Efficient Constructions for t-$(k, n)^*$-Random Grid Visual Cryptographic Schemes

Bibhas Chandra Das, Md Kutubuddin Saradr, Avishek Adhikari
Department of Pure Mathematics, University of Calcutta,
35 Ballygunge Circular Road,
Kolkata 700019, India
{bibhas.iitm, kutub.pmath, avishek.adh}@gmail.com

August 11, 2017

Abstract

In this paper we consider both "OR" and "XOR" based monochrome random grid visual cryptographic schemes (RGVCS) for t-$(k, n)^*$ access structure which is a generalization of the threshold (k, n) access structure in the sense that in all the successful attempts to recover the secret image, the t essential participants must always be present, i.e., a group of k or more participants can get back the secret if these t essential participants are among them. Up to the best of our knowledge, the current proposed work is the first in the literature of RGVCS which provides efficient direct constructions for the t-$(k, n)^*$-RGVCS for both "OR" and "XOR" model. Finding the closed form of light contrast is a challenging work. However, in this paper we come up with the closed forms of the light contrasts for the "OR" as well as for the "XOR" model. As our proposed schemes are the first proposed schemes for t-$(k, n)^*$-RGVCS, it is not possible for us to compare our schemes directly with the existing schemes. However, we have constructed t-$(k, n)^*$-RGVCS, as a particular case, from the random grid based schemes for general access structures. Theoretical as well as simulation based data show that our proposed schemes work much efficiently than all these customized schemes.

Keywords: Random Grid, essential participants, light contrast, monotone and non-monotone access structures.

1 Introduction

Visual cryptography is a cryptographic technique which allows visual information to be encrypted in such a way that decryption becomes the job of the person to decrypt via sight reading. Visual cryptography does not really require much sophisticated techniques that are normally used in other branches of cryptology like public key cryptosystem or symmetric key cryptosystem or even in other branches of secret sharing. Moreover, here the decryption process completely stands upon the human visual system. That is why visual cryptography attracts attention of many researchers. It was first introduced by Naor and Shamir in Eurocrypt'94[23]. They proposed a (k, n)-threshold scheme to distribute a secret image S among n participants in such a way that if any k (or more) of them superimpose their individual shares they get back S with a loss of contrast, while less than k participants have no information about S. A visual cryptographic scheme (VCS) with one essential participant was first introduced by Arungam et. al. [22] as an extension of threshold (k, n)-VCS. Their work was further generalized by Sabyasachi et. al. [15] to an access structure known as a t-$(k, n)^*$-VCS where $t(\leq k)$ is the number of essential participants who must always be present in all the successful attempts to recover the secret image. A group of k or more participants can get back the secret if those t essential participants are among them.

The works on visual cryptography, at the very initial stage, came with huge pixel expansion and very small contrast. That is why researchers started to think to apply different techniques to reduce the pixel expansion or to increase relative contrast. Probabilistic VCS was proposed to reduce the pixel expansion of a visual cryptography scheme. Ito et. al.[24] described a size invariant VSS scheme that encodes a white pixel (respectively black) by a column selected from a white (respectively black) basis matrix with equal probabilities. It was then Yang[35] who proposed a bunch of schemes to implement non expandable probabilistic VCS. But in all these the problem of selecting suitable basis matrices remained as it was. A detailed work on classical as well as probabilistic VCS may be found in [1], [2],[3],[4], [5], [6], [7], [8], [9], [10], [11], [14], [16], [17], [18], [19], [20], [26], [33].

Random Grid Visual Cryptography (RGVCS) is one of the solutions to all these problems. The main difference between RGVCS and conventional VCS is that RGVCS has no extra pixel expansion and does not really require to choose basis matrices. In RGVCS we treat each pixel of share as a random grid and assign color to it according to the corresponding secret pixel. For the already proposed schemes in the literature of RGVCS one can refer to [12],[13] [21], [25],[27], [28], [30], [31], [32].

This paper deals with efficient direct constructions of algorithms for both "OR" and "XOR" based t-$(k, n)^*$ schemes for RGVCS. Our theoretical as well as experimental simulated results show that our algorithms work much efficiently than the existing customized algorims proposed in [34] and [29] which are obtained as a particular case of general access structures.

The organization of the remaining part of the paper is as follows. In Section 2 we shall discuss some basic concepts of RGVCS and classical VCS that will be useful throughout the paper. Section 3 deals with our proposed efficient "OR" based scheme and related theoretical discussions and justifications with example to illustrate the theory behind the scheme. Section 4 deals with the theoretical justifications behind our proposed "XOR" based scheme. In Section 5, we will show by comparison and by various examples why our schemes are significant in the study of RGVCS. Finally, the paper ends with conclusion and discussions on future direction of research.

2 Preliminaries

In this section we will define some important terms related to VCS and RGVCS that will be required in our subsequent sections. Consider a secret pixel S to be shared among a set of n participants, say $\mathscr{P} = \{P_1, P_2, ..., P_n\}$. Let Γ_{Qual} be the collection of all subsets of $\mathscr{P}$ who can get the secret S back by superimposing their shares. Further let Γ_{Forb} be the collection of all those subsets of $\mathscr{P}$ who are unable to get the secret S back. We call each element of Γ_{Qual} as qualified set while each element of Γ_{Forb} is called a forbidden set. The ordered pair $(\Gamma_{Qual}, \Gamma_{Forb})$ is called an access structure for $\mathscr{P}$ corresponding to S. Given $\mathscr{B} \subseteq 2^P$, $\mathscr{B}$ is said to be monotone increasing if for all $B \in \mathscr{B}$ and $C \subseteq \mathscr{P}$ with $B \cap C = \emptyset$ we have $B \cup C \in \mathscr{B}$. Similarly $\mathscr{B}$ is said to be monotone decreasing if for all $B \in \mathscr{B}$ and $C \subseteq B$ we have $B \setminus C \in \mathscr{B}$. In case where Γ_{Qual} is monotone increasing, Γ_{Forb} is monotone decreasing and $\Gamma_{Qual} \cup \Gamma_{Forb} = 2^{\mathscr{P}}$, we say that the access structure is strong. Now we note that, for a strong access structure, a subset of a forbidden set is always forbidden and a super set of qualified set is always qualified. A participant $a \in \mathscr{P}$ is said to be essential if there exists $X \subseteq \mathscr{P}$ such that $X \cup \{a\} \in \Gamma_{Qual}$ but $X \notin \Gamma_{Qual}$. Given a strong access structure we define $Minimal\ Qualified\ set$ (Γ_0) and $Maximal\ forbidden\ set$ (Z_M) as follows:

$$\Gamma_0 = \{A \in \Gamma_{Qual} | A' \notin \Gamma_{Qual}, \forall A' \subset A\},$$
$$Z_M = \{B \in \Gamma_{Forb} | B \cup \{i\} \in \Gamma_{Qual}, \forall i \in \mathscr{P} \setminus B\}.$$

For a (k, n) threshold access structure, $\Gamma_{Qual} = \{Q \subseteq \mathscr{P} : |Q| \geq k\}$ and $\Gamma_{Forb} = \{F \subseteq \mathscr{P} : |F| < k\}$, where $2 \leq k \leq n$. By a t-$(k, n)^*$ access structure, we mean that it is a (k, n) scheme where t of the n participants are essential. In a t-$(k, n)^*$ monotone access structure, a maximal forbidden set can be of the following two types. Type I: Sets of size $k-1$ sets containing all the essential participants. Type II: Sets of size $n-1$ containing all but one of the t essential participants. Mathematically:

$$Z_M = \Big\{\{i_1, i_2, \ldots, i_{k-1}\} | i_j = P_j \text{ for } 1 \leq j \leq t; i_j \in \{P_{t+1}, P_{t+2}, \ldots, P_n\} \text{ for } t+1 \leq j \leq k-1\Big\} \cup \Big\{\{P_1, P_2, \ldots, P_n\} \setminus \{P_j\} | j \in \{1, 2, \ldots, t\}\Big\}.$$

On the other hand if we assume that the t essential participants are the first t participants from the set $\mathscr{P} = \{1, 2, \ldots, n\}$, then the minimal qualified sets for the t-$(k, n)^*$ access structure are described by the set of k participants where these t essential participants are always there. Thus the collection of all minimal qualified sets for the t-$(k, n)^*$ monotone access structure is described as

$$\Gamma_0 = \left\{ \{i_1, i_2, ..., i_k\} : i_j = P_j \text{ for } 1 \leq j \leq t; i_j \in \{P_{t+1}, P_{t+2}, ..., P_n\} \text{ for } t+1 \leq j \leq k \right\}.$$

Now we are going to define the concept of grid based VCS. As in [30], we consider a binary transparency Y in which each pixel y is either transparent (0) or opaque (1). Suppose that the value of each pixel y is determined by a biased coin-flip procedure with parameter λ such that the probability of $y = 0$ is λ. We refer to y as a random pixel with $\Pr(y = 0) = \lambda$. Due to the fact that $y = 0$ lets through light, while $y = 1$ stops it, we define the light transmission of y, denoted by $\mathscr{t}(y)$, to be $Pr(y = 0)$. Formally, the light transmission of a random pixel is defined as follows.

