Efficient Random Grid Visual Cryptographic Schemes having Essential Members

Bibhas Chandra Das, Md Kutubuddin Sardar, and Avishek Adhikari

1 Introduction

The essence of visual cryptography is that the encryption of a visual secret is done in such a way that the reconstruction can be performed only via sight-reading. So one can easily conclude that visual cryptography does not require many sophisticated cryptographic techniques like polynomial based secret image sharing [18–20, 26], yet it produces strong schemes for many practical scenarios. For this reason, throughout time many researchers have developed a strong interest in this specific area of cryptography.

The seminal paper by Naor and Shamir [17] is considered as the starting point of the (k, n)-visual cryptographic scheme. They proposed a way to distribute a secret image S among n members, where any k (or more) of them can superimpose their shares to reconstruct S. Obviously, the reconstruction comes with loss of contrast but still it is human readable. Then in 2017 Arungam et. al. [16] extended the idea of (k, n)-VCS to incorporate one essential member. This work was further extended by Sabyasachi et. al. [9] by extending it to a $(t, k, n)^*$-VCS, with t essential members. Some notable works on classical VCS may be found in [1–8, 10–14, 27, 29].

A thorough study of the literature will suggest that at the very initial stage the works in this area experienced huge pixel expansion with very little contrast. Researchers engaged themselves to deal with this problem and introduced the best solution,

B. Chandra Das
Institute for Advancing Intelligence (IAI), TCG CREST, Kolkata, India
e-mail: bibhas.iitm@gmail.com

M. K. Sardar
Department of Pure Mathematics University of Calcutta, Kolkata, India
e-mail: mks.pubm@gmail.com

A. Adhikari (✉)
Department of Mathematics, Presidency University, Kolkata, India
e-mail: avishek.adh@gmail.com

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2021

P. Stănică et al. (eds.), *Security and Privacy*, Lecture Notes in Electrical Engineering 744,
https://doi.org/10.1007/978-981-33-6781-4_4

namely Random Grid Visual Cryptography (RGVCS). In RGVCS, there is no pixel expansion and we can reach the optimal level for contrast. The basic idea of RGVCS is that each pixel of the secret image here is considered to be a random grid with an associated color. The literature study of RGVCS can be found in [15, 22, 24, 25].

In this paper, we have proposed a (t, k, n) scheme for black and white RGVCS for both "OR" and "XOR" models. Besides constructing the scheme, we have described the closed forms of the corresponding light contrasts. We have deviated a bit from the traditional "OR" operation to "XOR" operation with a motif of increasing the light contrast. The only thing that we have to keep in mind for the scheme with the "XOR" operation is that the reconstruction will no longer be visual. The experimental results presented indicate the efficiency of our proposed schemes.

The rest of the paper is organized as follows. We have started with Sect. 2 to describe the notations and basic concepts of VCS as well as RGVCS which we will need for construction and security analysis of our proposed scheme. In Sect. 3, we have given the construction of schemes with detailed theoretical security analysis. Section 4 deals with the experimental results to justify the theoretical results that we proved for analyzing the security of our scheme. Also, we have performed a comparison of the light contrast of our scheme with that of the modified versions of the schemes that are already proposed. The theoretical study together with the experimental results shows the significance of our scheme in the area of RGVCS. The paper concludes with Sect. 5, where we have pointed out the future direction of research.

2 Preliminaries

This section presents the notations that we will widely use to describe our proposed schemes. To start with let us assume a secret pixel S is to be shared among a set of n members, $\mathcal{P} = \{M_1, M_2, \ldots, M_n\}$. By Γ_{Qual}, we will denote the collection of all subsets of $\mathcal{P}$ who are eligible to reconstruct S by superimposing their shares. On the other hand, Γ_{Forb} denotes the collection of all those subsets of $\mathcal{P}$ who are not eligible to reconstruct S. Elements of Γ_{Qual} are called qualified set while elements of Γ_{Forb} are called forbidden set. The ordered pair $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}})$ is called an access structure for $\mathcal{P}$ corresponding to S. Now a given access structure is called monotone when Γ_{Qual} is monotone increasing and Γ_{Forb} is monotone decreasing. For such an access structure, Minimal Qualified set and Maximal Forbidden set are defined as $\Gamma_0 = \{A \in \Gamma_{\text{Qual}} | A' \notin \Gamma_{\text{Qual}}, \forall A' \subset A\}$, $Z_M = \{B \in \Gamma_{\text{Forb}} | B \cup \{i\} \in \Gamma_{\text{Qual}}, \forall i \in \mathcal{P} \setminus B\}$. These two sets are, respectively, denoted by Γ_0 and Z_M. For our schemes, we talk about a special kind members, namely essential members. A member $a \in \mathcal{P}$ is said to be essential if there exists $X \subseteq \mathcal{P}$ such that $X \cup \{a\} \in \Gamma_{\text{Qual}}$ but $X \notin \Gamma_{\text{Qual}}$. The notation of a (k, n) threshold access structure is adapted from [24]. For our purpose, we have incorporated the idea of essential members with the notation of a (k, n) threshold access structure and have defined (t, k, n) access structure. By that, we mean that it is a (k, n) access structure where t of the n members are

essential. Clearly enough, the values of the parameters for which $0 \leq t \leq k \leq n$ admit a meaningful (t, k, n) visual cryptographic scheme. Note that in such an access structure, a maximal forbidden set may be of the two types. Type I: Sets containing $k-1$ members including all the essential members. Type II: Sets having a size exactly $n-1$ which contains all but one of the t essential members.

