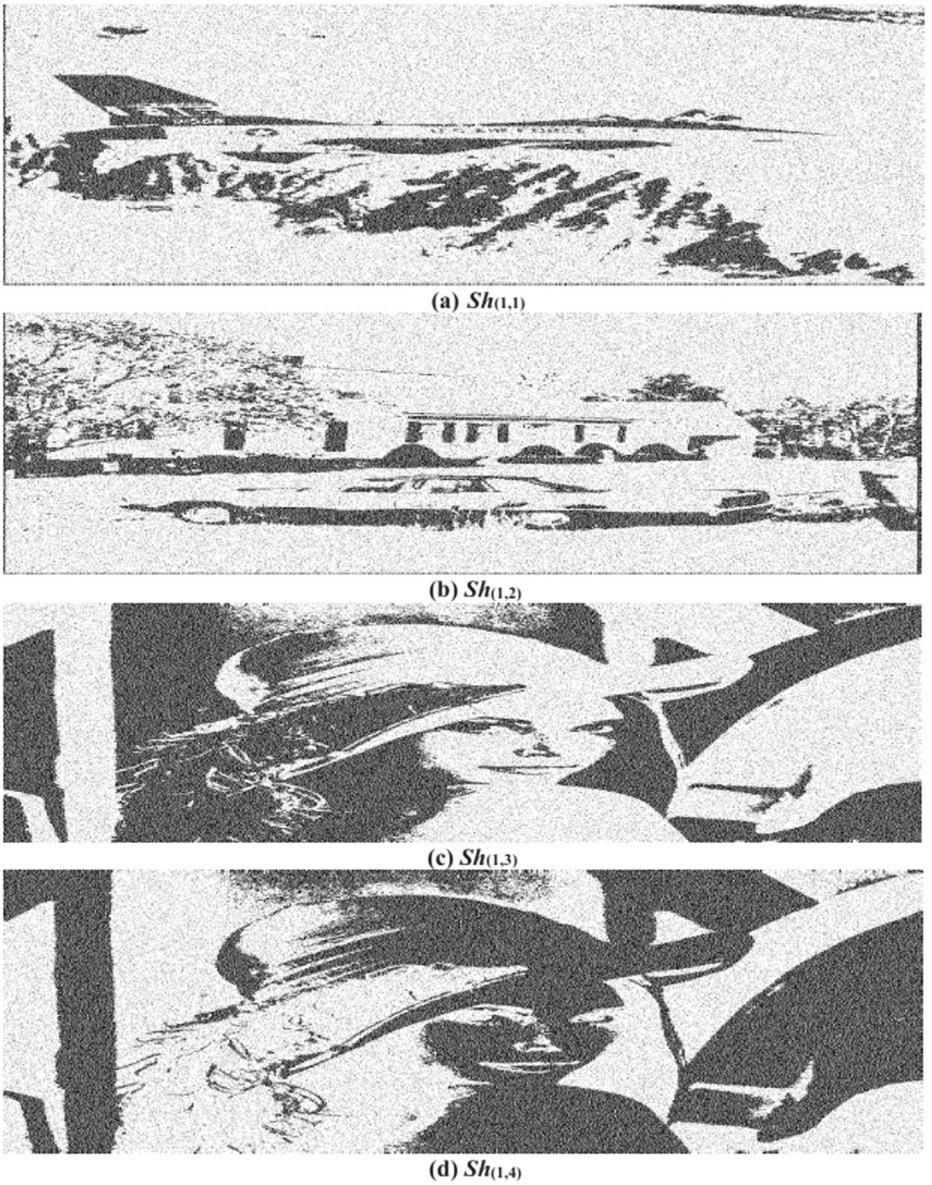
Let $\Omega_1(g,h) = \bigotimes_{p_u\in\Gamma_{QM}} Sh_{(u,1)}(g,h)$, $\Omega_2(g,h) = \bigotimes_{p_u\in\Gamma_{QM}} Sh_{(u,2)}(g,h)$, ..., $\Omega_{m-1}(g,h) = \bigotimes_{p_u\in\Gamma_{QM}} Sh_{(u,m-1)}(g,h)$, $\Omega_m(g,h) = \bigotimes_{p_u\in\Gamma_{QM}} Sh_{(u,m)}(g,h)$.

Let $RI(g,h) = \overset{z}{\underset{j=1}{\odot}} \Omega_j(g,h) \odot \Omega_{m-1}(g,h) \odot \Omega_m(g,h)$, where $z = m$ - 2= $\overset{z}{\underset{j=1}{\odot}} \Omega_j(g,h)$ $\odot \begin{bmatrix} \Omega_{m-1}(g,h) \odot \Omega_m(g,h) \end{bmatrix} = \overset{z}{\underset{j=1}{\odot}} \Omega_j(g,h) \odot \begin{bmatrix} 0 & (\Delta_{m-1}(g,h) \odot \Delta_m(g,h)) & 0 \end{bmatrix} =$ $\begin{bmatrix} 0 & \overset{m}{\underset{j=1}{\odot}} \Delta_j(g,h) & 0 \end{bmatrix} = \begin{bmatrix} 0 & SI(g,h) & 0 \end{bmatrix}$. When $SI = \begin{bmatrix} 1 & 0 \end{bmatrix}$, for $SI(0,0)$ the reconstructed $RI(0,0) = \begin{bmatrix} 0 & 1 & 0 \end{bmatrix}$ and for $SI(0,1)$ the reconstructed $RI(0,1) = \begin{bmatrix} 0 & 0 & 0 \end{bmatrix}$. Then relative contrast of reconstructed image RI is calculated as $\frac{\left(w\left(\begin{bmatrix} 0 & 1 & 0 \end{bmatrix}\right) - w\left(\begin{bmatrix} 0 & 0 & 0 \end{bmatrix}\right)\right)}{3} = 0.333$. This implies that when the participants in the qualified set join, the 0 and 1 pixel are distinguishable so that secret is revealed.

Proof of Security :

Generate $\Omega_1(g,h) = \bigotimes_{p_u\in\Gamma_{FM}} Sh_{(u,1)}(g,h)$, $\Omega_2(g,h) = \bigotimes_{p_u\in\Gamma_{FM}} Sh_{(u,2)}(g,h)$, ..., $\Omega_{m-1}(g,h) = \bigotimes_{p_u\in\Gamma_{FM}} Sh_{(u,m-1)}(g,h)$, $\Omega_m(g,h) = \bigotimes_{p_u\in\Gamma_{FM}} Sh_{(u,m)}(g,h)$. Here, when SI

=[1 0], for $SI(0, 0)$ the reconstructed $RI(0, 0) = [\,0\ 0\ 0\,]$ and for $SI(0, 1)$ the reconstructed $RI(0, 1) = [\,0\ 0\ 0\,]$. Then relative contrast of reconstructed image RI is calculated as $\frac{(w([\,0\ 0\ 0\,])-w([\,0\ 0\ 0\,]))}{3} = 0$ and this implies that when the participants in the forbidden set join, the 0 and 1 pixel are indistinguishable so that secret cannot be revealed.



(a) $Sh_{(1,1)}$

(b) $Sh_{(1,2)}$

(c) $Sh_{(1,3)}$

(d) $Sh_{(1,4)}$

Fig. 4 Meaningful share images of participant p_1 for (2, 3) PC1-EVCS

Proof of Contrast for meaningful shares :

According to the construction when $H_{(u,j)}(g,h) = 0$ and $COV_{(u,j)}(g,h) = 0$, then $Sh_{(u,j)}(g,h) = \begin{bmatrix} 0 & 0 & 0 \end{bmatrix}$, when $H_{(u,j)}(g,h) = 0$ and $COV_{(u,j)}(g,h) = 1$, then $Sh_{(u,j)}(g,h) = \begin{bmatrix} 1 & 0 & 1 \end{bmatrix}$, when $H_{(u,j)}(g,h) = 1$ and $COV_{(u,j)}(g,h) = 0$, then $Sh_{(u,j)}(g,h) = \begin{bmatrix} 0 & 1 & 0 \end{bmatrix}$, when