Definition 2.1. *[30] A random pixel y is said to have a light transmission $\mathscr{t}(y) = \lambda$ if $Pr(y = 0) = \lambda$, where λ is a constant such that $0 < \lambda < 1$.*

Once $\mathscr{t}(y) = \lambda$ for each pixel $y \in Y$, we call Y a random grid, defined as follows.

Definition 2.2. *[30] A random grid Y is said to have a light transmission of $\mathscr{T}(Y) = \lambda$ if $\mathscr{t}(y) = \lambda$ for each pixel $y \in Y$.*

Property 1. *[30] If X is a random grid with $\mathscr{T}(X) = \lambda$, then $X \otimes X$ is also a random grid with $\mathscr{T}(X \otimes X) = \mathscr{T}(X) = \lambda$, where $\otimes$ denotes Boolean "OR" operation.*

Property 2. *[30] If X and Y are two independent random grids with $\mathscr{T}(X) = \lambda_1$ and $\mathscr{T}(Y) = \lambda_2$, then $\mathscr{T}(X \otimes Y) = \lambda_1\lambda_2$.*

Notation: As in [27], let $S(0)$ ($S(1)$) denote the area of all of the transparent (opaque) pixels in the secret image S, i,e., ijth pixel $S[i, j]$ of the secret S is in $S(0)$ ($S(1)$) if and only if $S[i, j] = 0$ ($S[i, j] = 1$) where $S = S(0) \cup S(1)$ and $S(0) \cap S(1) = \emptyset$. Likewise, we denote the area of pixels in random grid R corresponding to $S(0)(S(1))$ by $R[S(0)]$ ($R[S(1)]$), i.e., ijth pixel $R[i, j]$ of the random grid R is in $R[S(0)]$ ($R[S(1)]$) if and only if $R[i, j]$'s corresponding pixel $S[i, j]$ is in $S(0)(S(1))$. Needless to mention, $R = R[S(0)] \cup R[S(1)]$ and $R[S(0)] \cap R[S(1)] = \emptyset$.

Definition 2.3. *Given an $N \times M$ binary secret image S and valid parameters t, k and n for t-$(k, n)^*$ strong access structure on the set of n participants, the set of random grids $\mathscr{R} = \{R_1, R_2, \ldots, R_n\}$ forms an "OR" based t-$(k, n)^*$-RGVCS for the secret image S if the following conditions are satisfied.*

1. *$\mathscr{T}(R_j) = \frac{1}{2}$ for all $1 \leq j \leq n$.*

2. *Let $\mathscr{F}$ denote the collection of all maximal forbidden sets for the t-$(k,n)^*$ access structure. Then for each $F = \{P_{i_1}, P_{i_2}, \ldots, P_{i_p}\} \in \mathscr{F}$, $\mathscr{T}(R^F[S(0)]) = \mathscr{T}(R^F[S(1)])$, where $R^F = R_{i_1} \otimes R_{i_2} \otimes \cdots \otimes R_{i_p}$, i.e., $\mathscr{t}(R^F[i,j] \mid S[i,j] = 0) = \mathscr{t}(R^F[i,j] \mid S[i,j] = 1)$, $\forall\ i, j$.*

3. *Let $Q \in \Gamma_0$, where Γ_0 denotes the collection of all minimal qualified sets. Then $\mathscr{T}(R^Q[S(0)]) > \mathscr{T}(R^Q[S(1)])$ where $R^Q = R_1 \otimes R_2 \otimes \cdots \otimes R_q$, i.e., $\mathscr{t}(R^Q[i,j] \mid S[i,j] = 0) > \mathscr{t}(R^Q[i,j] \mid S[i,j] = 1)$, $\forall\ i, j$.*

Definition 2.4. *For a given t-$(k,n)^*$-RGVCS, the light contrast for a given set $H \subseteq \mathscr{P}$, denoted as α_{OR}^H, is defined as*

$$\alpha_{OR}^H = \mathscr{T}(R^H[S(0)]) - \mathscr{T}(R^H[S(1)]).$$

3 Proposed "OR" Based Scheme

In this section we propose an efficient method for constructing a t-$(k,n)^*$-RGVCS for strong access structure.

3.1 Construction

In the proposed scheme, based on a secret $N \times M$ binary image S, the trusted Dealer first constructs the shares depending on the given strong t-$(k,n)^*$ access structure and then distributes these constructed shares among the participants. For that the dealer first selects the essential participants and marks them as $P_1, P_2, \ldots, P_t$. The rest of the participants are marked as $P_{t+1}, P_{t+2}, \ldots, P_{n-1}, P_n$. Let $S[i,j]$ denote the ijth pixel of the secret image S. Let us explain our proposed method for one secret pixel $S[i,j]$ from the secret image S. For the construction of shares, for each secret pixel $S[i,j]$, the dealer selects $k-1-t$ participants randomly from $P_{t+1}, P_{t+2}, \ldots, P_{n-1}$. These participants together with the essential ones form a set A of size $k-1$. Then the dealer assigns them random grids 0 or 1. Now by applying the function f, defined below, the dealer generates a new share and assigns it to all of the remaining participants. The function f is defined as follows:

$$f(s,x) = s \oplus x, \tag{1}$$

where $\oplus$ denotes binary "XOR" operation, $s, x \in \{0,1\}$.

Detailed description of the share generation algorithm by the dealer is described in Algorithm 1.

Algorithm 1: An efficient algorithm for constructing a t-$(k,n)^*$-RGVCS

Input: A binary secret image S of size $N \times M$, and a strong access structure t-$(k,n)^*$ for valid parameters t, k, n.

Output: n shares R_1, R_2, …, R_n each of size $N \times M$.

Select the t essential participants from the set $\mathscr{P}$ of n participants and denote them as $P_1, P_2, \ldots, P_t$. Denote the rest of the participants as P_{t+1}, P_{t+2}, $\ldots$, P_{n-1}, P_n.
for $(i = 1; i \leq N; i++)$ **do**
    for $(j = 1; j \leq M; j++)$ **do**
        Generate $(k-1)$ random grids $r_1[i,j], r_2[i,j], \ldots, r_{k-1}[i,j]$
        Randomly select $k-t-1$ participants, say $P_{l_1}, P_{l_2}, \ldots, P_{l_{k-t-1}}$ from $\{P_{t+1}, P_{t+2}, \ldots, P_{n-1}\}$. Let $A = \{P_1, P_2, \ldots, P_t, P_{l_1}, P_{l_2}, \ldots, P_{l_{k-t-1}}\}$
        Construct $a_1[i,j], a_2[i,j], \ldots, a_k[i,j]$ as

$$
\begin{aligned}
a_1[i,j] &= r_1[i,j]\\
a_p[i,j] &= f(r_p[i,j], a_{p-1}[i,j]) \; \forall p = 2, 3, \ldots, k-1\\
a_k[i,j] &= f(S[i,j], a_{k-1}[i,j])
\end{aligned}
$$

        for $(q = 1; q \leq t; q++)$ **do**
            $R_q[i,j] \leftarrow r_q[i,j]$
        end
        for $(q = 1; q \leq k-t-1; q++)$ **do**
            $R_{l_q}[i,j] \leftarrow r_{t+q}[i,j]$
        end
        $R_s[i,j] \leftarrow a_k[i,j]$, for all $s \in \{1, 2, \ldots, n\} \setminus \{1, 2, \ldots, t, l_1, l_2, \ldots, l_{k-t-1}\}$.
    end
end
Participant P_i is given the share R_i, $i = 1, 2, \ldots, n$.