Now the notations related to grid based VCS are adapted from [24]. We have considered a binary transparency Y in which each pixel is either transparent (0) or opaque (1). Generally, the value of each pixel is determined by a coin flip where it is assumed that probability of $y = 0$ is λ. Keeping in mind the fact that the pixel with $y = 0$ lets through light and the pixel with $y = 1$ stops it, the light transmission of y, denoted by $t(y)$, is defined to be $Pr(y = 0)$. The light transmission of a random grid, denoted by $\mathcal{T}(Y)$, is λ when $t(y) = \lambda$ for each pixel $y \in Y$ [24]. From this definition of light transmission, we can observe that for a random grid X with $\mathcal{T}(X) = \lambda$, $X \otimes X$ is a random grid with $\mathcal{T}(X \otimes X) = \mathcal{T}(X) = \lambda$. Also for two independent random grids with $\mathcal{T}(X) = \lambda_1$ and $\mathcal{T}(Y) = \lambda_2$, we have $\mathcal{T}(X \otimes Y) = \lambda_1\lambda_2$. With this setting in our hand, we can now define the formal model of a (t, k, n) random grid based visual cryptographic scheme.

Notation: As in [21], let $S(0)$ $(S(1))$ denote the area of all of the transparent (opaque) pixels in the secret image S, i.e., (u, v)th pixel $S[u, v]$ of the secret S is in $S(0)$ $(S(1))$ if and only if $S[u, v] = 0$ $(S[u, v] = 1)$ where $S = S(0) \cup S(1)$ and $S(0) \cap S(1) = \emptyset$. Likewise, we denote the area of pixels in random grid G corresponding to $S(0)(S(1))$ by $G[S(0)]$ $(G[S(1)])$, i.e., (u, v)th pixel $G[u, v]$ of the random grid G is in $G[S(0)]$ $(G[S(1)])$ if and only if $G[u, v]$'s corresponding pixel $S[u, v]$ is in $S(0)(S(1))$. Needless to mention, $G = G[S(0)] \cup G[S(1)]$ and $G[S(0)] \cap G[S(1)] = \emptyset$.

Definition 1 For valid parameters t, k and n, an $H' \times W$ binary secret image S and set of n members the set of random grids $\mathcal{G} = \{G_1, G_2, \ldots, G_n\}$ forms an "OR" based (t, k, n)-RGVCS if:

1. $\mathcal{T}(G_v) = \frac{1}{2}$ for all $1 \leq v \leq n$.
2. For each $F = \{M_{u_1}, M_{u_2}, \ldots, M_{u_p}\} \in \mathcal{F}, \mathcal{T}(G^F[S(0)]) = \mathcal{T}(G^F[S(1)])$, where $G^F = G_{u_1} \otimes G_{u_2} \otimes \cdots \otimes G_{u_p}$, i.e., $t(G^F[u, v] \mid S[u, v] = 0) = t(G^F[u, v] \mid S[u, v] = 1), \forall\, u, v$.
3. For $Q \in \Gamma_0, \mathcal{T}(G^Q[S(0)]) > \mathcal{T}(G^Q[S(1)])$ where $G^Q = G_1 \otimes G_2 \otimes \cdots \otimes G_q$, i.e., $t(G^Q[u, v] \mid S[u, v] = 0) > t(G^Q[u, v] \mid S[u, v] = 1), \forall\, u, v$.

Definition 2 The light contrast for any given set $H \subseteq \mathcal{P}$, denoted as α^H_{OR}, is defined as $\alpha^H_{\mathrm{OR}} = \mathcal{T}(G^H[S(0)]) - \mathcal{T}(G^H[S(1)])$.

3 Proposed Scheme

In this section, we propose an efficient (t, k, n)-RGVCS for both monotone and non-monotone access structures. We will first start with describing the constructions and then discuss their light corresponding light transmission. To our knowledge, this is the first ever (t, k, n)-RGVCS.

3.1 Construction

For a secret $H' \times W$ binary image S, the dealer first constructs the shares for the members and distributes them in the following manner.

- The dealer first identifies the essential members and marks them as $M_1, M_2, \ldots, M_t$. The rest of the members are marked as $M_{t+1}, M_{t+2}, \ldots, M_{n-1}, M_n$.
- For each secret pixel $S[u, v]$ of S, the dealer selects $k - 1 - t$ members randomly from $M_{t+1}, M_{t+2}, \ldots, M_{n-1}$, and together with $M_1, M_2, \ldots, M_t$ form a set A of size $k - 1$.
- The dealer assigns 0 or 1 random grids to the members of A.
- For the remaining members the share is generated as $g(s, x) = s \oplus x$, for $s, x \in \{0, 1\}$, where $\oplus$ denotes binary "XOR" operation.