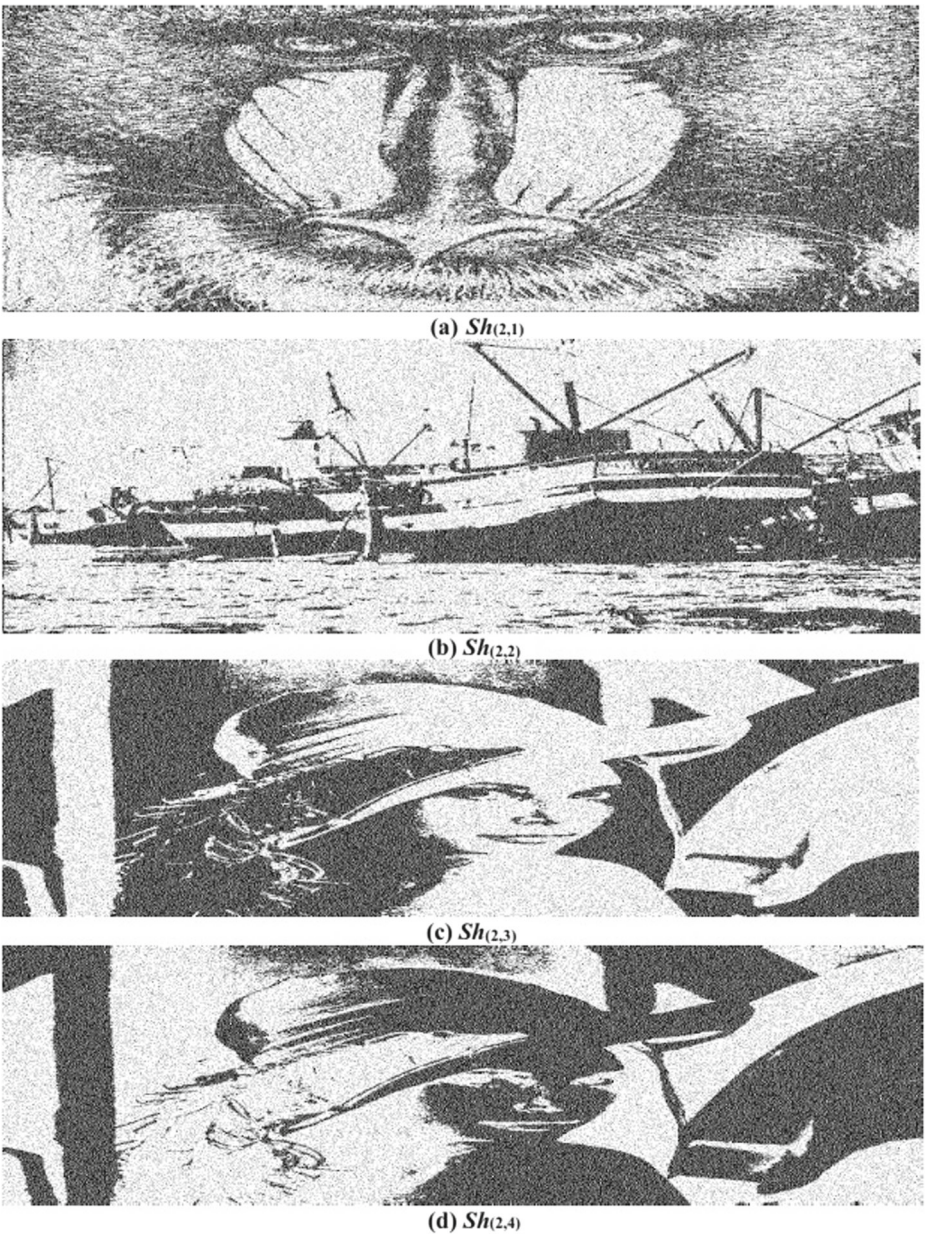
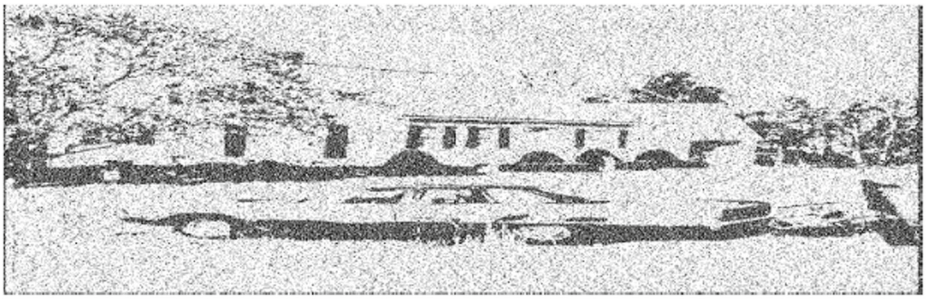
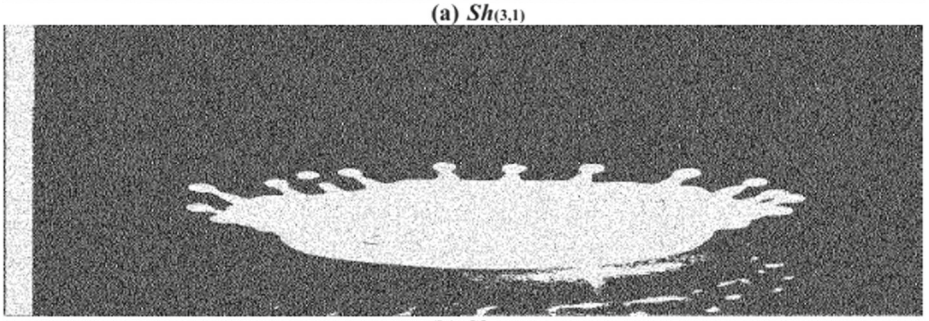


Fig. 5 Meaningful share images of participant p_2 for (2, 3) PC1-EVCS

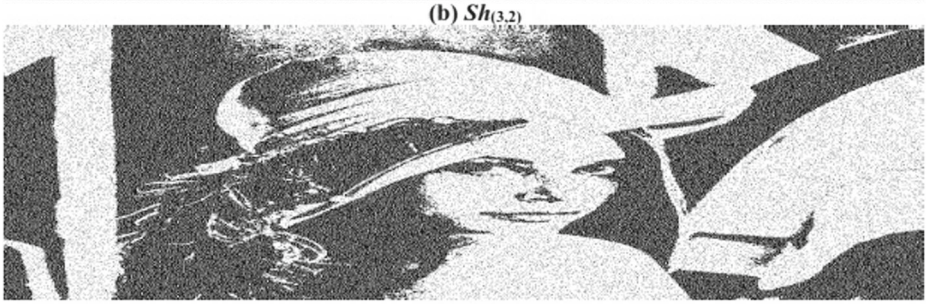
$H_{(u,j)}(g,h) = 1$ and $COV_{(u,j)}(g,h) = 1$, then $Sh_{(u,j)}(g,h) = \begin{bmatrix} 1 & 1 & 1 \end{bmatrix}$. So $W(\begin{bmatrix} 0 & 0 & 0 \end{bmatrix}) < W(\begin{bmatrix} 0 & 1 & 0 \end{bmatrix}) < W(\begin{bmatrix} 1 & 0 & 1 \end{bmatrix}) < W(\begin{bmatrix} 1 & 1 & 1 \end{bmatrix})$ which implies that the contrast of the cover images is preserved in the meaningful shares. The contrast value will range from 1 to 3. So



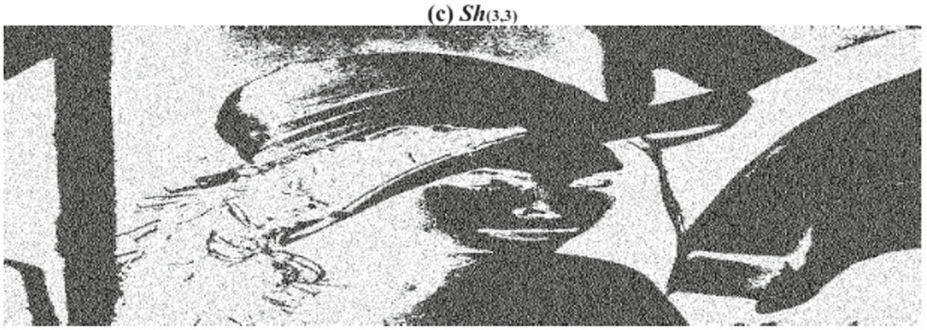
(a) $Sh_{(3,1)}$



(b) $Sh_{(3,2)}$



(c) $Sh_{(3,3)}$



(d) $Sh_{(3,4)}$

Fig. 6 Meaningful share images of participant p_3 for (2, 3) PC1-EVCS

the ratio of cover pixel (resp. secret information pixel) preserved in a block of size 1×3 of the meaningful share is 0.666 (resp. 0.333).

Example 3 Let $P = \{p_1, p_2, p_3\}$ be the set of participants, $\Gamma_{QM} = \{\{p_1, p_2\}, \{p_1, p_3\}, \{p_2, p_3\}\}$ and $\Gamma_{FM} = \{\{p_1\}, \{p_2\}, \{p_3\}\}$. Let $SI = \begin{bmatrix} 1 & 0 \end{bmatrix}$, $S_0 = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix}$ and $S_1 = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{bmatrix}$. The cover images used for creating meaningful shares are $COV_{(1,1)} = \begin{bmatrix} 0 & 0 \end{bmatrix}$, $COV_{(1,2)} = \begin{bmatrix} 0 & 1 \end{bmatrix}$, $COV_{(1,3)} = \begin{bmatrix} 1 & 1 \end{bmatrix}$, $COV_{(1,4)} = \overline{COV_{(1,3)}}$, $COV_{(2,1)} = \begin{bmatrix} 1 & 0 \end{bmatrix}$, $COV_{(2,2)} = \begin{bmatrix} 1 & 1 \end{bmatrix}$, $COV_{(2,3)} = COV_{(1,3)}$, $COV_{(2,4)} = \overline{COV_{(1,3)}}$, $COV_{(3,1)} = \begin{bmatrix} 0 & 1 \end{bmatrix}$, $COV_{(3,2)} = \begin{bmatrix} 0 & 0 \end{bmatrix}$, $COV_{(3,3)} = COV_{(1,3)}$, $COV_{(3,4)} = \overline{COV_{(1,3)}}$. The constructed H matrices are $H_{(1,1)} = \begin{bmatrix} 0 & 0 \end{bmatrix}$, $H_{(1,2)} = \begin{bmatrix} 1 & 1 \end{bmatrix}$, $H_{(1,3)} = \begin{bmatrix} 1 & 1 \end{bmatrix}$, $H_{(1,4)} = \begin{bmatrix} 1 & 1 \end{bmatrix}$, $H_{(2,1)} = \begin{bmatrix} 1 & 0 \end{bmatrix}$, $H_{(2,2)} = \begin{bmatrix} 0 & 1 \end{bmatrix}$, $H_{(2,3)} = \begin{bmatrix} 1 & 1 \end{bmatrix}$, $H_{(2,4)} = \begin{bmatrix} 1 & 1 \end{bmatrix}$, $H_{(3,1)} = \begin{bmatrix} 1 & 0 \end{bmatrix}$, $H_{(3,2)} = \begin{bmatrix} 1 & 1 \end{bmatrix}$, $H_{(3,3)} = \begin{bmatrix} 0 & 1 \end{bmatrix}$, $H_{(3,4)} = \begin{bmatrix} 1 & 1 \end{bmatrix}$. Then the constructed meaningful shares are $Sh_{(1,1)} = \begin{bmatrix} 000 & 000 \end{bmatrix}$, $Sh_{(1,2)} = \begin{bmatrix} 010 & 111 \end{bmatrix}$, $Sh_{(1,3)} = \begin{bmatrix} 111 & 111 \end{bmatrix}$, $Sh_{(1,4)} = \begin{bmatrix} 010 & 010 \end{bmatrix}$, $Sh_{(2,1)} = \begin{bmatrix} 111 & 000 \end{bmatrix}$, $Sh_{(2,2)} = \begin{bmatrix} 101 & 111 \end{bmatrix}$, $Sh_{(2,3)} = \begin{bmatrix} 111 & 111 \end{bmatrix}$, $Sh_{(2,4)} = \begin{bmatrix} 010 & 010 \end{bmatrix}$, $Sh_{(3,1)} = \begin{bmatrix} 010 & 101 \end{bmatrix}$, $Sh_{(3,2)} = \begin{bmatrix} 010 & 010 \end{bmatrix}$, $Sh_{(3,3)} = \begin{bmatrix} 101 & 111 \end{bmatrix}$, $Sh_{(3,4)} = \begin{bmatrix} 010 & 010 \end{bmatrix}$. Same column permutations are applied to all Sh matrices corresponding to a single pixel in SI. According to this construction $RI = \begin{bmatrix} 010 & 000 \end{bmatrix}$. Thus relative contrast of reconstructed image is 0.333 and APE = 12. Figs. 4 , 5 , 6 and 7 shows the experimental results for this Example.