3.2 Discussion on Light Transmission

In this section we are going to prove the correctness of the Algorithm 1 by showing that the collection of the random grids as an output of the Algorithm 1 satisfies the conditions of Definition 2.3. Before that let us fix one notation.

Notation: In Algorithm 1, we have seen that for each secret pixel $S[i,j]$, a set A is generated. Let $\mathscr{A}$ denote the collection of all possible A's.

Let us now proceed by proving the following three Lemmas for a given strong access structure.

Lemma 1. *The light transmission* $\mathscr{T}(R_i) = \dfrac{1}{2}$ *for* $1 \leq i \leq n$.

Proof. A single share R_i is either a random grid or it is generated by using the function f as defined in Equation (1). The rest of the proof follows from [**?**].

As the given access structure is a strong access structure, it is sufficient to discuss the light transmission only for the maximal forbidden sets and for the minimal qualified sets.

Lemma 2. *For a given t-$(k,n)^*$-RGVCS, let $\{R_{l_1}, R_{l_2}, \ldots, R_{l_m}\}$ denote the set of shares, obtained in Algorithm 1, corresponding to a maximal forbidden set of participants $F = \{P_{l_1}, P_{l_2}, \ldots, P_{l_m}\}$. Then*

$$\mathscr{T}(R^F[S(0)]) = \mathscr{T}(R^F[S(1)]),$$

where $R^F = R_{l_1} \otimes R_{l_2} \otimes \cdots \otimes R_{l_m}$ and $\otimes$ denotes binary "OR" operation.

Proof. Recall that a maximal forbidden set can be of the following two types. Type I: Sets of size $k-1$ containing all the t essential participants. Type II: Sets of size $n-1$ containing all but one of the t essential participants.

For Type I sets, while calculating the light transmission, they behave like a set of size $\leq k-1$ of a (k,k)-scheme. For different choices of $A \in \mathscr{A}$, the light transmission would be different. Let us start with a forbidden set F of Type I. Now we will try to explicitly write down how this set F behaves under different choices of $A \in \mathscr{A}$. The main thing is that we have to look at the number of shares in the intersection of A and F. Let for a particular choice of A, $\mid F \cap A \mid = h$. Light transmission for these sets is given by:

$$t(R^F[i,j] | S[i,j] = 0) = \frac{1}{2^{h+1}} = t(R^F[i,j] | S[i,j] = 1).$$

If $P_n \in F$ then h can run from t to $k-2$. In that case we can choose $A \in \mathscr{A}$ in $\binom{k-2-t}{h-t} \times \binom{n-k+1}{k-1-h}$ many ways such that the cardinality of the intersection can be h. But if $P_n \notin F$ the number of choices of A, where this happens, becomes $\binom{k-1-t}{h-t} \times \binom{n-k}{k-1-h}$. In this case, $\mid F \cap A \mid$ not only runs over t to $k-2$ but also can be $k-1$ and the latter case is a unique case.

So we get the the total light transmission of F as:

$$
\begin{aligned}
&t(R^F[i,j]|S[i,j]=0)\\
&=t(R^F[i,j]|S[i,j]=0)\\
&=\frac{1}{\binom{n-1-t}{k-1-t}}\left[\sum_{h=t}^{k-2}\frac{\binom{k-2-t}{h-t}\times\binom{n-k+1}{k-1-h}}{2^{h+1}}\right], \text{ if } P_n\in F\\
&=\frac{1}{\binom{n-1-t}{k-1-t}}\left[\frac{1}{2^{k-1}}+\sum_{h=t}^{k-2}\frac{\binom{k-1-t}{h-t}\times\binom{n-k}{k-1-h}}{2^{h+1}}\right], \text{ if } P_n\notin F.
\end{aligned}
$$

Again for Type II sets, for all choices of $\mathscr{A}$, they behave like sets of size $k-1$ of a (k,k)-scheme. So for these F's light transmission would be

$$t(R^F[i,j]|S[i,j]=0)=\frac{1}{2^{k-1}}=t(R^F[i,j]|S[i,j]=1).$$

This proves the security of our proposed scheme.

Lemma 3. *For a given t-$(k,n)^*$-RGVCS, let $\{R_{l_1},R_{l_2},\ldots,R_{l_q}\}$ denote the set of shares, obtained in Algorithm 1, corresponding to a minimal qualified set of participants $Q=\{P_{l_1},P_{l_2},\ldots,P_{l_q}\}$. Then*

$$\mathscr{T}(R^Q[S(0)])>\mathscr{T}(R^Q[S(1)]).$$

Proof. The minimal qualified sets in the scheme are those having k participants of which t are essential. Mathematically

$$\Gamma_0=\left\{\{i_1,i_2,...,i_k\}|i_j=P_j \text{ for } 1\le j\le t; i_j\in\{P_{t+1},P_{t+2},...,P_n\} \text{ for } t+1\le j\le k\right\}.$$

Let us start with such a minimal qualified set Q. Again as in Lemma 2, to find the light transmission of Q, we have to look for $\mid Q\cap A\mid$. Now $\mid Q\cap A\mid$ can run over t to $k-1$. If $P_n\in Q$ then we have $\binom{k-1-t}{h-t}\times\binom{n-k}{k-1-h}$ choices of A where $\mid Q\cap A\mid=h$, $h<k-1$ and it becomes $k-1$ uniquely. But if $P_n\notin Q$ then we have $\binom{k-t}{h-t}\times\binom{n-1-k}{k-1-h}$ choices of A where $\mid Q\cap A\mid=h$, $h<k-1$ and for $\binom{k-t}{k-1-t}$, i.e. $k-t$ choices it becomes $k-1$. So as

a whole light transmission of stacked share for Q is:

$$
\begin{aligned}
&t(R^Q[i,j]|S[i,j]=0)\\
&=\frac{1}{\binom{n-1-t}{k-1-t}}\left[\frac{1}{2^{k-1}}+\sum_{h=t}^{k-2}\frac{\binom{k-1-t}{h-t}\times\binom{n-k}{k-1-h}}{2^{h+1}}\right], \text{ if } P_n\in Q\\
&=\frac{1}{\binom{n-1-t}{k-1-t}}\left[\frac{k-t}{2^{k-1}}+\sum_{h=t}^{k-2}\frac{\binom{k-t}{h-t}\times\binom{n-1-k}{k-1-h}}{2^{h+1}}\right], \text{ if } P_n\notin Q.
\end{aligned}
$$

And

$$
\begin{aligned}
&t(R^Q[i,j]|S[i,j]=1)\\
&=\frac{1}{\binom{n-1-t}{k-1-t}}\left[\sum_{h=t}^{k-2}\frac{\binom{k-1-t}{h-t}\times\binom{n-k}{k-1-h}}{2^{h+1}}\right], \text{ if } P_n\in Q\\
&=\frac{1}{\binom{n-1-t}{k-1-t}}\left[\sum_{h=t}^{k-2}\frac{\binom{k-t}{h-t}\times\binom{n-1-k}{k-1-h}}{2^{h+1}}\right], \text{ if } P_n\notin Q.
\end{aligned}
$$

So light contrast for Q is :

$$
\alpha_{OR}^{Q}=\begin{cases}\dfrac{1}{\binom{n-1-t}{k-1-t}}\cdot\dfrac{1}{2^{k-1}}, & P_n\in Q,\\ \dfrac{1}{\binom{n-1-t}{k-1-t}}\cdot\dfrac{k-t}{2^{k-1}}, & P_n\notin Q.\end{cases}
$$

The contrast being a strictly positive quantity we can easily say that the scheme obeys the contrast conditions of RGVCS.
Thus we can now state the following theorem:

Theorem 3.1. *For a given secret binary image S and a given strong t-$(k,n)^*$ threshold access structure with valid parameters t, k and n, the proposed scheme as described in Algorithm 1 is a t-$(k,n)^*$-RGVCS with light contrast for a minimal qualified set:*

$$
\alpha_{OR}^{Q}=\begin{cases}\dfrac{1}{\binom{n-1-t}{k-1-t}}\cdot\dfrac{1}{2^{k-1}}, & \text{if } P_n\in Q,\\ \dfrac{1}{\binom{n-1-t}{k-1-t}}\cdot\dfrac{k-t}{2^{k-1}}, & \text{if } P_n\notin Q.\end{cases}
$$

Proof. The proof of the theorem is very much clear from Lemma 1, Lemma 2 and Lemma 3.