Algorithm 1 is the detailed construction of the share generation phase of our proposed scheme.

Algorithm 1: Algorithm toward constructing a (t, k, n)-RGVCS

Input: A black and white secret image S of size $H' \times W$, and the access structure (t, k, n) with meaningful triplet (t, k, n) and set $\mathcal{P}$ of n members.
Output: n shares $G_1, G_2, \ldots, G_n$ each of size $H' \times W$.
From the set $\mathcal{P}$ of n members, select the t essential members. Denote them as $M_1, M_2, \ldots, M_t$. Denote the remaining members as $M_{t+1}, M_{t+2}, \ldots, M_{n-1}, M_n$.
for $(u = 1; u \leq H'; u++)$ **do**
  for $(v = 1; v \leq W; v++)$ **do**
    Generate $(k-1)$ random grids $r_1[u, v], r_2[u, v], \ldots, r_{k-1}[u, v]$
    Randomly select $k - t - 1$ members, say $M_{l_1}, M_{l_2}, \ldots, M_{l_{k-t-1}}$ from $\{M_{t+1}, M_{t+2}, \ldots, M_{n-1}\}$. Let $A = \{M_1, M_2, \ldots, M_t, M_{l_1}, M_{l_2}, \ldots, M_{l_{k-t-1}}\}$
    Construct $b_1[u, v], b_2[u, v], \ldots, b_k[u, v]$ as
      $b_1[u, v] = r_1[u, v]$
      $b_p[u, v] = g(r_p[u, v], b_{p-1}[u, v])\ \forall p = 2, 3, \ldots, k-1$
      $b_k[u, v] = g(S[u, v], b_{k-1}[u, v])$
    for $(q = 1; q \leq t; q++)$ **do**
      $G_q[u, v] \leftarrow r_q[u, v]$
    end
    for $(q = 1; q \leq k - t - 1; q++)$ **do**
      $G_{l_q}[u, v] \leftarrow r_{t+q}[u, v]$
    end
    $G_s[u, v] \leftarrow b_k[u, v]$, for all $s \in \{1, 2, \ldots, n\} \setminus \{1, 2, \ldots, t, l_1, l_2, \ldots, l_{k-t-1}\}$.
  end
end
Member M_i is given the share $G_i, i = 1, 2, \ldots, n$.

Now in the secret reconstruction phase, the member can adapt one of the following two methods:

1. Either they can superimpose their shares to reconstruct the secret image. The way the random grid is defined superimposition corresponds to classical "OR" operation. Algorithm 1 together with this type of secret reconstruction gives us a scheme for strong monotone access structure.
2. On the other hand, if the members can provide some computational power they can use "XOR" operation in the place of "OR" operation. Algorithm 1 together with this type of secret reconstruction gives us a scheme for non-monotone access structure.

3.2 Discussion on Light Transmission

Now we will prove theoretically that the proposed scheme is a valid (t, k, n) scheme by showing that it satisfies the conditions of Definition 1.

Before going to the direct proof we will start by proving three lemmas which in turn will take us to the final conclusion.

Lemma 1 *The light transmission* $\mathcal{T}(G_u) = \frac{1}{2}$ *for* $1 \le u \le n$.

Proof Note that each G_i is either a random grid or constructed by applying f on $k-1$ random grids. In both the cases, the randomness is not hampered.

Lemma 2 *For a given* (t, k, n)*-RGVCS, let* F *be a maximal forbidden set of members. Then* $\mathcal{T}(G^F[S(0)]) = \mathcal{T}(G^F[S(1)])$*, where* G^F *is obtained by applying any reconstruction function "OR" or "XOR" on* $G_{l_1}, G_{l_2}, \ldots, G_{l_m}$.

Proof First of all, let us denote the two types of maximal forbidden sets that we mentioned earlier as Type I and Type II sets, respectively. One can now easily observe that the Type I sets are nothing but the sets of size $\le k-1$ of a (k, k)-scheme. The light transmission of this set depends on the choice of A. The length of the intersection of A and F can vary from t to $k-2$ when $M_n \in F$. But when $M_n \notin F$ the the length of intersection can vary from t to $k-1$. If we consider the classical "OR" reconstruction then the total light transmission of F is given as $t(G^F[u, v] \mid S[u, v] = 0) = t(G^F[u, v] \mid S[u, v] = 1) = \frac{1}{\binom{n-1-t}{k-1-t}} \left[\sum_{h=t}^{k-2} \frac{\binom{k-2-t}{h-t} \times \binom{n-k+1}{k-1-h}}{2^{h+1}} \right]$, if $M_n \in F$

$= \frac{1}{\binom{n-1-t}{k-1-t}} \left[\frac{1}{2^{k-1}} + \sum_{h=t}^{k-2} \frac{\binom{k-1-t}{h-t} \times \binom{n-k}{k-1-h}}{2^{h+1}} \right]$, if $M_n \notin F$. But for Type II sets, their behavior does not vary for different choices of $\mathcal{A}$. So for them the light transmission will be

$$t(G^F[u, v] \mid S[u, v] = 0) = \frac{1}{2^{k-1}} = t(G^F[u, v] \mid S[u, v] = 1).$$

The same type of calculation follows for "XOR" operation.