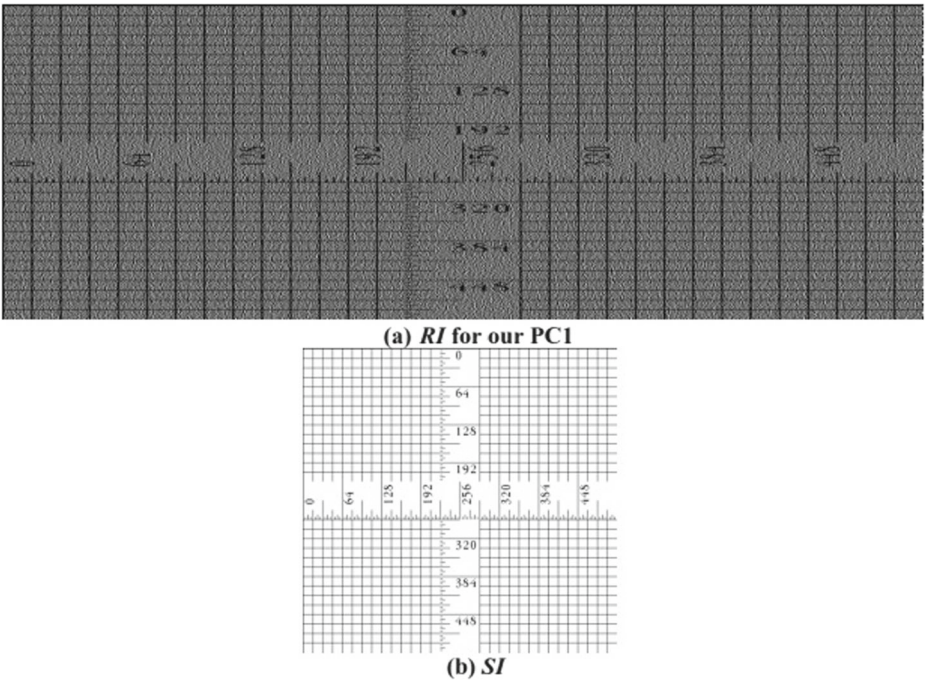


Fig. 7 Secret image and Reconstructed image in the case of (2, 3) PC1-EVCS

3.2 Proposed Construction (PC2)

Initially, generate $\{H_{(u,j)} : 1 \leq u \leq n, 1 \leq j \leq N_u\}$ by XOR step construction [28] for VCS given in share generation phase of Section 2.3. The algorithm to generate $(N_u + 1)$ meaningful shares from $\{H_{(u,j)} : 1 \leq u \leq n, 1 \leq j \leq N_u\}$ for each u^{th} participant is given below.

3.2.1 Share generation and distribution phase

Input :

1. Secret image SI of size $p \times q$
2. Set of distinct cover images $\{COV_{(u,j)}(g, h) : 1 \leq u \leq n, 1 \leq j \leq N_u, 1 \leq g \leq p, 1 \leq h \leq q\}$

Algorithm :

For $u = 1$ to n
  Assign R_u = A randomly selected number from 1 to N_u
End
For $g = 1$ to p
  For $h = 1$ to q
    For $j = 1$ to N_u
      For $u = 1$ to n
        $D_{(u,j)} = \left[COV_{(u,j)}(g, h) \;\; H_{(u,j)}(g, h) \;\; COV_{(u,j)}(g, h) \right]$
      End
    End
    For $u = 1$ to n
      Set $D_{(u,(N_u+1))} = \left[D_{(u,R_u)}(1) \;\; \overline{D_{(u,R_u)}(2)} \;\; D_{(u,R_u)}(3) \right]$
    End
    For $j = 1$ to $(N_u + 1)$
      For $u = 1$ to n
        Apply same column permutation to all the D matrices which are of size 1×3.
        For $t = 1$ to 3
          $Sh_{(u,j)}(g, h, t) = D_{(u,j)}(t)$
        End
      End
    End
  End
End

Output:

Set of meaningful shares, $\{Sh_{(u,j)} : 1 \leq u \leq n, 1 \leq j \leq (N_u + 1)\}$ which are of size $p \times 3q$. The $(N_u + 1)$ meaningful shares, $Sh_{(u,j)}$ are given to u^{th} participant.

3.2.2 *Secret reconstruction phase* [28]

Let $A = \{i_1, i_2, ..., i_p\} \in \Gamma_{QM}$. Assume the shares carried by the participant i_p are $Sh_{(i_p,j)}$, where $1 \leq j \leq Ni_p$. Here Ni_p denotes the number of shares carried by the participant i_p.

For j_1 =1 to Ni_1

  For j_2 =1 to Ni_2

    .

    .

    For j_p =1 to Ni_p

      $O_{(j_1,j_2,.....,j_p)}(g, h) = Sh_{(i_1,j_1)} \bigoplus Sh_{(i_2,j_2)} \bigoplus .....\bigoplus Sh_{(i_{p-1},j_{p-1})} \bigoplus Sh_{(i_p,j_p)}$.

    End

    .

    .

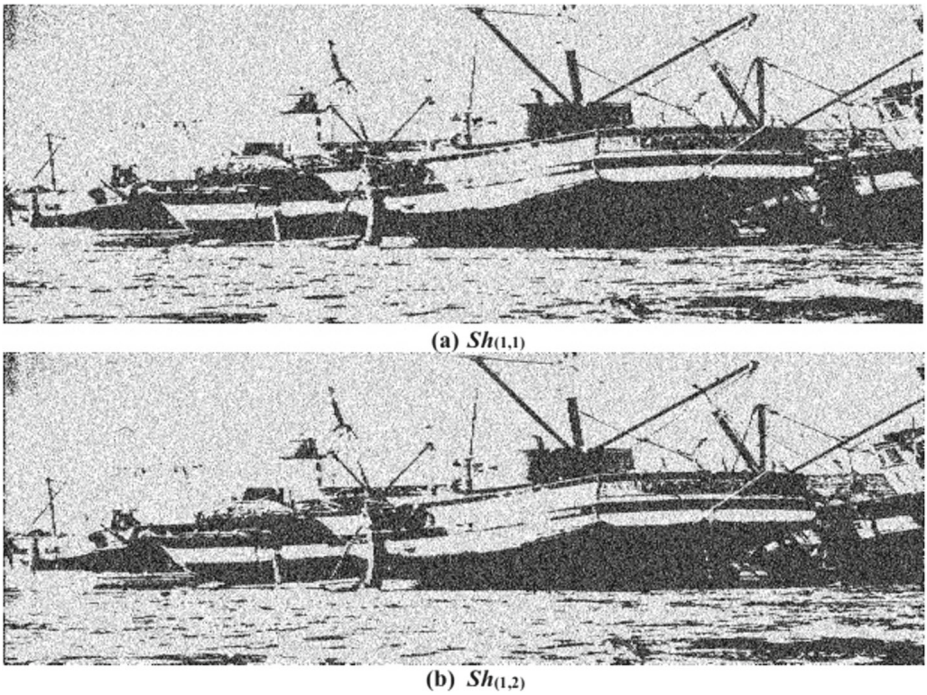
  End

End

Here only one $OI(g, h)$ from the set of all $O_{(j_1,j_2,.....,j_p)}(g, h)$ will be used to generate $RI(g, h)$. So, each u^{th} participant in Γ_{QM} generates the secret, $RI(g, h) = OI(g, h) \bigodot (Sh_{(u,(N_u+1))} \bigoplus Sh_{(u,R_u)})$.

3.2.3 *Analysis on the APE, contrast and security*

This construction is based on the proper arrangement of first, second and third bit in the blocks $D_{(u,j)}$ which is of size 1×3. In the construction same column permutation is applied