Remark 1. *In general we can do the same thing for any qualified set of participants. The light transmission for any qualified set Q of size q will be :*

$$\begin{aligned}
&t(R^Q[i,j]|S[i,j]=0)\\
&= \frac{1}{\binom{n-1-t}{k-1-t}}\left[\frac{\binom{q-1-t}{k-1-t}}{2^{k-1}} + \sum_{h=t}^{k-2}\frac{\binom{q-1-t}{h-t}\times\binom{n-q}{k-1-h}}{2^{h+1}}\right],\\
&\text{if } P_n \in Q\\
&= \frac{1}{\binom{n-1-t}{k-1-t}}\left[\frac{\binom{q-t}{k-1-t}}{2^{k-1}} + \sum_{h=t}^{k-2}\frac{\binom{q-t}{h-t}\times\binom{n-1-q}{k-1-h}}{2^{h+1}}\right],\\
&\text{if } P_n \notin Q.
\end{aligned}$$

and

$$\begin{aligned}
&t(R^Q[i,j]|S[i,j]=1)\\
&= \frac{1}{\binom{n-1-t}{k-1-t}}\left[\sum_{h=t}^{k-2}\frac{\binom{q-1-t}{h-t}\times\binom{n-q}{k-1-h}}{2^{h+1}}\right], \text{ if } P_n \in Q\\
&= \frac{1}{\binom{n-1-t}{k-1-t}}\left[\sum_{h=t}^{k-2}\frac{\binom{q-t}{h-t}\times\binom{n-1-q}{k-1-h}}{2^{h+1}}\right], \text{ if } P_n \notin Q.
\end{aligned}$$

So light contrast for Q is :

$$\alpha_{OR}^{Q} = \begin{cases} \frac{1}{\binom{n-1-t}{k-1-t}} \cdot \frac{\binom{q-1-t}{k-1-t}}{2^{k-1}}, & \text{if } P_n \in Q,\\ \frac{1}{\binom{n-1-t}{k-1-t}} \cdot \frac{\binom{q-1-t}{k-1-t}}{2^{k-1}}, & \text{if } P_n \notin Q. \end{cases}$$

Example 3.1. *Let us now illustrate the whole theoretical computation through an example of t-$(k,n)^*$-RGVCS with the parameters as $t=2, k=4$ and $n=6$.*

As we have discussed in the proofs of Lemma 1, Lemma 2 and Lemma 3, the light contrast of the set of participants (say H) mainly depends on $|H \cap A|$, where $A \in \mathscr{A}$. So, to start with, let us first identify $\mathscr{A}$ for this specific case. In the current example,

$$\mathscr{A} = \{\{P_1, P_2, P_3\}, \{P_1, P_2, P_4\}, \{P_1, P_2, P_5\}\}.$$

We further identify the maximal forbidden set Z_M and the minimal qualified set Γ_0 respectively as:

$$Z_M = \{\{P_1, P_2, P_3\}, \{P_1, P_2, P_4\}, \{P_1, P_2, P_5\}, \{P_1, P_2, P_6\},$$
$$\{P_2, P_3, P_4, P_5, P_6\}, \{P_1, P_3, P_4, P_5, P_6\}\},$$
$$\Gamma_0 = \{\{P_1, P_2, P_3, P_4\}, \{P_1, P_2, P_3, P_5\}, \{P_1, P_2, P_3, P_6\},$$
$$\{P_1, P_2, P_4, P_5\}, \{P_1, P_2, P_4, P_6\}, \{P_1, P_2, P_5, P_6\}\}.$$

Clearly, for $H \in Z_M \cup \Gamma_0$, $|H \cap A|$ can be 2 or 3. Note that, the light transmission of the stacked shares corresponding to the set of participants H depends on whether P_6 is an element of the set or not. Keeping this in mind we have categorized all the set of participants as "In" and "Out", where "In" means $P_6 \in H$ and "Out" means $P_6 \notin H$. Clearly, the elements $\{P_1, P_2, P_3\}, \{P_1, P_2, P_4\}, \{P_1, P_2, P_5\}$ of $\mathscr{A}$ of type I maximal forbidden sets have same behaviour under different choices of A whereas $\{P_1, P_2, P_6\}$ acts differently. On the other hand, the two type II maximal forbidden sets for this access structure being in "Out" category have same behaviour. Again, the elements of maximal qualified sets $\{P_1, P_2, P_3, P_4\}$, $\{P_1, P_2, P_3, P_5\}$ and $\{P_1, P_2, P_4, P_5\}$ are all in "Out" category and $\{P_1, P_2, P_3, P_6\}$, $\{P_1, P_2, P_4, P_6\}$, $\{P_1, P_2, P_5, P_6\}$ are all in "In" category. So, discussion on light transmission for $\{P_1, P_2, P_3\}$, $\{P_1, P_2, P_6\}$, $\{P_2, P_3, P_4, P_5, P_6\}$, $\{P_1, P_2, P_3, P_4\}$ and $\{P_1, P_2, P_3, P_6\}$ will be sufficient.

Let $H = \{P_1, P_2, P_3\}$. Then $|H \cap A|$ is 2 for $\binom{4-1-2}{2-2} \times \binom{6-4}{4-1-2}$, i.e., 2 choices of A and it is 3 for a unique case. Now, if $H = \{P_1, P_2, P_6\}$, then $|H \cap A|$ is 2 for $\binom{4-2-2}{2-2} \times \binom{6-4+1}{4-1-2}$, i.e., for all the choices of A. Again, if $H = \{P_2, P_4, P_5, P_6\}$, then $|H \cap A|$ is always 2. Now, for the qualified ones first let $H = \{P_1, P_2, P_3, P_4\}$, then $|H \cap A|$ is 2 for $\binom{4-2}{2-2} \times \binom{6-1-4}{4-1-2}$, i.e., for only 1 choice of A and it is 3 for $4-2$, i.e., 2 choices of A. Lastly, take $H = \{P_1, P_2, P_3, P_6\}$, then $|H \cap A|$ is 2 for $\binom{4-1-2}{2-2} \times \binom{6-4}{4-1-2}$, i.e., 2 choices of A and it is 3 for a unique choice of A.

In Table 1, we have verified the corresponding light contrasts of H using these data.