Lemma 3 *For a given* (t, k, n)*-RGVCS, let* Q *be a minimal qualified set of members. Then* $\mathcal{T}(G^Q[S(0)]) > \mathcal{T}(G^Q[S(1)])$*, where* G^Q *is obtained by applying any reconstruction function "OR" or "XOR" on* $G_{l_1}, G_{l_2}, \cdots, G_{l_k}$.

Proof We will proceed again here as in the previous lemma. Here $\mid Q \cap A \mid$ can vary from t to $k-1$. So depending on number of different choices of $\mathcal{A}$ for classical reconstruction method "OR" the light transmission for Q is

$$t(G^Q[u, v] \mid S[u, v] = 0) = \frac{1}{\binom{n-1-t}{k-1-t}} \left[\frac{1}{2^{k-1}} + \sum_{h=t}^{k-2} \frac{\binom{k-1-t}{h-t} \times \binom{n-k}{k-1-h}}{2^{h+1}} \right], \text{ if } M_n \in Q$$

$$= \frac{1}{\binom{n-1-t}{k-1-t}} \left[\frac{k-t}{2^{k-1}} + \sum_{h=t}^{k-2} \frac{\binom{k-t}{h-t} \times \binom{n-1-k}{k-1-h}}{2^{h+1}} \right], \text{ if } M_n \notin Q.$$

$$\text{And } t\,(G^Q[u,v] \mid S[u,v] = 1) = \frac{1}{\binom{n-1-t}{k-1-t}} \left[\sum_{h=t}^{k-2} \frac{\binom{k-1-t}{h-t} \times \binom{n-k}{k-1-h}}{2^{h+1}} \right], \text{ if } M_n \in Q$$

$$= \frac{1}{\binom{n-1-t}{k-1-t}} \left[\sum_{h=t}^{k-2} \frac{\binom{k-t}{h-t} \times \binom{n-1-k}{k-1-h}}{2^{h+1}} \right], \text{ if} M_n \notin Q.$$

Subtracting this two we get the light contrast for Q as $\alpha_{\text{OR}}^{Q} = \frac{1}{\binom{n-1-t}{k-1-t}} \cdot \frac{1}{2^{k-1}}$, $M_n \in Q$, and $\alpha_{\text{OR}}^{Q} = \frac{1}{\binom{n-1-t}{k-1-t}} \cdot \frac{k-t}{2^{k-1}}$, $M_n \notin Q$. Now to conclude the theorem we notice that the validity condition $k > t$ makes the light contrast a strictly positive quantity. Similar arguments can be followed to show that for "XOR" reconstruction the light contrast becomes exactly 1. Now we are in good shape two state the following results:

Theorem 1 *Let S be a secret image. Then for a (t, k, n) threshold access structure our scheme in Algorithm 1 gives a (t, k, n)-RGVCS with light contrast for a minimal qualified set:*

$$\alpha_{OR}^{Q} = \frac{1}{\binom{n-1-t}{k-1-t}} \cdot \frac{1}{2^{k-1}}, \text{ if } M_n \in Q, \text{ and } \alpha_{OR}^{Q} = \frac{1}{\binom{n-1-t}{k-1-t}} \cdot \frac{k-t}{2^{k-1}}, \text{ if } M_n \notin Q \text{ for}$$

classical "OR" reconstruction method and exactly 1 for "XOR" -based reconstruction method.

Proof From Lemmas 1–3, the proof is very much obvious.

The following table shows a practical example for the calculations we have just described theoretically.

Now in a nutshell the security of our proposed scheme is given in form of the following theorem.

Theorem 2 *Let S be a secret image and n be the number of members, t of them are essential. Let the threshold value be k. Then our scheme produces a (t, k, n)-RGVCS. If $\bar{\alpha}_{OR}^{Q}$ denotes the light contrast of a minimal qualified set $Q \subseteq \mathcal{P}$ then $\bar{\alpha}_{OR}^{Q}$ is given by $\bar{\alpha}_{OR}^{Q} = \frac{1}{\binom{n-t}{k-1-t}} \cdot \frac{1}{2^{k-1}}$ for classical "OR" reconstruction and 1 for "XOR" reconstruction method.*

3.3 Comparison Among the Schemes Proposed by Wu and Sun [28] and Shyu [23]

To the best of our knowledge, our proposed (t, k, n)-random grid visual cryptographic scheme for black and white images is the first proposed scheme in the literature of visual cryptography for essential access structures. That is why, it is not possible for us to have a direct comparison with the existing schemes. However, as particular cases, we can construct (t, k, n)-RGVCS, from the random grid based schemes for general access structures. In this section, we are comparing our proposed Algorithm 1 with the customized schemes, obtained as a particular case from general access structures proposed in [23, 28]. To the best of our knowledge, these schemes are the most efficient schemes that exist in the literature for general access structures.