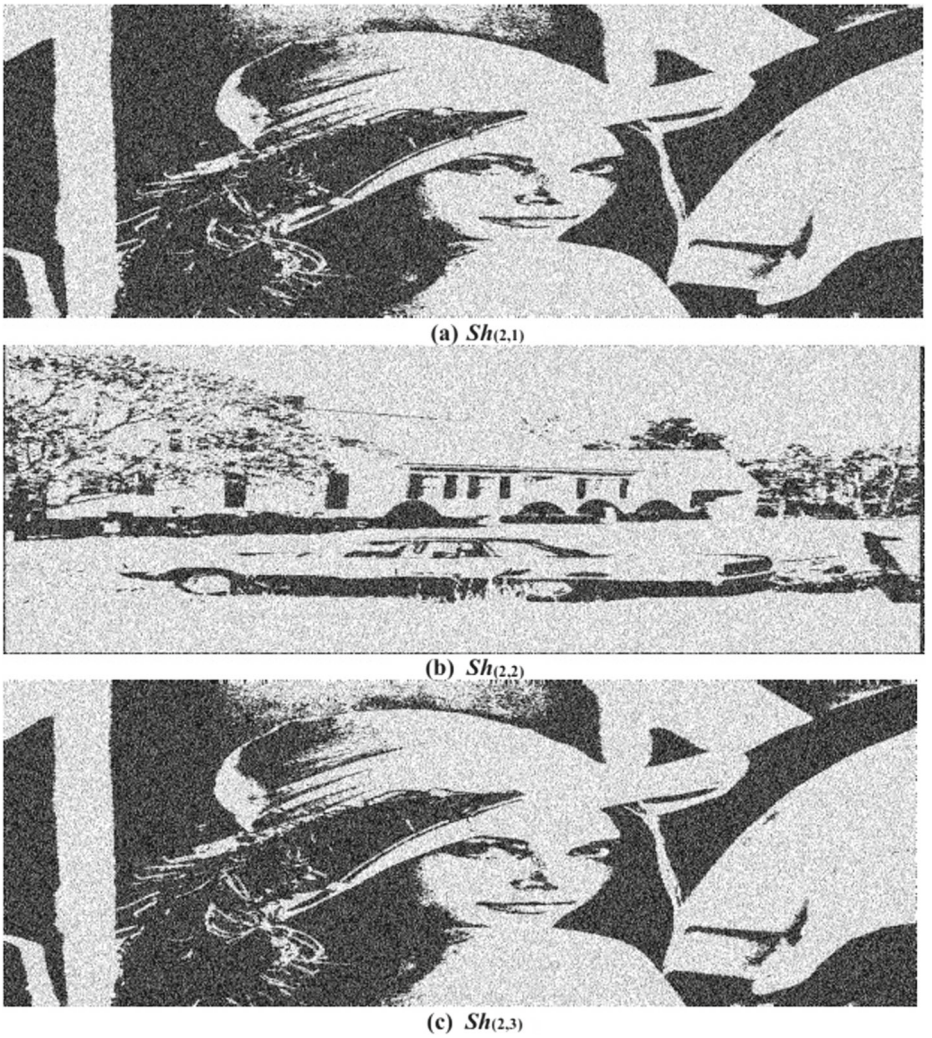


(a) $Sh_{(1,1)}$

(b) $Sh_{(1,2)}$

Fig. 8 Meaningful share images of participant p_1 for (2, 3) PC2-EVCS

for all D matrices corresponding to a secret pixel s in SI. Let us assume r_1, r_2, r_3 as random bits either 0 or 1 and $\{COV_{(u,j)} : 1 \leq u \leq n, 1 \leq j \leq N_u\}$ be the set of distinct cover images. Assign the second bit of all $D_{(u,j)}$ as $H_{(u,j)}$, the first and third bit are same as that of corresponding $\{COV_{(u,j)}\}$. During reconstruction phase, when XOR-ing $D_{(u,j)}$ blocks of the qualified participants $\begin{bmatrix} r_1 & s & r_3 \end{bmatrix}$ block is generated. Then $\begin{bmatrix} 0 & s & 0 \end{bmatrix}$ block corresponding to s in RI is generated when AND-ing $\begin{bmatrix} r_1 & s & r_3 \end{bmatrix}$ with $\begin{bmatrix} 0 & 1 & 0 \end{bmatrix}$. Each u^{th} participant can generate $\begin{bmatrix} 0 & 1 & 0 \end{bmatrix}$ block by XOR-ing $D_{(u,(N_u+1))}$ with $D_{(u,R_u)}$ because the first and the third bit of blocks $D_{(u,(N_u+1))}$ and $D_{(u,R_u)}$ are generated using same cover image $COV_{(u,R_u)}$. Here each i^{th} participant in P holds (N_i+1) shares, so **APE** for this step construction based EVCS is $\frac{3\times\left(\sum_{i=1}^{n} N_i+n\right)}{n}$.



(a) $Sh_{(2,1)}$

(b) $Sh_{(2,2)}$

(c) $Sh_{(2,3)}$

Fig. 9 Meaningful share images of participant p_2 for (2, 3) PC2-EVCS

Proof of Contrast :

Consider the case of (n, n) access structure, where $OI(g, h) = Sh_{(i_1,1)} \bigoplus Sh_{(i_2,1)} \bigoplus ..... \bigoplus Sh_{(i_{p-1},1)} \bigoplus Sh_{(i_p,1)}$, $\{i_1, i_2, ..., i_p\} \in \Gamma_{QM}$. Let us denote the following

$b_1 = \bigoplus_{p_u \in \Gamma_{QM}} COV_{(u,1)}(g, h)$

$Sh_{(u,R_u)}(g, h) = \left[COV_{(u,R_u)}(g, h) \;\; H_{(u,R_u)}(g, h) \;\; COV_{(u,R_u)}(g, h) \right]$

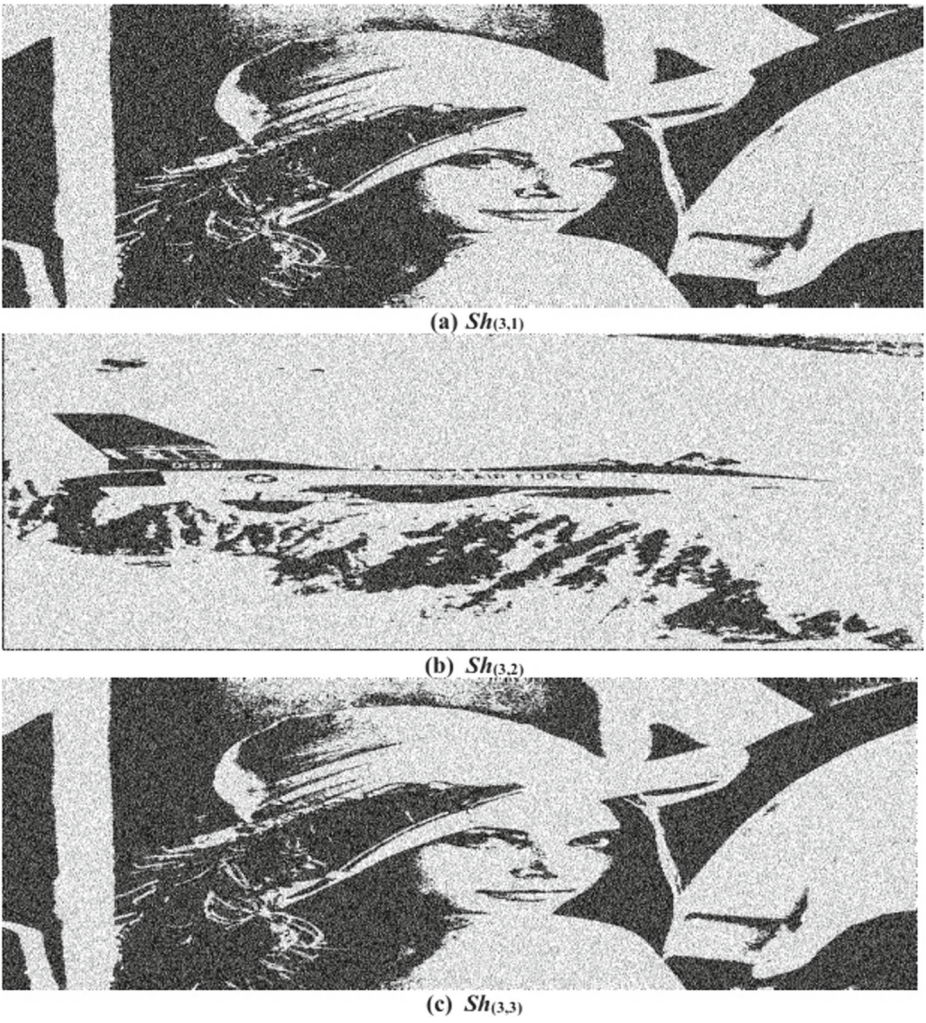
$Sh_{(u,(N_u+1))}(g, h) = \left[COV_{(u,R_u)}(g, h) \;\; \overline{H_{(u,R_u)}(g, h)} \;\; COV_{(u,R_u)}(g, h) \right]$

$RI(g, h) = OI(g, h) \bigodot (Sh_{(u,(N_u+1))}(g, h) \bigoplus Sh_{(u,R_u)}(g, h))$

$= \left[b_1 \;\; SI(g, h) \;\; b_1 \right] \bigodot \left[0 \;\; 1 \;\; 0 \right]$

$= \left[0 \;\; SI(g, h) \;\; 0 \right]$.

When $SI = \left[1 \;\; 0 \right]$, for $SI(0, 0)$ reconstructed pixel $RI(0, 0) = \left[b_1 \;\; 1 \;\; b_1 \right] \bigodot \left[0 \;\; 1 \;\; 0 \right] = \left[0 \;\; 1 \;\; 0 \right]$ and for $SI(0, 1)$ reconstructed $RI(0, 1) = \left[b_1 \;\; 0 \;\; b_1 \right] \bigodot \left[0 \;\; 1 \;\; 0 \right] = \left[0 \;\; 0 \;\; 0 \right]$. So the



(a) $Sh_{(3,1)}$

(b) $Sh_{(3,2)}$

(c) $Sh_{(3,3)}$

Fig. 10 Meaningful share images of participant p_3 for (2, 3) PC2-EVCS

relative contrast of the reconstructed image RI is calculated as $\frac{\left(w\left(\left[\begin{array}{ccc}0&1&0\end{array}\right]\right)-w\left(\left[\begin{array}{ccc}0&0&0\end{array}\right]\right)\right)}{3}$ = 0.333. This implies that when the participants in the qualified set join, the 0 and 1 pixel are distinguishable so that secret is revealed.

In Figs. 8, 9 and 10 $(Sh_{(1,1)}, Sh_{(1,2)})$, $(Sh_{(2,1)}, Sh_{(2,3)})$ and $(Sh_{(3,1)}, Sh_{(3,3)})$ are the similar cover shares held by participants p_1, p_2 and p_3 respectively for (2, 3) - EVCS.

Proof of Security:

Here, for $SI = \left[\begin{array}{cc}1&0\end{array}\right]$, when $\{i_1, i_2, ..., i_p\} \in \Gamma_{FM}$, for $SI(0, 0)$ (resp. $SI(0, 1)$) the intermediate pixels $OI(0, 0)$ (resp. $OI(0, 1)$) is $\left[\begin{array}{ccc}b_1&0&b_1\end{array}\right]$, the reconstructed pixels $RI(0, 0)$ (resp. $RI(0, 1)$) is $\left[\begin{array}{ccc}b_1&0&b_1\end{array}\right] \odot \left[\begin{array}{ccc}0&1&0\end{array}\right] = \left[\begin{array}{ccc}0&0&0\end{array}\right]$. So the relative contrast is calculated as $\frac{\left(w\left(\left[\begin{array}{ccc}0&0&0\end{array}\right]\right)-w\left(\left[\begin{array}{ccc}0&0&0\end{array}\right]\right)\right)}{3} = 0$. This provides a 0 contrast and implies that when the participants in the forbidden set join, the 0 and 1 pixel are indistinguishable so that secret cannot be revealed.

Proof of Contrast for meaningful shares:

According to the construction when $H_{(u,j)}(g, h) = 0$ and $COV_{(u,j)}(g, h) = 0$, then $Sh_{(u,j)}(g, h) = \left[\begin{array}{ccc}0&0&0\end{array}\right]$, when $H_{(u,j)}(g, h) = 0$ and $COV_{(u,j)}(g, h) = 1$, then $Sh_{(u,j)}(g, h) = \left[\begin{array}{ccc}1&0&1\end{array}\right]$, when $H_{(u,j)}(g, h) = 1$ and $COV_{(u,j)}(g, h) = 0$, then $Sh_{(u,j)}(g, h) = \left[\begin{array}{ccc}0&1&0\end{array}\right]$, when $H_{(u,j)}(g, h) = 1$ and $COV_{(u,j)}(g, h) = 1$, then $Sh_{(u,j)}(g, h) = \left[\begin{array}{ccc}1&1&1\end{array}\right]$. So $W\left(\left[\begin{array}{ccc}0&0&0\end{array}\right]\right) < W\left(\left[\begin{array}{ccc}0&1&0\end{array}\right]\right) < W\left(\left[\begin{array}{ccc}1&0&1\end{array}\right]\right) < W\left(\left[\begin{array}{ccc}1&1&1\end{array}\right]\right)$ which implies that the contrast of the cover images is preserved in the meaningful shares. The contrast value will range from 1 to 3. So the ratio of cover