Remark 2. *If we have a deeper look at the algorithm as described in Algorithm 1, we see that when constructing the $k-1$ set $A \in \mathscr{A}$, we have never selected P_n as an element of A. But if we include it in our choice then also we will get a scheme for t-$(k,n)^*$-RGVCS. The light contrast for that scheme can also be calculated exactly in the same manner as we have done in Theorem 3.1. Notice that in our Algorithm 1, P_n is treated*

Set of Participants: H	$n_2(A)$	$n_3(A)$	$\mathscr{T}(R^H[S(0)])$	$\mathscr{T}(R^H[S(1)])$	α_{OR}^H
$\{P_1, P_2, P_3\}$	2	1	0.250	0.250	0.000
$\{P_1, P_2, P_6\}$	3	0	0.250	0.250	0.000
$\{P_2, P_3, P_4, P_5, P_6\}$	3	0	0.250	0.250	0.000
$\{P_1, P_2, P_3, P_4\}$	1	2	0.167	0.083	0.083
$\{P_1, P_2, P_3, P_6\}$	2	1	0.208	0.167	0.042

Table 1: Verification table of light contrast for the access structure 2-$(4,6)^*$-RGVCS, where $n_2(A)$ and $n_3(A)$ denote the number of choices of A for which $|H \cap A|$ is 2 and 3 respectively.

same as the other non essential participants. So, for the current case, when calculating the light transmission of some set, two cases as occurred earlier, will not arise. So light transmission for all the sets of a fixed length will be the same. As a result, instead of $\binom{n-1-t}{k-1-t}$, *we will have* $\binom{n-t}{k-1-t}$ *choices for selecting the* $k-1$ *set. So in a nutshell we can have the following theorem.*

Theorem 3.2. *Given a secret binary image S and n participants, of which t are essential, sharing the secret binary image S with a threshold value k, the above procedure, described in Remark 2, produces a t-$(k,n)^*$-RGVCS with light contrast $\bar{\alpha}_{OR}^Q$ for a minimal qualified set $Q \subseteq \mathscr{P}$ and is given by*

$$\bar{\alpha}_{OR}^Q = \frac{1}{\binom{n-t}{k-1-t}} \cdot \frac{1}{2^{k-1}}.$$

Note: It is clear from the closed forms of $\bar{\alpha}_{OR}^Q$ and α_{OR}^Q (even in "In" case) that, α_{OR}^Q gives higher value than $\bar{\alpha}_{OR}^Q$ and they become same when $t = k-1$.

3.3 Comparison with the Schemes Proposed by Wu and Sun [34] and Shyu [29]

Up to the best of our knowledge, our proposed scheme is the first proposed scheme for t-$(k,n)^*$-RGVCS. As a result, it is not possible for us to compare our scheme with the existing schemes. However, we can construct t-$(k,n)^*$-RGVCS, as particular cases, from the random grid based schemes for general access structures. In this section we are going to compare our proposed Algorithm 1 with the customized schemes, obtained as a particular case from general access structures proposed in [34] and [29] which are, upto the best of our knowledge, the most efficient schemes for general access structures that exist in the literature.

If we apply the scheme proposed in [34] on the access structure for t-$(k,n)^*$ we have the following theorem:

Theorem 3.3. *(customized from [34]) For a given secret binary image S and valid parameters t, k and n for a t-$(k, n)^*$ access structure, the scheme described in [34] produces a t-$(k, n)^*$-RGVCS with light contrast:*

$$\alpha_w = \frac{1}{\binom{n-t}{k-t}} \cdot \frac{1}{2^{k-1}}.$$

If we apply the scheme proposed by Shyu [29] on the access structure for t-$(k, n)^*$ we have the following theorem:

Theorem 3.4. *(customized from [29]) For a given secret binary image S and valid parameters t, k and n for a t-$(k, n)^*$ access structure, the scheme described in [29] produces a t-$(k, n)^*$-RGVCS with light contrast:*

$$\alpha_s = \tfrac{1}{2^{\mathscr{K}}}, \textit{ where } \mathscr{K} = 1 + \sum_{h=t}^{k-1} \binom{k-t}{h-t} \binom{n-k}{k-h} h.$$

Remark 3. *It is not difficult to check that the light contrast for our scheme is better than that of the schemes proposed in [34] and [29]. Numerical evidences from Table 2 show that our scheme performs much better than the existing schemes in terms of light contrast.*

4 Non Monotone Access Structure: "XOR" Based Scheme

Our construction of t-$(k, n)^*$-RGVCS uses binary "OR" operation at secret reconstruction phase. In literature we have visual cryptographic schemes where the secret reconstruction is done by binary "XOR" operation instead of "OR" operation. Keeping that in mind we will now apply the "XOR" operation to our construction with an intuition that it will result to a non-monotone access structure for t-$(k, n)^*$-XOR-based Random Grid VCS, we call it as t-$(k, n)^*$-XRVCS. The reason of saying the specific kind of access structure as non-monotone is that there is no guarantee for a super set of a minimal qualified set to be a qualified set again. The definitions for t-$(k, n)^*$-XRGVCS and the corresponding light contrast are similar to that of the Definition 2.3 and Definition 2.4, except for the fact that instead of applying "OR" operation we shall use "XOR" operation for superimposition of shares. We denote the light contrast corresponding to a set of participants $H \subseteq \mathscr{P}$ for a t-$(k, n)^*$-XRGVCS by α^H_{XOR}.

Remark 4. *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.*

Theorem 4.1. *If we put $t = 0$, $k = n$ in our construction as described in Algorithm 1 and replace the binary "OR" operation by "XOR" operation in the reconstruction phase, we obtain a (k, k)-XRGVCS with perfect light contrast* 1.

Proof. Firstly, for single shares $R_i, 1 \leq i \leq n$, as we have discussed previously, $\mathscr{T}(R_i) = \frac{1}{2}, \forall 1 \leq i \leq n$.

In this specific access structure the maximal forbidden sets are the sets of participants with cardinality $(k-1)$. When participants of such a set try to get back the secret by "XOR"ing their corresponding shares, the following two cases arise:

Case I: It may happen that all the $(k-1)$ pixels corresponding to chosen secret pixel are assigned with random grids. Then

$$\begin{aligned}
&t(R^F[i,j] \mid S[i,j]=0) \\
&= \Pr(R^F[i,j]=0 \mid S[i,j]=0) \\
&= \Pr(r_1[i,j] \oplus \cdots \oplus r_{k-1}[i,j]=0 \mid S[i,j]=0) \\
&= \Pr(r_1[i,j] \oplus \cdots \oplus r_{k-1}[i,j]=0) \\
&= \Pr(r_1[i,j] \oplus \cdots \oplus r_{k-1}[i,j]=0 \mid S[i,j]=1) \\
&= \Pr(R^F[i,j]=0 \mid S[i,j]=1) \\
&= t(R^F[i,j] \mid S[i,j]=1).
\end{aligned}$$

Case II: It may also happen that one of the pixels, say $r_k[i,j]$ is assigned with the grid generated by f function as described in Equation 1. Then

$$\begin{aligned}
&t(R^F[i,j] \mid S[i,j]=0) \\
&= \Pr(R^F[i,j]=0 \mid S[i,j]=0) \\
&= \Pr(r_1[i,j] \oplus \cdots \oplus r_{k-2}[i,j] \\
&\qquad\qquad \oplus a_k[i,j]=0 \mid S[i,j]=0) \\
&= \Pr(S[i,j] \oplus r_{k-1}[i,j]=0 \mid S[i,j]=0) \\
&= \Pr(r_{k-1}[i,j]=0 \mid S[i,j]=0) \\
&= \Pr(r_{k-1}[i,j]=1 \mid S[i,j]=1) \\
&= \Pr(S[i,j] \oplus r_{k-1}[i,j]=0 \mid S[i,j]=1) \\
&= \Pr(R^F[i,j]=0 \mid S[i,j]=1) \\
&= t(R^F[i,j] \mid S[i,j]=1).
\end{aligned}$$

Now for the minimal qualified set, that is to say for the set of all k participants:

$$\begin{aligned}
&\not{t}(R^F[i,j] \mid S[i,j]=0)\\
&= \Pr(r_1[i,j] \oplus \cdots \oplus r_{k-1}[i,j] \oplus a_k[i,j] = 0 \mid S[i,j]=0)\\
&= \Pr(S[i,j]=0 \mid S[i,j]=0)\\
&= 1
\end{aligned}$$

and

$$\begin{aligned}
\not{t}(R^F[i,j] \mid S[i,j]=1) &= \Pr(S[i,j]=0 \mid S[i,j]=1)\\
&= 0.
\end{aligned}$$

Hence we have the theorem.