The following theorem is obtained if we apply the scheme proposed in [28] on the essential access structure for (t, k, n):

Theorem 3 (customized from *[28]) For an essential* (t, k, n) *access structure with a given black and white secret image* S *and valid parameters* t, k, *and* n, *the scheme described in [28] produces a* (t, k, n)*-RGVCS with light contrast:* $\alpha_w = \frac{1}{\binom{n-t}{k-t}} \cdot \frac{1}{2^{k-1}}$.

Analogously, we can obtain the following theorem, if we apply the scheme proposed by Shyu [23] on the essential access structure for valid parameters t, k, and n:

Theorem 4 (customized from *[23]) For an essential* (t, k, n) *access structure with a black and white secret image* S *along with the valid parameters* t, k, *and* n, *the scheme described in [23] generates a* (t, k, n)*-RGVCS with light contrast:* $\alpha_s = \frac{1}{2^{\mathcal{K}}}$, *where* $\mathcal{K} = 1 + \sum_{h=t}^{k-1} \binom{k-t}{h-t} \binom{n-k}{k-h} h$.

Remark 1 Note that the light contrast for our proposed scheme is better than that of the schemes proposed in [23, 28]. Numerical evidence as shown in Table 1 demonstrates that our scheme performs better in terms of light contrast than the existing schemes.

Table 1 Calculation of the light contrast with access structure (2, 4, 6)-RGVCS. Here, $n_2(A)$ and $n_3(A)$ denote, respectively, the number of choices of A for which $|H \cap A|$ is 2 and 3.

Set of members: H	$n_2(A)$	$n_3(A)$	$\mathcal{T}(G^H[S(0)])$	$\mathcal{T}(G^H[S(1)])$	α_{OR}^H
$\{M_1, M_2, M_3\}$	2	1	0.2500	0.2500	0.0000
$\{M_1, M_2, M_6\}$	3	0	0.2500	0.2500	0.0000
$\{M_2, M_3, M_4, M_5, M_6\}$	3	0	0.2500	0.2500	0.0000
$\{M_1, M_2, M_3, M_4\}$	1	2	0.1670	0.0830	0.0830
$\{M_1, M_2, M_3, M_6\}$	2	1	0.2080	0.1670	0.0420

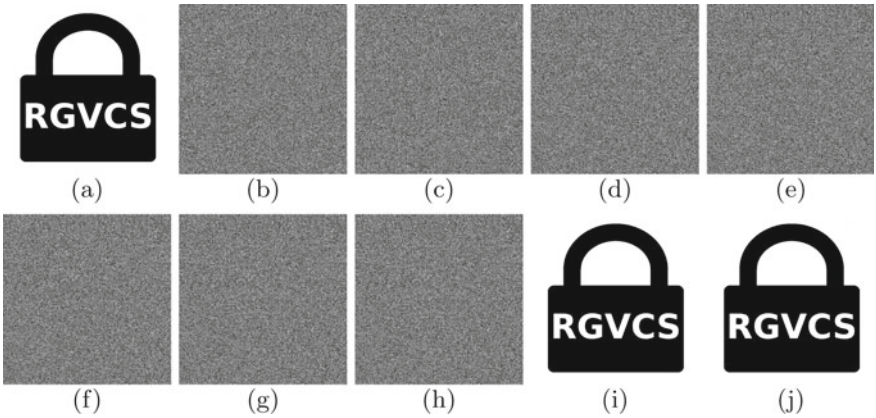


Fig. 1 The results for (2, 3, 5)-XRGVCS are implied. Here **(a)** the secret. stands for the random grid **(b)** G_1, **(c)** G_2, **(d)** G_3, **(e)** G_4, **(f)** G_5. The stacked images **(g)** $G_1 \oplus G_2$, **(h)** $G_1 \oplus G_2 \oplus G_3 \oplus G_4$, **(i)** $G_1 \oplus G_2 \oplus G_3 \oplus G_4 \oplus G_5$, **(j)** $G_1 \oplus G_2 \oplus G_3$, where the operation "$\oplus$" represents binary "XOR"

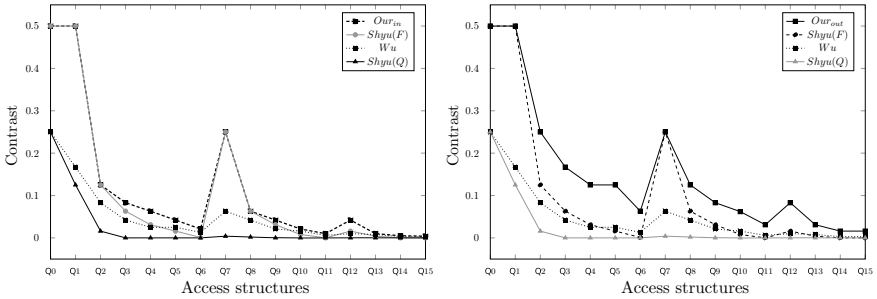
Remark 2 From the construction of our scheme, it is clear that we are doing nothing but repeated application of (k, k) scheme. So, to start with, we put $t = 0, k = n$ in our construction as described in Algorithm 1 and apply "XOR" operation in the secret reconstruction phase to get the following theorem.