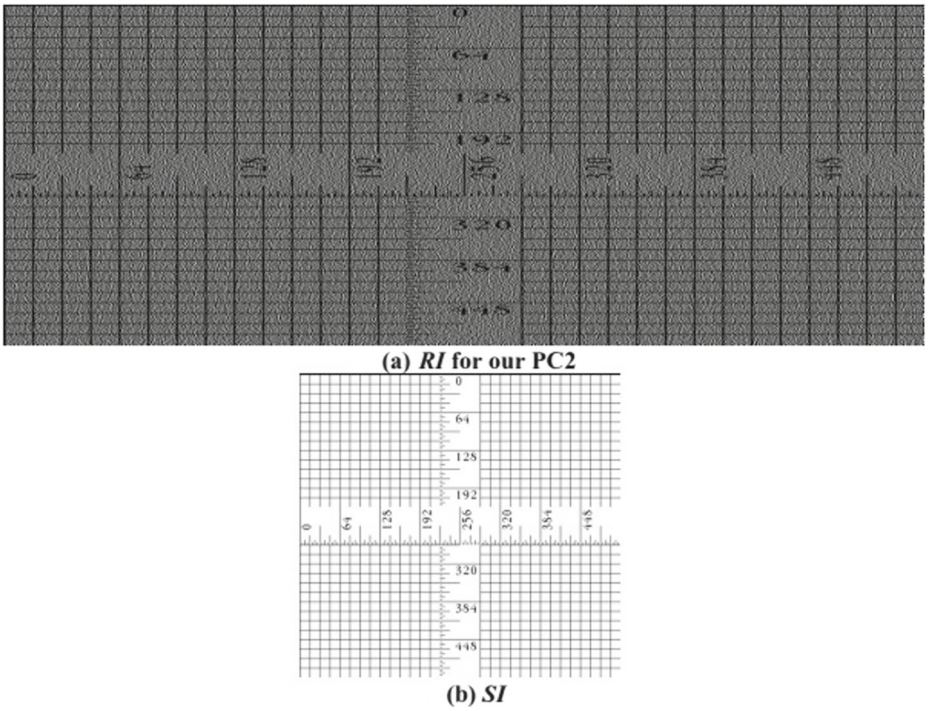


Fig. 11 Secret image and Reconstructed image in the case of (2, 3) PC2-EVCS

pixel (resp. secret information pixel) preserved in a block of size 1×3 of the meaningful share is 0.666 (resp. 0.333).

Example 4 Consider same P, Γ_{QM}, Γ_{FM}, SI as given in Example 1. Let $R_u = \{1, 2, 1\}$. The cover images used are $COV_{(1,1)} = \begin{bmatrix} 0 & 0 \end{bmatrix}$, $COV_{(1,2)} = COV_{(1,1)}$, $COV_{(2,1)} = \begin{bmatrix} 1 & 0 \end{bmatrix}$, $COV_{(2,2)} = \begin{bmatrix} 1 & 1 \end{bmatrix}$, $COV_{(2,3)} = COV_{(2,2)}$, $COV_{(3,1)} = \begin{bmatrix} 0 & 1 \end{bmatrix}$, $COV_{(3,2)} = \begin{bmatrix} 0 & 0 \end{bmatrix}$, $COV_{(3,3)} = COV_{(3,1)}$. The constructed H matrices are $H_{(1,1)} = \begin{bmatrix} 0 & 1 \end{bmatrix}$, $H_{(2,1)} = \begin{bmatrix} 1 & 1 \end{bmatrix}$, $H_{(2,2)} = \begin{bmatrix} 1 & 0 \end{bmatrix}$, $H_{(3,1)} = \begin{bmatrix} 1 & 1 \end{bmatrix}$, $H_{(3,2)} = \begin{bmatrix} 0 & 0 \end{bmatrix}$. Then the constructed meaningful shares with APE $= \frac{(3+3)+(3+3+3)+(3+3+3)}{3} = 8$ are $Sh_{(1,1)} = \begin{bmatrix} 000 & 010 \end{bmatrix}$, $Sh_{(1,2)} = \begin{bmatrix} 010 & 000 \end{bmatrix}$, $Sh_{(2,1)} = \begin{bmatrix} 111 & 010 \end{bmatrix}$, $Sh_{(2,2)} = \begin{bmatrix} 111 & 101 \end{bmatrix}$, $Sh_{(2,3)} = \begin{bmatrix} 101 & 111 \end{bmatrix}$, $Sh_{(3,1)} = \begin{bmatrix} 010 & 111 \end{bmatrix}$, $Sh_{(3,2)} = \begin{bmatrix} 000 & 000 \end{bmatrix}$, $Sh_{(3,3)} = \begin{bmatrix} 000 & 101 \end{bmatrix}$. Same column permutations are applied to all Sh matrices corresponding to a single pixel in SI. After reconstruction $RI = \begin{bmatrix} 010 & 000 \end{bmatrix}$ with $\alpha = 0.330$. Figs. 8 , 9 , 10 and 11 shows the experimental results for this example.

3.3 Comparison with related works

There are plenty of deterministic and probabilistic schemes applicable for Binary/Gray/Color images available in the literature. The reconstruction operations for these schemes are Stacking(OR) and XOR operation. Each participant may hold Single/Multiple meaningful shares based on the construction. In Halftone VCS [27, 63], a

Table 2 Review of different EVCS construction

Scheme	APE	Operations	*SPP*	Γ
PC1	Yes	OR with AND	Multiple	General
PC2	Yes	XOR with AND	Multiple	General
Ateniese et al. [5]	Yes	OR	Single	General
Liu et al. [27]	Yes	OR	Single	General
Zhou et al. [63]	Yes	OR	Multiple	General
Wang et al. [48]	Yes	OR	Single	General
Wang et al. [46]	Yes	OR	Single	(k, n)
Yang et al. [62]	Yes	OR	Single	(n, n),(k, n)
Yan et al. [56]	Yes	OR	Single	General
Lu et al. [31]	Yes	OR	Single	$(2, n)$
Kang et al. [20]	Yes	OR	Single	(k, n)
Yang et al. [59]	Yes	OR	Single	General
Lee et al. [22]	No	OR	Single	General
Guo et al. [18]	No	OR	Single	(n, n)
Chiu et al. [9]	No	OR	Single	(k, n)
Ou et al. [36]	No	XOR	Single	(n, n)
Yan et al. [55]	No	OR	Single	(k, n)
Wang et al. [47]	No	OR	Single	(k, n)
Yan et al. [54]	No	OR	Single	$(2, 2)$
Lathif et al. [15]	No	OR	Single	(k, n)
Shyu et al. [41]	No	OR	Single	(k, n)
Ou et al. [35]	No	XOR	Single	$(2, infinity)$
Shivani et al. [39]	No	OR	Single	$(2, 2)$

Table 3 Comparison for (2, 3) - EVCS

Scheme	APE	α	N_i	$Size_i$	#OR	#AND	#XOR
Ateniese et al. [5]	7	0.140	1, 1, 1	7	7	0	0
Liu et al. [27]	16	0.062	1, 1, 1	16	16	0	0
Zhou et al. [63]	26.63	0.062	1, 2, 2	16	16(or 32)	0	0
Wang et al. [48]	12	0.083	1, 1, 1	12	12	0	0
Wang et al. [46]	7	0.140	1, 1, 1	7	7	0	0
Yang et al. [62]	16	0.062	1, 1, 1	16	16	0	0
Yan et al. [56]	16	0.062	1, 1, 1	16	16	0	0
Lu et al. [31]	15	0.066	1, 1, 1	15	15	0	0
PC1	21	0.333	7, 7, 7	3	21	18	0
PC2	8	0.333	2, 3, 3	3	0	3(or 6)	6(or 12)

Table 4 Comparison for (1, 3, 4) - deterministic schemes

Scheme	APE	α	N_i	$Size_i$	Share Type
Arumugam et al. [4]	6	0.160	1, 1, 1, 1	6	Random
Adhikari et al. [3]	6	0.160	1, 1, 1, 1	6	Random
Ateniese et al. [5]	10	0.100	1, 1, 1, 1	10	Meaningful
Liu et al. [27]	16	0.062	1, 1, 1, 1	16	Meaningful
Zhou et al. [63]	24	0.062	1, 1, 2, 2	16	Meaningful
Wang et al. [48]	16	0.062	1, 1, 1, 1	16	Meaningful
Yan et al. [56]	16	0.062	1, 1, 1, 1	16	Meaningful
PC1	18	0.333	6, 6, 6, 6	3	Meaningful
PC2	7.50	0.333	2, 2, 3, 3	3	Meaningful

Table 5 Comparison for (2, 4, 5) - deterministic schemes

Scheme	APE	α	N_i	$Size_i$	Share Type
Guo et al. [19]	12	0.083	1, 1, 1, 1, 1	12	Random
Dutta et al. [14]	12	0.083	1, 1, 1, 1, 1	12	Random
Ateniese et al. [5]	18	0.055	1, 1, 1, 1, 1	18	Meaningful
Liu et al. [27]	25	0.040	1, 1, 1, 1, 1	25	Meaningful
Zhou et al. [63]	22.4	0.062	1, 1, 1, 2, 2	25	Meaningful
Wang et al. [48]	32	0.031	1, 1, 1, 1, 1	32	Meaningful
Yan et al. [56]	32	0.031	1, 1, 1, 1, 1	32	Meaningful
PC1	36	0.330	12, 12, 12, 12	3	Meaningful
PC2	7.20	0.330	2, 2, 2, 3, 3	3	Meaningful

single secret pixel is encoded with a halftone cell size which is selected based on the access structure and the number of participants. In order to avoid image distortion (maintain the aspect ratio) during halftoning process, halftone cell size is selected as square number