The following theorem shows what will happen if we apply the same above technique to Algorithm 3 of [30]. We put (S) in the expression $\alpha^{Q}_{XOR}(S)$ to emphasize that the method is originated from the scheme proposed by Shyu in [30].

Theorem 4.2. *If we replace the "OR" operation by "XOR" operation in the reconstruction phase of Algorithm 3 of [30], then the modified scheme leads to a non-monotone (k,n)-XRGVCS with light contrast $\alpha^{Q}_{XOR}(S)$ for the minimal qualified set Q, which is given by*

$$\alpha^{Q}_{XOR}(S) = \frac{1}{\binom{n}{k}}.$$

Proof. Firstly, for single shares $R_i, 1 \leq i \leq n$, as we have discussed previously, $\mathscr{T}(R_i) = \frac{1}{2}, \forall 1 \leq i \leq n$.

If we look back at the construction of Algorithm 3 of [30] we note that the participants get $q_1, q_2, \ldots, q_k, g_1, g_2, \ldots, g_{n-k}$ as shares, where $q_1, q_2, \ldots, q_k$ form shares for a (k,k) scheme.

From Theorem 4.1, it is clear that only when $q_1, q_2, \ldots, q_k$ are stacked together, their will be difference in light transmission for areas corresponding to black pixels with that of the areas corresponding to white pixels of the secret. So, for $F \in Z_M, |F| = k-1$ implies at least one of $q_1, q_2, \ldots, q_k$ is not assigned to any element of F as share. Clearly, F will have equal light transmission corresponding to the areas of all white as well as black pixels of the secret. If $Q \in \Gamma_0$, i.e., $|Q| = k$, then only in the unique case, where elements of Q are assigned with $q_1, q_2, \ldots, q_k$, $\not{t}(R^Q[i,j] \mid S[i,j]=0) = 1$ and $\not{t}(R^Q[i,j] \mid S[i,j]=1) = 0$. But we have $\binom{n}{k}$ many choices to select those k participants out of those n participants. So we have light contrast corresponding to the set Q of participants as

$$\alpha^{Q}_{XOR}(S) = \frac{1}{\binom{n}{k}}.$$

Hence we have the theorem.

Now we shall discuss the corresponding case for general t, k and n as described in Algorithm 1.

Theorem 4.3. *"XOR" operation in the reconstruction phase of Algorithm 1 leads to a Non-Monotone t-$(k,n)^*$-XRGVCS with light contrast α^Q_{XOR}, where*

$$\alpha^Q_{XOR} = \begin{cases} \frac{1}{\binom{n-1-t}{k-1-t}}, & \text{if } P_n \in Q \\ \frac{k-t}{\binom{n-1-t}{k-1-t}}, & \text{if } P_n \notin Q, \end{cases}$$

where Q is a minimal qualified set.

Proof. The proof follows the same line of arguments as in the proofs of Lemma 1, Lemma 2 and Lemma 3. The only thing that is different here is the values of light transmission of a set of participants under different choices of $\mathscr{A}$. For single share, the value of light transmission is independent of black and white secret pixel. Now let for $F \in Z_M$, $|F \cap \mathscr{A}| = h$. So, h runs from t to $k-1$. As discussed in Theorem 4.2, here also, F will have same light transmission for all the areas corresponding to white and black pixels of the secret S. Again, for $Q \in \Gamma_0$ when $|Q \cap A| = k-1$ then elements of Q are assigned with $r_1, r_2, \ldots, r_{k-1}, a_k$. So, only for those choices of $A \in \mathscr{A}$, Q will have different values of light transmission for area corresponding to black region of secret with that corresponding to white region. From Lemma 3, it is clear that light contrast for the stacked share corresponding to Q will be:

$$\alpha^Q_{XOR} = \begin{cases} \dfrac{1}{\binom{n-1-t}{k-1-t}}, & \text{if } P_n \in Q \\ \dfrac{k-t}{\binom{n-1-t}{k-1-t}}, & \text{if } P_n \notin Q. \end{cases}$$

Hence the theorem.

Corollary 1. *A non monotone t-$(k,n)^*$-XRGVCS gives optimal light contrast 1 if $k = t+1$ or $n = k+1$.*

Proof. The result follows by putting the value of n as $k+1$ or k as $t+1$ in the expression of α^Q_{XOR} in Theorem 4.3.

Remark 5. *The Theorem 4.3 shows that for a (k,n)-XRGVCS, our scheme works better than the scheme as described in Theorem 4.2.*

The next theorem shows that our "XOR" based t-$(k,n)^*$-XRGVCS works much better than our "OR" based t-$(k,n)^*$-RGVCS.

Theorem 4.4. *Our proposed t-$(k,n)^*$-XRGVCS is much more efficient than our proposed t-$(k,n)^*$-RGVCS with respect to light contrast.*

Proof. For a minimal qualified set Q, the light contrast of t-$(k,n)^*$-RGVCS constructed in Algorithm 1 is given by

$$\alpha_{OR}^{Q} = \begin{cases} \frac{1}{\binom{n-1-t}{k-1-t}} \dfrac{1}{2^{k-1}}, & \text{if } P_n \in Q \\ \frac{k-t}{\binom{n-1-t}{k-1-t}} \dfrac{1}{2^{k-1}}, & \text{if } P_n \notin Q. \end{cases}$$

So, comparing with α_{XOR}^{Q}, we have if $P_n \in Q$, then

$$\alpha_{XOR}^{Q} = \frac{1}{\binom{n-1-t}{k-1-t}} > \frac{1}{\binom{n-1-t}{k-1-t}} \frac{1}{2^{k-1}},$$

and if $P_n \notin Q$, then

$$\alpha_{XOR}^{Q} = \frac{k-t}{\binom{n-1-t}{k-1-t}} > \frac{k-t}{\binom{n-1-t}{k-1-t}} \frac{1}{2^{k-1}}.$$

Hence we have the theorem.

5 Experiment and Discussions

In this section we shall validate our theoretical results through experimental simulations. For that let us first fix few notations. Let $\mathscr{R}$ be a set of all n random grids, obtained through our proposed Algorithm 1, corresponding to a t-$(k,n)^*$ access structure with valid parameters t, k and n. Let $H \subseteq \mathscr{R}$ be such that $1 \leq h(=\mid H \mid) \leq n$. For experimental verification, we use a Python code which superimposes all the shares coming from the participants in H. In Tables 6, 7 and 8, we compare the analytic light contrasts α_{OR}^{H} and α_{XOR}^{H} obtained in Section 3.2 and Section 4 respectively against the experimental values as done in Experiments 1, 2 and 3. To calculate the experimental values of light contrast, we use the following notations. Recall that $R^H[S(0)](R^H[S(1)])$ denotes the area of pixels in the stacked share R^H corresponding to $S(0)(S(1))$, where $S(0)(S(1))$ is the area of all transparent (opaque) pixels in the secret image S. Then we calculate the experimental light contrast $e\alpha_{OR}^{H}$ for "OR" based scheme as

$$e\alpha_{OR}^{H} = \frac{\eta_0(R^H[S(0)])}{\eta_0(S)} - \frac{\eta_0(R^H[S(1)])}{\eta_1(S)},$$

where $\eta_0(X)(\eta_1(X))$ denotes the number of transparent (opaque) pixels in X. Similarly, we calculate the experimental light contrast $e\alpha_{XOR}^{H}$, for "XOR" based RGVCS.

We have also given comparison table of numerical values of light contrast of our scheme with that of the already proposed general access structures restricted to customized t-$(k,n)^*$ scenario. Comparison among different schemes in terms of numerical values of the light contrast and their corresponding graphical representations are shown in Tables 2, 3 and in Figures 4, 5. In this section the computer programs are coded in Python Builder, run in a PC with operating system UBUNTU 16.04. The graphs are prepared with TikZ in LaTeX. We have given three experiments. Experiment 1, Experiment 2 and Experiment 3 have discussion on access structures 1-$(2,4)^*$, 1-$(3,5)^*$ and 2-$(3,5)^*$.