4 Experiment and Discussions

In this section, we have shown the experimental as well as simulation results to validate our theoretical results. Before we proceed, let us first fix up few notations. Corresponding to an essential (t, k, n) access structure with valid parameters t, k, and n, let us denote $\mathscr{R}$ to be the set of all n random grids that are generated through the proposed Algorithm 1. Let $H \subseteq \mathscr{R}$ be such that $1 \leq h(=| H |) \leq n$. Python code is being used for experimental verification. The analytic light contrasts α_{OR}^{H} and α_{XOR}^{H} are compared in Tables 4 and 5. The comparison table of numerical values as

Table 2 Table of comparisons: proposed "OR"- and "XOR" -based schemes (See Fig. 3)

Access structures	OR		XOR	
	In	Out	In	Out
Q0: (1, 2, 3)	0.5000	0.5000	1.0000	1.0000
Q1: (1, 2, 4)	0.5000	0.5000	1.0000	1.0000
Q2: (1, 2, 5)	0.5000	0.5000	1.0000	1.0000
Q3: (1, 3, 4)	0.1250	0.2500	0.5000	1.0000
Q4: (1, 3, 5)	0.0830	0.1670	0.3330	0.6670
Q5: (1, 3, 6)	0.0630	0.1250	0.2500	0.5000
Q6: (1, 4, 5)	0.0420	0.1250	0.3330	1.0000
Q7: (1, 4, 6)	0.0210	0.0630	0.1670	0.5000
Q8: (2, 3, 4)	0.2500	0.2500	1.0000	1.0000
Q9: (2, 3, 5)	0.2500	0.2500	1.0000	1.0000
Q10: (2, 3, 6)	0.2500	0.2500	1.0000	1.0000
Q11: (2, 4, 5)	0.0630	0.1250	0.5000	1.0000
Q12: (2, 4, 6)	0.0420	0.0830	0.3330	0.6670
Q13: (3, 4, 5)	0.1250	0.1250	1.0000	1.0000
Q14: (3, 5, 6)	0.0310	0.0630	0.5000	1.0000
Q15: (3, 6, 7)	0.0100	0.0310	0.3330	1.0000



(i): Values that it takes "In" (ii): Values that it takes "Out"

Fig. 2 (i) and (ii) display the graphical representation of simulation data from the Table 1

well as the graphical representations of light contrast of our scheme with that of the already proposed general access structures restricted to customized (t, k, n) scenario are shown in Tables 1 and 2 and in Figs. 2 and 3 (Fig. 1 and Table 3).

The theoretical results α^H_{XOR} and the related experimental results $e\alpha^H_{\text{XOR}}$ and their differences are summarized in Table 5. Note that for each cases, $\alpha^H_{\text{XOR}} - e\alpha^H_{\text{XOR}} < 0.004$. This explains why the experimental outputs of the light contrast are very similar to the analytical values.

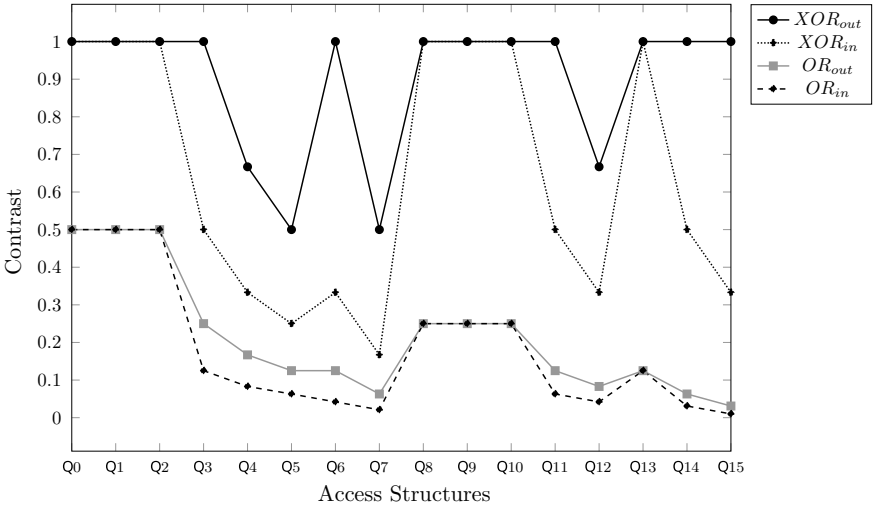


Fig. 3 Graphical representation of values, as shown in Table 2, for our "OR"- and "XOR"-based schemes