Table 6 Comparison for (k, n) access structure

(k, n)	[5] (APE, α)	[46] (APE, α)	[48, 56] (APE, α)	PC1(APE, α)
(2, 3)	(5, 1/5)	($\geq$ 5, $\leq$ 1/5)	($\geq$ 6, $\leq$ 1/6)	(9, 1/3)
(2, 4)	(6, 1/6)	($\geq$ 6, $\leq$ 1/6)	($\geq$ 8, $\leq$1/8)	(12, 1/3)
(2, 5)	(7, 1/7)	($\geq$7, $\leq$ 1/7)	($\geq$ 10, $\leq$ 1/10)	(15, 1/3)
(2, 6)	(8, 1/8)	($\geq$8, $\leq$ 1/8)	($\geq$ 12, $\leq$ 1/12)	(18, 1/3)
(2, 7)	(9, 1/9)	($\geq$9, $\leq$ 1/9)	($\geq$14, $\leq$ 1/14)	(21, 1/3)
(2, 8)	(10, 1/10)	($\geq$10, $\leq$ 1/10)	($\geq$ 16, $\leq$ 1/16)	(24, 1/3)
(2, 9)	(11, 1/11)	($\geq$11, $\leq$ 1/11)	($\geq$ 18, $\leq$ 1/18)	(27, 1/3)
(2, 10)	(12, 1/12)	($\geq$12, $\leq$ 1/12)	($\geq$ 20, $\leq$ 1/20)	(30, 1/3)
(3, 4)	(11, 1/11)	($\geq$11, $\leq$ 1/11)	($\geq$ 18, $\leq$ 1/18)	(27, 1/3)
(3, 5)	(19, 1/19)	($\geq$19, $\leq$ 1/19)	($\geq$ 32, $\leq$ 1/32)	(48, 1/3)
(4, 5)	(27, 1/27)	($\geq$27, $\leq$ 1/27)	($\geq$ 50, $\leq$ 1/50)	(75, 1/3)
(3, 6)	(28, 1/28)	($\geq$28, $\leq$ 1/28)	($\geq$ 50, $\leq$ 1/50)	(75, 1/3)
(4, 6)	(58, 1/58)	($\geq$58, $\leq$ 1/58)	($\geq$ 112, $\leq$ 1/112)	(168, 1/3)
(5, 6)	(67, 1/67)	($\geq$67, $\geq$ 1/67)	($\geq$ 130, $\leq$ 1/130)	(195, 1/3)
(3, 7)	(40, 1/40)	($\geq$40, $\leq$ 1/40)	($\geq$ 72, $\leq$ 1/72)	(108, 1/3)
(4, 7)	(108, 1/108)	($\geq$108, $\leq$ 1/108)	($\geq$ 210, $\leq$ 1/210)	(315, 1/3)
(5, 7)	(178, 1/178)	($\geq$178, $\leq$ 1/178)	($\geq$ 352, $\leq$ 1/352)	(528, 1/3)
(6, 7)	(163, 1/163)	($\geq$163, $\leq$ 1/163)	($\geq$ 322,$\leq$ 1/322)	(483, 1/3)
(3, 8)	(53, 1/53)	($\geq$53, $\leq$ 1/53)	($\geq$ 98, $\leq$ 1/98)	(147, 1/3)
(4, 8)	(179, 1/179)	($\geq$179, $\leq$ 1/179)	($\geq$ 352, $\leq$ 1/352)	(528, 1/3)
(5, 8)	(387, 1/387)	($\geq$387, $\leq$ 1/387)	($\geq$ 770, $\leq$ 1/770)	(1155, 1/3)
(6, 8)	(514, 1/514)	($\geq$514, $\leq$ 1/514)	($\geq$ 1024, $\leq$ 1/1024)	(1536, 1/3)
(7, 8)	(387, 1/387)	($\geq$387, $\leq$ 1/387)	($\geq$ 770, $\leq$ 1/770)	(1155, 1/3)
(3, 9)	(69, 1/69)	($\geq$69, $\leq$ 1/69)	($\geq$ 128, $\leq$ 1/128)	(192, 1/3)
(4, 9)	(276, 1/276)	($\geq$276, $\leq$ 1/276)	($\geq$ 546, $\leq$ 1/546)	(819, 1/3)
(5, 9)	(739, 1/739)	($\geq$739, $\leq$ 1/739)	($\geq$ 1472, $\leq$ 1/1472)	(2208, 1/3)
(6, 9)	(1283, 1/1283)	($\geq$1283, $\leq$ 1/1283)	($\geq$ 2562, $\leq$ 1/2562)	(3848, 1/3)
(7, 9)	(1410, 1/1410)	($\geq$1410, $\leq$ 1/1410)	($\geq$ 2816, $\leq$ 1/2816)	(4224, 1/3)
(8, 9)	(899, 1/899)	($\geq$899, $\leq$ 1/899)	($\geq$ 1794, $\leq$ 1/1794)	(2691, 1/3)
(3,10)	(86, 1/86)	($\geq$86, $\leq$ 1/86)	($\geq$ 162, $\leq$ 1/162)	(243, 1/3)
(4,10)	(404, 1/404)	($\geq$404, $\leq$ 1/404)	($\geq$ 800, $\leq$ 1/800)	(1200, 1/3)
(5,10)	(1284, 1/1284)	($\geq$1284, $\leq$ 1/1284)	($\geq$ 2562, $\leq$ 1/2562)	(3843, 1/3)
(6,10)	(2754, 1/2754)	($\geq$2754, $\leq$ 1/2754)	($\geq$ 5504, $\leq$ 1/5504)	(8256, 1/3)
(7,10)	(3971, 1/3971)	($\geq$ 3971, $\leq$ 1/3971)	($\geq$ 7938, $\leq$ 1/7938)	(11907, 1/3)
(8,10)	(3714, 1/3714)	($\geq$3714, $\leq$ 1/3714)	($\geq$ 7424, $\leq$ 1/7424)	(11136, 1/3)
(9,10)	(2051, 1/2051)	($\geq$2051, $\leq$ 1/2051)	($\geq$ 4098, $\leq$ 1/4098)	(6147, 1/3)

like 4, 9, 16, 25, 32 etc. According to EVCS by Wang et al. [48] and Yan et al. [56] for maintaining good quality meaningful shares, if m is the pixel expansion of a VCS then the halftone cell size needs to be $\geq 2 \times m$ based on the access structure. According to EVCS by Wang et al. [46] if m is the pixel expansion of a (k, n) - VCS the pixel expansion of (k, n) - EVCS will be $\geq m + \lceil \frac{n}{k-1} \rceil$. Guo et al. [19] derived that, the pixel expansion for a (t, k, n) - VCS by Ateniese et al. [6] is $2^{\binom{n-t}{k-t-1}+t-1}$. So, the pixel expansion for a (t, k, n) - EVCS by Ateniese et al. [5] is obtained as $2^{\binom{n-t}{k-t-1}+t}$. Based on these observations comparison of our schemes with related works is shown below.

1) Table 2 shows that our PC1 (resp. PC2) are deterministic general access structure schemes applicable to Binary images which use OR-AND (resp. XOR-AND) operations for reconstruction. Based on our constructions each participant need to hold multiple shares similar to the EVCS constructed by Zhou et al. [63]. The advantages

Table 7 Comparison for (t, k, n) access structure

(t,k, n)	[19] (APE)	[5] (APE, α)	[48, 56] (APE, α)	PC1(APE, α)
(2, 5, 6)	$m= 2^7$	$(m+2, 1/(m+2))$	$(\geq 2m, \leq 1/2m)$	$(3m, 0.333)$
(2, 5, 7)	$m= 2^{11}$	$(m+2, 1/(m+2))$	$(\geq 2m, \leq 1/2m)$	$(3m, 0.333)$
(2, 6, 7)	$m= 2^{11}$	$(m+2, 1/(m+2))$	$(\geq 2m, \leq 1/2m)$	$(3m, 0.333)$
(2, 5, 8)	$m= 2^{16}$	$(m+2, 1/(m+2))$	$(\geq 2m, \leq 1/2m)$	$(3m, 0.333)$
(2, 6, 8)	$m= 2^{21}$	$(m+2, 1/(m+2))$	$(\geq 2m, \leq 1/2m)$	$(3m, 0.333)$
(2, 7, 8)	$m= 2^{16}$	$(m+2, 1/(m+2))$	$(\geq 2m, \leq 1/2m)$	$(3m, 0.333)$
(2, 5, 9)	$m= 2^{22}$	$(m+2, 1/(m+2))$	$(\geq 2m, \leq 1/2m)$	$(3m, 0.333)$
(2, 6, 9)	$m= 2^{36}$	$(m+2, 1/(m+2))$	$(\geq 2m, \leq 1/2m)$	$(3m, 0.333)$
(2, 7, 9)	$m= 2^{36}$	$(m+2, 1/(m+2))$	$(\geq 2m, \leq 1/2m)$	$(3m, 0.333)$
(2, 8, 9)	$m= 2^{22}$	$(m+2, 1/(m+2))$	$(\geq 2m, \leq 1/2m)$	$(3m, 0.333)$
(2, 5, 10)	$m= 2^{29}$	$(m+2, 1/(m+2))$	$(\geq 2m, \leq 1/2m)$	$(3m, 0.333)$
(2, 6, 10)	$m= 2^{57}$	$(m+2, 1/(m+2))$	$(\geq 2m, \leq 1/2m)$	$(3m, 0.333)$
(2, 7, 10)	$m= 2^{71}$	$(m+2, 1/(m+2))$	$(\geq 2m, \leq 1/2m)$	$(3m, 0.333)$
(2, 8, 10)	$m= 2^{57}$	$(m+2, 1/(m+2))$	$(\geq 2m, \leq 1/2m)$	$(3m, 0.333)$
(2, 9, 10)	$m= 2^{29}$	$(m+2, 1/(m+2))$	$(\geq 2m, \leq 1/2m)$	$(3m, 0.333)$
(2, 5, 11)	$m= 2^{37}$	$(m+2, 1/(m+2))$	$(\geq 2m, \leq 1/2m)$	$(3m, 0.333)$
(2, 6, 11)	$m= 2^{85}$	$(m+2, 1/(m+2))$	$(\geq 2m, \leq 1/2m)$	$(3m, 0.333)$
(2, 7, 11)	$m= 2^{127}$	$(m+2, 1/(m+2))$	$(\geq 2m, \leq 1/2m)$	$(3m, 0.333)$
(2, 8, 11)	$m= 2^{127}$	$(m+2, 1/(m+2))$	$(\geq 2m, \leq 1/2m)$	$(3m, 0.333)$
(2, 9, 11)	$m= 2^{85}$	$(m+2, 1/(m+2))$	$(\geq 2m, \leq 1/2m)$	$(3m, 0.333)$
(2, 10, 11)	$m= 2^{37}$	$(m+2, 1/(m+2))$	$(\geq 2m, \leq 1/2m)$	$(3m, 0.333)$
(2, 5,12)	$m= 2^{46}$	$(m+2, 1/(m+2))$	$(\geq 2m, \leq 1/2m)$	$(3m, 0.333)$
(2, 6,12)	$m= 2^{121}$	$(m+2, 1/(m+2))$	$(\geq 2m, \leq 1/2m)$	$(3m, 0.333)$
(2, 7,12)	$m= 2^{211}$	$(m+2, 1/(m+2))$	$(\geq 2m, \leq 1/2m)$	$(3m, 0.333)$
(2, 8,12)	$m= 2^{253}$	$(m+2, 1/(m+2))$	$(\geq 2m, \leq 1/2m)$	$(3m, 0.333)$
(2, 9,12)	$m= 2^{211}$	$(m+2, 1/(m+2))$	$(\geq 2m, \leq 1/2m)$	$(3m, 0.333)$
(2, 10,12)	$m= 2^{121}$	$(m+2, 1/(m+2))$	$(\geq 2m, \leq 1/2m)$	$(3m, 0.333)$
(2, 11,12)	$m= 2^{46}$	$(m+2, 1/(m+2))$	$(\geq 2m, \leq 1/2m)$	$(3m, 0.333)$

of our PC1 (resp. PC2) with a computing model of OR-AND (resp. XOR-AND) compared to other approaches are the following a)Less APE b)High relative contrast for the reconstructed image(α) c) High relative contrast for the meaningful share images(ρ).