Remark 6. *Recently, a new scheme is proposed in [25] . However, as the model does not match with our model of random grid, we are unable to compare the scheme with our scheme.*

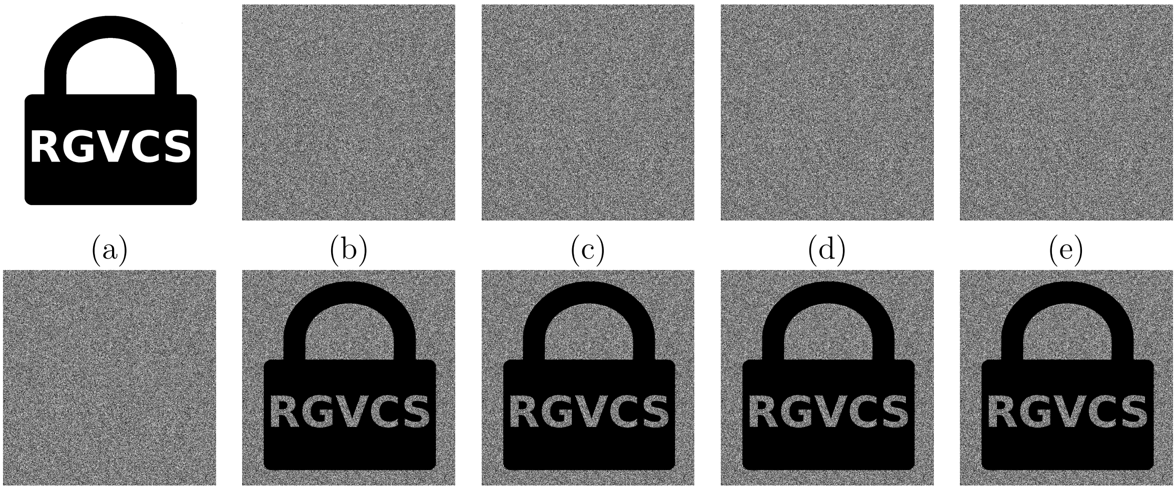
Experiment 1 for RGVCS

In this experiment we have prepared four shares for 1-$(2,4)^*$-RGVCS. Here in the superimposition stage we have used the binary "OR" operation of the shares. In Fig. 1, (a) is the secret binary image and (b)-(e) are the four shares: R_1, R_2, R_3, and R_4. Note that R_1 is the share of the only essential participant. Here (f), (g), (h), (i), (j) are the superimposed images corresponding to $R_2 \otimes R_3$, $R_1 \otimes R_2$, $R_1 \otimes R_4$, $R_1 \otimes R_2 \otimes R_3$ and $R_1 \otimes R_2 \otimes R_3 \otimes R_4$. From the images we can note that the superimposed image of $R_2 \otimes R_3$ does not reveal anything about the secret, as R_1, the share for P_1, is not present in that superimposition, which verifies $\{P_2, P_3\}$ as a Type 1 maximal forbidden set. At the same time $R_1 \otimes R_2$ gives back the image with some loss of light contrast as expected from Lemma 3. Also from (g) and (h) it is clear that $R_1 \otimes R_4$ gives the same light contrast as $R_1 \otimes R_2$.

The corresponding values of $\alpha^H_{OR}, e\alpha^H_{OR}$ are summarized in Table 6. One can easily notice from the table that $\alpha^H_{OR} - e\alpha^H_{OR}$ is less than 0.004 for each of the cases. So, we realize that the analytic values of light contrast are pretty close to that of the experimental values. In Table 6, we further compare the values for α^H_{XOR} and the corresponding experimental values for $e\alpha^H_{XOR}$. So in a nutshell we have a verification for our proposed algorithm for a 1-$(2,4)^*$-RGVCS.

Experiment 2 for RGVCS

In this experiment we have prepared five shares for an 1-$(3,5)^*$-RGVCS. In Fig.2, (a) is the secret and (b) to (f) are the five shares: R_1, R_2, R_3, R_4, and R_5. Note that R_1 is the share for the only essential participant P_1. Here (g), (h), (i), (j), (k), (l) are the superimposed images corresponding to $R_1 \otimes R_2$, $R_1 \otimes R_3 \otimes R_4$, $R_1 \otimes R_2 \otimes R_3$, $R_1 \otimes R_2 \otimes R_5$ $R_1 \otimes R_2 \otimes R_3 \otimes R_4$, and $R_1 \otimes R_2 \otimes R_3 \otimes R_4 \otimes R_5$. From the images it is clear that the superimposed image of $R_2 \otimes R_3 \otimes R_4$ does not reveal anything about the secret, as R_1 is not present in that superimposition. Which gives the verification of $\{P_2, P_3, P_4\}$. At the same



(a) (b) (c) (d) (e) (f) (g) (h) (i) (j)

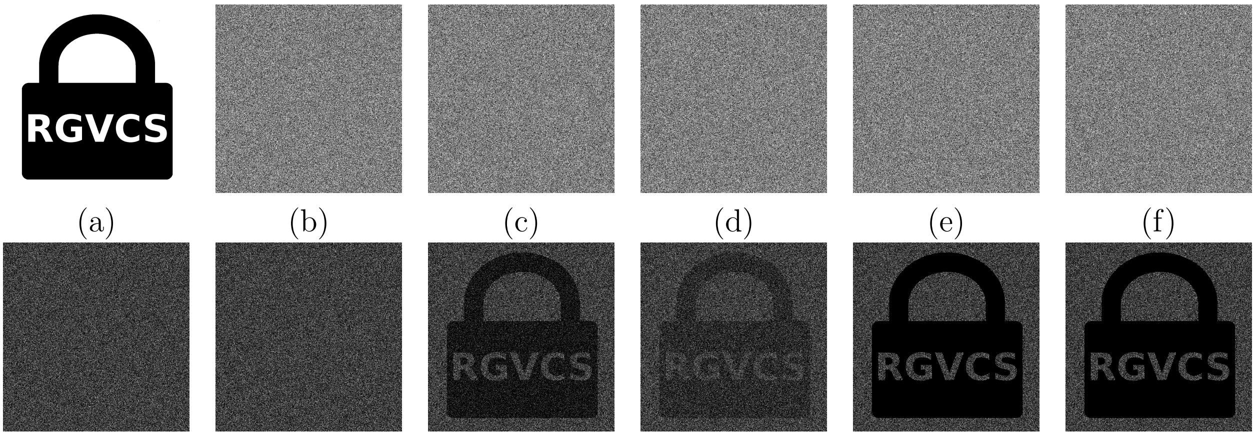
Figure 1: Implementation results of 1-$(2,4)^*$-RGVCS. Here (a) stands for the secret S. (b) stands for the random grid R_1. (c) R_2. (d) R_3. (e) R_4. (f) Stands for the stacked image $R_2 \otimes R_3$. (g) $R_1 \otimes R_2$. (h) $R_1 \otimes R_4$. (i) $R_1 \otimes R_2 \otimes R_3$. (j) $R_1 \otimes R_2 \otimes R_3 \otimes R_4$

time $R_1 \otimes R_2 \otimes R_3$ gives back the image with some loss of light contrast as expected. Also from (i) and (j) it is clear that whenever R_5 is included in the superimposition ($R_1 \otimes R_2 \otimes R_5$ the light contrast is relatively less, which verifies the different values of light contrast corresponding to two minimal qualified sets, one containing P_n, another not containing it.

The corresponding values of $\alpha^H_{OR}, e\alpha^H_{OR}$ and their differences are summarized in Table 7. One can easily notice from the table that $\alpha^H_{OR} - e\alpha^H_{OR}$ is less than 0.004 for each of the cases. So, we realize that the analytic values of light contrast are pretty close to that of the the experimental values. In Table 7, we further compare the values for α^H_{XOR} and the corresponding experimental values for $e\alpha^H_{XOR}$. So in a nutshell we have a verification for our proposed algorithm for 1-$(3,5)^*$-RGVCS.