Table 3 Comparison of contrasts for different access structures (1, 2, 4) (See Fig. 4)

Set of members	Shyu (Q)	Shyu (F)	Wu	Our	
				In	Out
S0: $\{M_1\}$	0.0000	0.0000	0.0000	0.0000	0.0000
S1: $\{M_1, M_2\}$	0.1250	0.5000	0.1670	0.5000	1.0000
S2: $\{M_1, M_4\}$	0.1250	0.5000	0.1670	0.5000	1.0000
S3: $\{M_1, M_2, M_3\}$	0.1250	0.5000	0.1670	0.5000	NS
S4: $\{M_1, M_2, M_4\}$	0.1250	0.5000	0.1670	0.5000	NA
S5: $\{M_1, M_2, M_3, M_4\}$	0.1250	0.5000	0.1250	0.5000	NA

Table 4 The proposed (1, 2, 4)-RGVCS

Set of members: H	α^H_{OR}	$e\alpha^H_{\text{OR}}$	α^H_{XOR}	$e\alpha^H_{\text{XOR}}$
$\{M_1, M_2\}$	0.5000	0.5004	1.0000	1.0000
$\{M_1, M_4\}$	0.5000	0.5004	1.0000	1.0000
$\{M_2, M_3\}$	0.000	0.0000	0.0000	0.0000
$\{M_1, M_2, M_3\}$	0.5000	0.5000	NA	NA
$\{M_1, M_2, M_4\}$	0.5000	0.5000	NA	NA
$\{M_2, M_3, M_4\}$	0.0000	0.0000	NA	NA
$\{M_1, M_2, M_3, M_4\}$	0.5000	0.5004	NA	NA

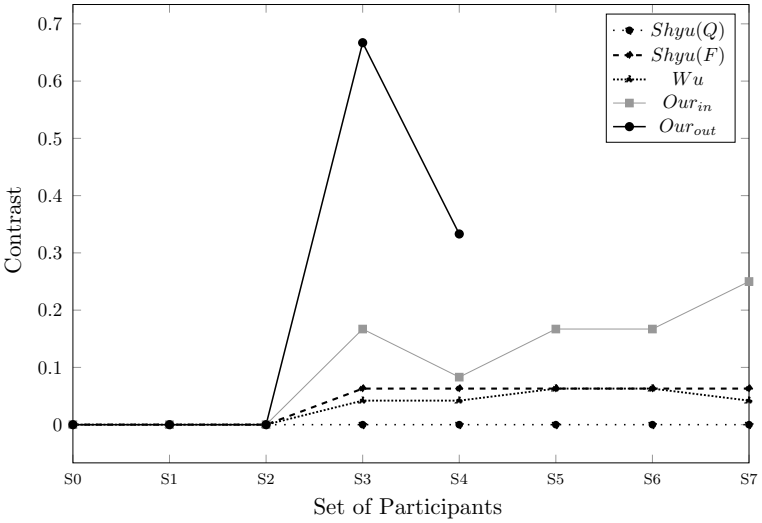


Fig. 4 (1, 2, 4)-RGVCS (See Table 3)

Table 5 The proposed (2, 3, 5)-RGVCS

Set of members: H	α_{OR}^{H}	$e\alpha_{\mathrm{OR}}^{H}$	$\alpha_{\mathrm{XOR}}^{H}$	$e\alpha_{\mathrm{XOR}}^{H}$
$\{M_1, M_2\}$	0.0000	0.0004	0.0000	0.0003
$\{M_1, M_2, M_3\}$	0.2500	0.2495	1.0000	1.0000
$\{M_1, M_2, M_5\}$	0.2500	0.2495	1.0000	1.0000
$\{M_2, M_3, M_4\}$	0.0000	0.0002	0.0000	0.0007
$\{M_1, M_2, M_3, M_4\}$	0.2500	0.2495	NA	NA
$\{M_1, M_2, M_3, M_5\}$	0.2500	0.2495	NA	NA
$\{M_2, M_3, M_4, M_5\}$	0.0000	0.0002	NA	NA
$\{M_1, M_2, M_3, M_4, M_5\}$	0.2500	0.2495	NA	NA

5 Conclusion

This paper puts forward efficient direct constructions of both "OR"- and "XOR"-based (t, k, n) schemes for random grid visual cryptographic schemes for black and white images. In the paper, we provide closed forms of light contrasts for both "OR" and "XOR" models. Our theoretical as well as experimental simulated results show that our algorithms work efficiently. As a a challenging future research work in the field of RGVCS, we will consider the problem of obtaining closed forms of the optimal light contrasts for both "OR" and "XOR" based VCSs for (t, k, n) access structure.