2) Table 2 shows a review on various EVCS constructions. In Table 3, 4 and 5, deterministic schemes which are applicable to Binary images are selected from Table 2 for comparison. In Table 3, for (2, 3)-Halftone VCS [63], participant p_1 holds one share each and participant p_2 and p_3 hold two shares each. The APE and relative contrast are $\frac{(16+(2\times16)+(2\times16))}{3} = 26.63$ and 0.062 respectively. In Table 4 , for (1, 3, 4)-Halftone VCS [63], participants p_1 and p_2 hold one share each and participants p_3 and p_4 hold two shares each. The APE and relative contrast are $\frac{(16+16+(2\times16)+(2\times16))}{4} = 24$ and 0.062 respectively. In Table 5, for (2, 4, 5)-Halftone VCS [63], participants p_1, p_2 and p_3 hold one share each and participants p_4 and p_5 hold two shares each. The APE and relative contrast are $\frac{(16+16+16+(2\times16)+(2\times16))}{5} = 22.4$ and 0.062 respectively. Our PC1(resp. PC2) have better results compared to Halftone VCS [63] and other related works because our computing model is OR-AND (resp. XOR-AND) instead of only OR or XOR reconstruction. The reconstruction operation count for different EVCS constructions for (2, 3) access structure is also given in Table 3. In case of EVCS given in paper [63] the minimum (resp. maximum) number of OR operations is 16(resp. 32). For PC2 the secret image will be reconstructed by minimum 6 XOR + 3 AND operations or by maximum 12 XOR + 6 AND operations. If more shares of a participant are involved in reconstruction the Boolean operations will also increase.

3) For (2, 2) and (3, 3) EVCS by Liu et al. [27], the APE is 9 and 16 respectively, but for our PC2 it is 6. Some probabilistic EVCS [18, 22] have better relative contrast of reconstructed secret image than 0.333 for some access structure. But the relative contrast calculations of deterministic and probabilistic schemes are different. Like our construction, schemes given in paper [5, 27] also use perfect black VCS as building blocks.

Table 8 Comparison for some access structure using step construction

Γ_{QM}	[28]	PC2(APE, α)
$\{p_1, p_2\}$	(1, 1)	(6, 0.333)
$\{p_1, p_2, p_3\}$	(1, 1)	(6, 0.333)
$\{p_1, p_2\}$,$\{p_2, p_3\}$,$\{p_3, p_4\}$	(1.25, 1)	(6.75, 0.333)
$\{p_1, p_2\}$,$\{p_1, p_3\}$,$\{p_1, p_4\}$	(1, 1)	(6, 0.333)
$\{p_1, p_2\}$,$\{p_1, p_4\}$,$\{p_2, p_3\}$,$\{p_3, p_4\}$	(1, 1)	(6, 0.333)
$\{p_1, p_2\}$,$\{p_2, p_3\}$,$\{p_2, p_4\}$,$\{p_3, p_4\}$	(1.50, 1)	(7.50, 0.333)
$\{p_1, p_2\}$,$\{p_1, p_3\}$,$\{p_1, p_4\}$,$\{p_2, p_3\}$,$\{p_2, p_4\}$	(1.50,1)	(7.50, 0.333)
$\{p_1, p_2\}$,$\{p_1, p_3\}$,$\{p_1, p_4\}$,$\{p_2, p_3\}$,$\{p_2, p_4\}$,$\{p_3, p_4\}$	(2.25, 1)	(9.75, 0.333)
$\{p_1, p_2, p_3\}$,$\{p_1, p_4\}$	(1, 1)	(6, 0.333)
$\{p_1, p_2, p_3\}$,$\{p_1, p_4\}$,$\{p_3, p_4\}$	(1.50, 1)	(7.50, 0.333)
$\{p_1, p_3, p_4\}$,$\{p_1, p_2\}$,$\{p_2, p_3\}$,$\{p_2, p_4\}$	(1.75, 1)	(8.25, 0.333)
$\{p_1, p_2, p_3\}$,$\{p_1, p_2, p_4\}$	(1,1)	(6, 0.333)
$\{p_1, p_2, p_4\}$,$\{p_1, p_3, p_4\}$,$\{p_2, p_3\}$	(1.50, 1)	(7.50, 0.333)
$\{p_1, p_2, p_3\}$,$\{p_1, p_2, p_4\}$,$\{p_1, p_3, p_4\}$	(1.50,1)	(7.50, 0.333)
$\{p_1, p_2, p_3, p_4\}$	(1,1)	(6, 0.333)

4) The (APE, α) values for the EVCS constructions [5, 27, 46, 48, 56, 62, 63] given in Tables 3, 4 and 5 are calculated under the assumption that the VCS used is Ateniese et al. [6] construction. But Blundo et al. [7] constructed a perfect black (k, n) - VCS with less pixel expansion in 2001. So the (APE, α) values for the EVCS constructions [5, 46, 48, 56] given in Table 6 (resp. 7) are calculated under the assumption that the (k, n) - VCS used is Blundo et al. [7] construction and (t, k, n) - VCS used is Guo et al. [19] construction. In Tables 8 and 9, the (APE, α) values for our PC2 - EVCS are calculated under the assumption that the VCS used is XOR based step construction by Liu et al. [28]. The APE values of our PC2 - EVCS are directly derived from the APE values of XOR based VCS given in Table 1 of paper [28].

5) In Halftoning EVCS, the halftone block size vary depends on the pixel expansion of VCS used, peak signal to noise ratio (PSNR) and universal quality index(UQI) measurements are used to calculate the distortion of cover share image compared to original

Table 9 Comparison for (k, n) access structure using step construction

(k, n)	[28] (APE, α)	PC2(APE, α)
(2, 3)	(1.60, 1)	(8, 0.333)
(2, 4)	(2.25, 1)	(9.75, 0.333)
(3, 4)	(2, 1)	(9, 0.333)
(2, 5)	(2.80, 1)	(11.40, 0.333)
(3, 5)	(3.6, 1)	(13.8, 0.333)
(4, 5)	(2.6, 1)	(10.8, 0.333)
(2, 6)	(3.33, 1)	(13, 0.333)
(3, 6)	(5.5, 1)	(19.5, 0.333)
(4, 6)	(5.33, 1)	(18.9, 0.333)
(5, 6)	(2.6, 1)	(10.98, 0.333)
(2, 7)	(3.85, 1)	(14.57, 0.333)
(3, 7)	(7.71, 1)	(21, 0.333)
(4, 7)	(9.42, 1)	(31.26, 0.333)
(5, 7)	(6.85, 1)	(23.55, 0.333)
(6, 7)	(3.28, 1)	(12.84, 0.333)
(2, 8)	(4.37, 1)	(16.12, 0.333)
(3, 8)	(10.25, 1)	(33.75, 0.333)
(4, 8)	(15.12, 1)	(48.37, 0.333)
(5, 8)	(14.25, 1)	(45.75, 0.333)
(7, 8)	(3.25, 1)	(12.75, 0.333)
(2, 9)	(4.88, 1)	(17.66, 0.333)
(3, 9)	(13.11, 1)	(42.33, 0.333)
(4, 9)	(22.66, 1)	(70.98, 0.333)
(5, 9)	(26.11, 1)	(81.33, 0.333)
(8, 9)	(3.88, 1)	(14.4, 0.333)
(2, 10)	(5.40, 1)	(19.20, 0.333)
(3,10)	(16.3, 1)	(51.9, 0.333)
(4,10)	(32.3, 1)	(99.9, 0.333)
(5,10)	(43.9, 1)	(134.7, 0.333)
(9,10)	(3.80, 1)	(14.4, 0.333)

Table 10 Comparison of visual quality of cover share images ρ for (3, 3) - EVCS

[5]	[27]	[48]	[56]	PC1	PC2
0.250	0.750	0.500	0.555	0.666	0.666

halftoned share images. Let us define *em* (resp. *m*) as the pixel expansion of an EVCS (resp. VCS). Then *em* = *m* (represents: secret information pixels) + *q* (represents: cover image information pixels + auxiliary black pixels). So the visual quality (relative contrast) of the cover share images is calculated as $\rho = \frac{em-m}{em} > 0$ [48, 56]. Table 10 shows that the visual quality of our EVCS constructions maintain the quality of existing deterministic EVCS in the literature. The user can select the values for *em* and *m* based on the applications.

6) The reconstructed image quality of our EVCS (Fig. 1) is better than Ateniese et al. [5] - EVCS and the probabilistic scheme of Yang [57] for (2, 3) access structure.

4 Conclusions

Our deterministic EVCS constructions have a relative contrast of 0.333 for both the reconstructed image and cover share images for all access structures. It is evident that our EVCS construction PC2 has less APE and high relative contrast for reconstructed image compared to all other deterministic EVCS constructions for any access structure. It is true that, our proposed deterministic EVCS constructions are complex due to a) Combined use of Boolean operations OR and AND (resp. XOR and AND) instead of only OR or XOR operation for reconstruction b) Each participant holds multiple shares instead of single share c) Selection of cover images (Complementary cover images in PC1, Similar cover images in PC2). But in our schemes there are no complex calculations involved in finding *q* (represents: cover image information pixels + auxiliary black pixels) needed for maintaining the visual quality of cover share images, as in halftoning EVCS constructions. In our schemes, for all the cover image shares the value of $q = 2$ for any access structure, but in halftoning EVCS constructions *q* will vary according to the access structure. Moreover our proposed schemes can be used effectively for applications [2, 11, 21, 30, 38, 43, 60, 61] which need less storage space (less APE) and high reconstructed image quality (high relative contrast). At the same time in deterministic EVCS, a thin line in the secret is converted to a thick line and due to pixel expansion problem it may lead to graying effect but in probabilistic EVCS, a thin line may not be visible in the reconstructed secret. Our deterministic EVCS constructions solves this problem of thin line discussed in papers [26, 29].

References

1. Abadi M, Burrows M, Kaufman C, Lampson B (1993) Authentication and delegation with smart-cards. Sci Comput Program 21(2):93–113
2. Abdullah MA, Dlay SS, Woo WL, Chambers JA (2016) A framework for iris biometrics protection: a marriage between watermarking and visual cryptography. IEEE Access 4:10180–10193
3. Adhikari A (2013) Linear algebraic techniques to construct monochrome visual cryptographic schemes for general access structure and its applications to color images. Des Codes Cryptography 73(3):865–895
4. Arumugam S, Lakshmanan R, Nagar AK (2014) On $(k, n)*$-visual cryptographic scheme. Des Codes Cryptography 71(1):153–162

5. Ateniese G, Blundo C, De Santis A, Stinson DR (2001) Extended capabilities for visual cryptography. Theoretical Comput Sci 250(1):143–161
6. Ateniese G, Blundo C, Santis AD, Stinson DR (1996) Visual cryptography for general access structures. Inform Comput 129(2):86–106
7. Blundo C, Bonis AD, Santis AD (2001) Improved schemes for visual cryptography. Des Codes Cryptography 24(3):255–278
8. Chen TH, Lee YS (2009) Yet another friendly progressive visual secret sharing scheme. In: Proceedings of the IIHMSP 2009, pp 353–356
9. Chiu PL, Lee KH (2015) User-friendly threshold visual cryptography with complementary cover images. Signal Process 108:476–488
10. Cimato S, Santis AD, Ferrara AL, Masucci B (2005) Ideal contrast visual cryptography schemes with Reversing. Inform Process Lett 93(4):199–206
11. Cimato S, Yang JC, Wu CC (2014) Visual cryptography based watermarking. Trans Data Hiding Multimed Secur 9:91–109
12. Dang W, He M, Wang D, Li X (2015) K out of k extended visual cryptography scheme based on XOR. Int J Comput Commun Eng 4(6)
13. De Bonis A, De Santis A (2004) Randomness in secret sharing and visual cryptography schemes. Theor Comput Sci 314(3):351–74
14. Dutta S, Rohit RS, Adhikari A (2015) Constructions and analysis of some efficient $t-(k,n)^*$- visual cryptographic schemes using linear algebraic techniques. Des Codes Cryptography:1–32
15. EL-Latif AAA, Yan X, LI L, Wang N, Peng JL, Niu X (2013) A new meaningful secret sharing scheme based on random grids, error diffusion and chaotic encryption. Opt Laser Technol 54:389–400
16. Fang WP (2008) Friendly progressive visual secret sharing. Pattern Recogn 41:1410–1414
17. Guo T, Liu F, Wu C, Ren Y, Wang W (2013) On the randomness of visual cryptography scheme. In: Ninth international IEEE conference on Intelligent Information Hiding and Multimedia Signal Processing, pp 391–394
18. Guo T, Liu F, Wu CK (2014) k out of k extended visual cryptographic scheme by random grids. Signal Process 94:90–101
19. Guo T, Liu F, Wu CK, Wang W (2014) On (k, n) visual cryptography scheme with t essential parties. LNCS 8317:56–68
20. Kang I, Arce GR, Lee HK (2011) Color extended visual cryptography using error diffusion. IEEE Trans image Process 20(1):132–145
21. Kaur H, Khanna P (2016) Biometric template protection using cancelable biometrics and visual cryptographic techniques. Multimed Tool Appl 75(23):16333–16361
22. Lee KH, Chiu PL (2012) An extended visual cryptography algorithm for general access structures. IEEE Trans Inform Forensics Secur 7(1):219–229
23. Liao X, Guo S, Yin J, Wang H, Li X, Sangaiah AK (2017) New cubic reference table based image steganography. Multimed Tool Appl
24. Liao X, Qin Z, Ding L (2017) Data embedding in digital images using critical functions. Signal Process: Image Commun 58:146–156
25. Liao X, Yin J, Guo S, Li X, Sangaiah AK (2017) Medical JPEG image steganography based on preserving inter-block dependencies. Comput Electric Eng
26. Liu F, Guo T, Wu C, Yang CN (2014) Flexible visual cryptography scheme and its application. in transactions on data hiding and multimedia security IX 2014. Springer, Berlin, pp 110–130
27. Liu F, Wu C (2011) Embedded extended visual cryptography schemes. IEEE Trans Inform Forensics Secur 6(2):307–322
28. Liu F, Wu C, Lin X (2010) Step construction of visual cryptographic schemes. IEEE Trans Inform Forensics Secur 5(1):25–34
29. Liu F, Wu C, Qian L (2012) Improving the visual quality of size invariant visual cryptography scheme. J Visual Commun Image Represent 23(2):331–342
30. Lu J, Yang Z, Li L, Yuan W, Li L, Chang CC (2017) Multiple schemes for mobile payment authentication using QR Code and visual cryptography. Mobile Inform Syst
31. Lu S, Manchala D, Ostrovsky R (2011) Visual cryptography on graphs. J Combin Optim 21(1):47–66
32. Nakajima M, Yamaguchi Y (2002) Extended visual cryptography for natural images. In: Proceedings of WSGC, p 2002
33. Naor M, Pinkas B (1997) Visual authentication and identification. In: Annual International Cryptology Conference. Springer, Berlin, pp 322–336

34. Naor M, Shamir A (1994) Visual cryptography. Proc Eurocrypt 1994:1–12
35. Ou D, Sun W (2016) Meaningful (2, infinity) secret image sharing scheme based on flipping operations. Multimed Tool Appl 75(6):3517–3536
36. Ou D, Sun W, Wu X (2015) Non-expansible XOR-based visual cryptography scheme with meaningful shares. Signal Process 108:604–621
37. Praveen K, Sethumadhavan M (2015) Ideal contrast visual cryptography for general access structures with AND operation. Proc Third ICACNI 2015:309–314
38. Ross A, Otham A (2011) Visual cryptography for biometric privacy. IEEE Trans inform Forensics secur 6(1):70–81
39. Shivani S (2017) Multi secret sharing with unexpanded meaningful shares. Multimed Tool Appl:1–24
40. Shivani S, Agarwal S (2017) Novel basis matrix creation and processing algorithms for friendly progressive visual secret sharing with space-efficient shares. Multimed Tool Appl 76(6):8711–8744
41. Shyu SJ (2014) Threshold visual cryptographic scheme with meaningful shares. IEEE Signal Process Lett 21(2):1521–1525
42. Shyu SJ, Chen MC (2015) Minimizing pixel expansion in visual cryptographic scheme for general access structures. IEEE Trans Circuits Syst for Video Technol 25(9):1557–1561
43. Tai GC, Chang LW (2004) Visual cryptography for digital watermarking in still images. Pacific-rim conference on multimedia. Springer, Berlin
44. Ulutas M (2010) Meaningful share generation for increased number of secrets in visual secret-sharing scheme. Math Probl Eng:2010
45. Wang DS, Song T, Dong L, Yang CN (2013) Optimal contrast grayscale visual cryptography schemes with reversing. IEEE Trans Inform Forensics Secur 8(12):2059–2072
46. Wang DS, Yi F, Li XB (2009) On general constructions for extended visual cryptographic schemes. Pattern Recogn 42(11):3071–3082
47. Wang S, Yan X, Sang J, Niu X (2016) Meaningful visual secret sharing based on error diffusion and random grids. Multimed Tool Appl 75(6):3353–3373
48. Wang Z, Arce GR, Di Crescenzo G (2009) Halftonevisual cryptography with error diffusion. IEEE Trans Inform Forensics Secur 4(3):383–396
49. Wang ZM, Arce GR (2006) Halftone visual cryptography through error diffusion. In: Proceedings of the IEEE International conference on Image Processing, pp 109–112
50. Wang ZM, Arce GR, Di Crescenzo G (2006) Halftone visual cryptography via direct binary search. In: Proceedings of the EUSIPCO, p 2006
51. Xiong L, Jian M, Wendong W, Yongping X, Junsong Z (2013) A novel smart card and dynamic ID based remote user authentication scheme for multi-server environments. Math Comput Model 58(1-2):85–95
52. Xiong L, Jianwei N, Junguo L, Wei L (2015) Cryptanalysis of a dynamic identity-based remote user authentication scheme with verifiable password update. 28(2):374–382
53. Yamaguchi Y (2014) Extended visual cryptography scheme for multiple-secrets continuous-tone images. Proc Trans Data Hiding Multimed Secur IX:25–41
54. Yan B, Wang YF, Song LY, Yang HM (2016) Size-invariant extended visual cryptography with embedded watermark based on error diffusion. Multimed Tool Appl 75(18):11157–11180
55. Yan X, Wang S, Niu X, Yang CN (2015) Generalized random grids-based threshold visual cryptography with meaningful shares. Signal Process 109:317–333
56. Yan X, Wang S, Niu X, Yang CN (2015) Halftone visual cryptography with minimum auxiliary black pixels and uniform image quality. Digital Signal Process 38:53–65
57. Yang CN (2004) New visual secret sharing schemes using probabilistic method. Pattern Recogn Lett 25:481–494
58. Yang CN, Chen TS (2005) Extended visual secret sharing schemes with high-quality shadow images using gray sub pixels. Proceedings of the ICIAR 2005:1184–1191
59. Yang CN, Chen TS (2007) Extended visual secret sharing schemes. Improving the shadow image quality. Int J Pattern Recogn Artif Intell 21(5):879–898
60. Yang CN, Liao JK, Wu FH, Yamaguchi Y (2016) Developing visual cryptography for authentication on smart phones. International conference on industrial IoT technologies and applications. Springer, Berlin
61. Yang CN, Sun LZ, Yan X, Kim C (2016) Design a new visual cryptography for human-verifiable authentication in accessing a database. J Real-Time Image Process 12(2):483–494
62. Yang CN, Yang YY (2014) New extended visual cryptography schemes with clearer shadow images. Inform Sci 271:246–263
63. Zhou Z, Arce GR, Di Crescenzo G (2006) Halftone visual cryptography. IEEE Trans Image Process 15(8):2441–2453

Praveen Kanakkath received his M.Tech (Cyber Security) from Amrita Vishwa Vidyapeetham, Coimbatore and currently pursuing his PhD from TIFAC-Center of Relevance and Excellence in Cyber Security, Amrita Vishwa Vidyapeetham, Coimbatore. His current research interests include: Visual Cryptography and System Security.

Sethumadhavan Madathil received his PhD from Calicut Regional En- gineering College. Currently, he is working as a Professor and Head of TIFAC Center of Relevance and Excellence in Cyber Security, Amrita Vishwa Vidyapeetham, Coimbatore. His current research interests include: Cryptology and Boolean functions.

Ramakrishnan Krishnan received his PhD from IISc, Bangalore. He is currently an Adjunct Professor in TIFAC-Center of Relevance and Excellence in Cyber Security, Amrita Vishwa Vidyapeetham, Coimbatore. His current research interests include: Image processing and Remote sensing.