Acknowledgements The second author is thankful to the Council of Scientific and Industrial Research (CSIR), Government of India for providing financial support (Award No.09/028(0975)/2016-EMR-1). The research of the third author is partially supported by DST-SERB Project MATRICS vide Sanction Order: MTR/2019/001573.

References

1. Adhikari A, Sikdar S (2003) A new $(2, n)$-color visual threshold scheme for color images, INDOCRYPT'03. Lecture Notes in Computer Science. vol 2904. Springer, pp 148–161
2. Adhikari A, Bose M (2004) A new visual cryptographic scheme using latin squares. IEICE Trans Fundam Electron Commun Comput Sci 87(5):1198–1202
3. Adhikari A, Dutta TK, Roy BK (2004) A new black and white visual cryptographic scheme for general access structures. In: Progress in cryptology—INDOCRYPT 2004, 5th international conference on cryptology in India, Chennai, India, 20–22 Dec 2004, Proceedings, pp 399–413
4. Adhikari A, Bose M, Kumar D, Roy BK (2007) Applications of partially balanced incomplete block designs in developing $(2, n)$ visual cryptographic schemes. IEICE Trans 90-A(5):949–951
5. Adhikari A (2014) Linear algebraic techniques to construct monochrome visual cryptographic schemes for general access structure and its applications to color images. Des Codes Cryptogr 73(3):865–895
6. Adhikari MR, Adhikari A (2014) Basic modern algebra with applications. Springer
7. Blundo C, Bonis AD, Santis AD (2001) Improved schemes for visual cryptography. Des Codes Cryptogr 24(3):255–278
8. Blundo C, De Santis A, Stinson DR (1999) On the contrast in visual cryptography schemes. J Cryptol 12(4):261–289
9. Dutta S, Adhikari A (2014) XOR based non-monotone t-$(k, n)^*$ -visual cryptographic schemes using linear algebra. In: Information and communications security—16th international conference, ICICS 2014, Hong Kong, China, 16–17 Dec 2014, Revised Selected Papers, pp 230–242
10. Dutta S, Rohit RS, Adhikari A (2016) Constructions and analysis of some efficient t-$(k, n)^*$-visual cryptographic schemes using linear algebraic techniques. Des Codes Cryptogr 80(1):165–196
11. Dutta S, Roy PS, Adhikari A, Sakurai K (2017) On the Robustness of visual cryptographic schemes, IWDW 2016: digital forensics and watermarking. Springer, LNCS, pp 251–262
12. Dutta S, Adhikari A (2017) Contrast optimal XOR based visual cryptographic schemes. In Information theoretic security—10th international conference, ICITS 2017, Hong Kong, China, Nov 29–Dec 2, 2017, Proceedings, pp 58–72
13. Dutta S, Adhikari A, Ruj S (2018) Maximal contrast color visual secret sharing schemes. Des Codes Cryptogr
14. Ryo Ito HK, Takana H (1999) Image size invariant visual cryptography. IEICE Trans Fundam, E82-A(10):2172–2177
15. Kafri O, Keren E (1987) Encryption of pictures and shapes by random grids. Opt Lett 12(6):377–379
16. Lakshmanan R, Arumugam S (2017) Construction of a (k, n)-visual cryptography scheme. Des Codes Cryptogr 82(3):629–645
17. Naor M, Shamir A (1995) Visual cryptography, pp 1–12. Springer, Berlin, Heidelberg, Berlin, Heidelberg
18. Sardar MK, Adhikari A (2020) A new lossless secret color image sharing scheme with small shadow size. J Vis Commun Image Represent 102768
19. Sardar MK, Adhikari A (2020) New lossless secret image sharing scheme for gray scale images with small shadow size. COMSYS-2020, ISBN 978-981-15-7833-5

20. Sardar MK, Adhikari A (2020) Essential secret image sharing scheme with small and equal sized shadows. Signal Process: Image Commun 87:115923
21. Shyu SJ (2007) Image encryption by random grids. Pattern Recognit 40(3):1014–1031
22. Shyu SJ (2009) Image encryption by multiple random grids. Pattern Recognit 42(7):1582–1596
23. Shyu SJ (2013) Visual cryptograms of random grids for general access structures. IEEE Trans Circuits Syst Video Technol 23(3):414–424
24. Shyu SJ (2015) Visual cryptograms of random grids for threshold access structures. Theor Comput Sci 565:30–49
25. Shyu SJ, Chen MC (2015) Minimizing pixel expansion in visual cryptographic scheme for general access structures. IEEE Trans Circuits Syst Video Technol 25(9):1557–1561
26. Thien C-C, Lin J-C (2002) Secret image sharing. Comput Graph 26(5):765–770
27. Verheul ER, van Tilborg HCA (1997) Constructions and properties of k out of n visual secret sharing schemes. Des Codes Cryptogr 11(2):179–196
28. Wu X, Sun W (2012) Visual secret sharing for general access structures by random grids. IET Inform Secur 6(4):299–309
29. Yang C (2004) New visual secret sharing schemes using probabilistic method. Pattern Recognit Lett 25(4):481–494