Experiment 3 for XRGVCS

In this experiment we have prepared five shares for a 2-$(3,5)^*$-XRVCS, where we perform binary "XOR" operation of the shares coming from participants in the superimposition stage. In Fig.3, (a) is the secret S and (b) to (f) are five shares: R_1, R_2, R_3, R_4, and R_5. Note that R_1 and R_2 are the shares for the essential participants P_1 and P_2 respectively, while (g), (h), (i), (j) are the superimposed images corresponding to $R_1 \oplus R_2$, $R_1 \oplus R_2 \oplus R_3 \oplus R_4$, $R_1 \oplus R_2 \oplus R_3 \oplus R_4 \oplus R_5$, and $R_1 \oplus R_2 \oplus R_3$. From the figure we can note that the none of the superimposed images except $R_1 \oplus R_2 \oplus R_3$ and $R_1 \oplus R_2 \oplus R_3 \oplus R_4 \oplus R_5$



(a) (b) (c) (d) (e) (f)

(g) (h) (i) (j) (k) (l)

Figure 2: Implementation results for 1-$(3,5)^*$-RGVCS. Here (a) stands for the secret S. (b) stands for the random grid R_1. (c) R_2. (d) R_3. (e) R_4. (f) R_5. (g) Stands for the stacked image $R_1 \otimes R_2$. (h) $R_2 \otimes R_3 \otimes R_4$. (i) $R_1 \otimes R_2 \otimes R_3$. (j) $R_1 \otimes R_2 \otimes R_5$. (k) $R_1 \otimes R_2 \otimes R_3 \otimes R_4$. (l) $R_1 \otimes R_2 \otimes R_3 \otimes R_4 \otimes R_5$

reveals anything about the secret. The case of $R_1 \oplus R_2 \oplus R_3$ is evident from the Theorem 4.3. For the case of $R_1 \oplus R_2 \oplus R_3 \oplus R_4 \oplus R_5, R_4, R_5$ does not make any difference in the stack share, because they carry the same pixels.

The corresponding values of the theoretical values α^H_{XOR} and the corresponding experimental values $e\alpha^H_{XOR}$ and their differences are summarized in Table 8. One can easily notice from the table that $\alpha^H_{XOR} - e\alpha^H_{XOR}$ is less than 0.004 for each of the cases. This implies that the analytic values of light contrast are pretty close to that of the the experimental values. In Table 8, we further compare the values for α^H_{OR} and the corresponding experimental values for $e\alpha^H_{OR}$. So in a nutshell we have a verification for our proposed algorithm for 2-$(3,5)^*$-XRGVCS.

6 Conclusion

In this paper we propose efficient direct constructions of algorithms for both "OR" and "XOR" based t-$(k,n)^*$ schemes for RGVCS and come up with the closed forms of light contrast. Our theoretical as well as experimental simulated results show that our algorithms work much efficiently than the customized algorithms proposed in [34] and [29] which are obtained as a particular case of general access structures. Obtaining closed forms of the optimal light contrast for both "OR" and "XOR" based VCSs for t-$(k,n)^*$ access structure

Access Structures	Our		Wu	Shyu(Q)	Shyu(F)
	In	**Out**			
A0 : 1-$(2,3)^*$	0.500	0.500	0.250	0.250	0.500
A1 : 1-$(2,4)^*$	0.500	0.500	0.167	0.125	0.500
A2 : 1-$(3,4)^*$	0.125	0.250	0.083	0.016	0.125
A3 : 1-$(3,5)^*$	0.083	0.167	0.042	0.000 $*_1$	0.063
A4 : 1-$(3,6)^*$	0.063	0.125	0.025	0.000 $*_2$	0.031
A5 : 1-$(4,5)^*$	0.042	0.125	0.025	0.000 $*_3$	0.016
A6 : 1-$(4,6)^*$	0.021	0.063	0.013	0.000 $*_4$	0.001
A7 : 2-$(3,6)^*$	0.250	0.250	0.063	0.004	0.250
A8 : 2-$(4,5)^*$	0.063	0.125	0.042	0.002	0.063
A9 : 2-$(4,6)^*$	0.042	0.083	0.021	0.000 $*_5$	0.031
A10 : 2-$(5,6)^*$	0.021	0.062	0.016	0.000 $*_6$	0.008
A11 : 2-$(5,7)^*$	0.010	0.031	0.006	0.000 $*7$	0.000 $*_1$
A12 : 3-$(5,7)^*$	0.042	0.083	0.010	0.000 $*_8$	0.016
A13 : 3-$(6,7)^*$	0.010	0.031	0.008	0.000 $*_9$	0.004
A14 : 3-$(6,8)^*$	0.005	0.016	0.003	0.000 $*_{10}$	0.000 $*_1$
A15 : 3-$(7,8)^*$	0.004	0.016	0.003	0.000 $*_{11}$	0.000 $*_{12}$

Table 2: Comparison of different "OR" based light contrasts for different access structures, where $*_1, *_2, *_3, *_4, *_5, *_6, *_7, *_8, *_9, *_{10}, *_{11}, *_{12}$ correspond to the 3 digit approximations of the terms $\frac{1}{2048}, \frac{1}{4^7} \times \frac{1}{2^3}, \frac{1}{8^4}, \frac{1}{8^7} \times \frac{1}{4^3}, \frac{1}{8^5} \times \frac{1}{4}, \frac{1}{2^{16}}, \frac{1}{2^{38}}, \frac{1}{2^{23}}, \frac{1}{1048576}, \frac{1}{2^{43}}, \frac{1}{2^{18}}, \frac{1}{2^{13}}$ respectively. Here "In" and "Out" stands for the cases when nth participant $P_n \in Q$ and $P_n \notin Q$ respectively, where Q is the minimal qualified set. Further Shyu (Q) and Shyu (F) represent respectively the value of light contrasts obtained in schemes proposed by Shyu in Theorem 2 and Theorem 3 in [29] (See Fig.4).

Access Structures	OR		XOR	
	In	Out	In	Out
A0 : 1-$(2,3)^*$	0.500	0.500	1.000	1.000
A1 : 1-$(2,4)^*$	0.500	0.500	1.000	1.000
A2 : 1-$(2,5)^*$	0.500	0.500	1.000	1.000
A3 : 1-$(3,4)^*$	0.125	0.250	0.500	1.000
A4 : 1-$(3,5)^*$	0.083	0.167	0.333	0.667
A5 : 1-$(3,6)^*$	0.063	0.125	0.250	0.500
A6 : 1-$(4,5)^*$	0.042	0.125	0.333	1.000
A7 : 1-$(4,6)^*$	0.021	0.063	0.167	0.500
A8 : 2-$(3,4)^*$	0.250	0.250	1.000	1.000
A9 : 2-$(3,5)^*$	0.250	0.250	1.000	1.000
A10 : 2-$(3,6)^*$	0.250	0.250	1.000	1.000
A11 : 2-$(4,5)^*$	0.063	0.125	0.500	1.000
A12 : 2-$(4,6)^*$	0.042	0.083	0.333	0.667
A13 : 3-$(4,5)^*$	0.125	0.125	1.000	1.000
A14 : 3-$(5,6)^*$	0.031	0.063	0.500	1.000
A15 : 3-$(6,7)^*$	0.010	0.031	0.333	1.000

Table 3: Comparison table: our proposed "OR" based RGVCS and our "XOR" based XRGVCS (See Fig.5).

Set of Participants	Shyu(Q)	Shyu(F)	Wu	Our	
				In	Out
S0 : $\{P_1\}$	0.000	0.000	0.000	0.000	0.000
S1 : $\{P_1, P_2\}$	0.125	0.500	0.167	0.500	1.000
S2 : $\{P_1, P_4\}$	0.125	0.500	0.167	0.500	1.000
S3 : $\{P_1, P_2, P_3\}$	0.125	0.500	0.167	0.500	NS
S4 : $\{P_1, P_2, P_4\}$	0.125	0.500	0.167	0.500	NA
S5 : $\{P_1, P_2, P_3, P_4\}$	0.125	0.500	0.125	0.500	NA

Table 4: Comparison of access Structures 1-$(2,4)^*$ (See Fig.6(a)).

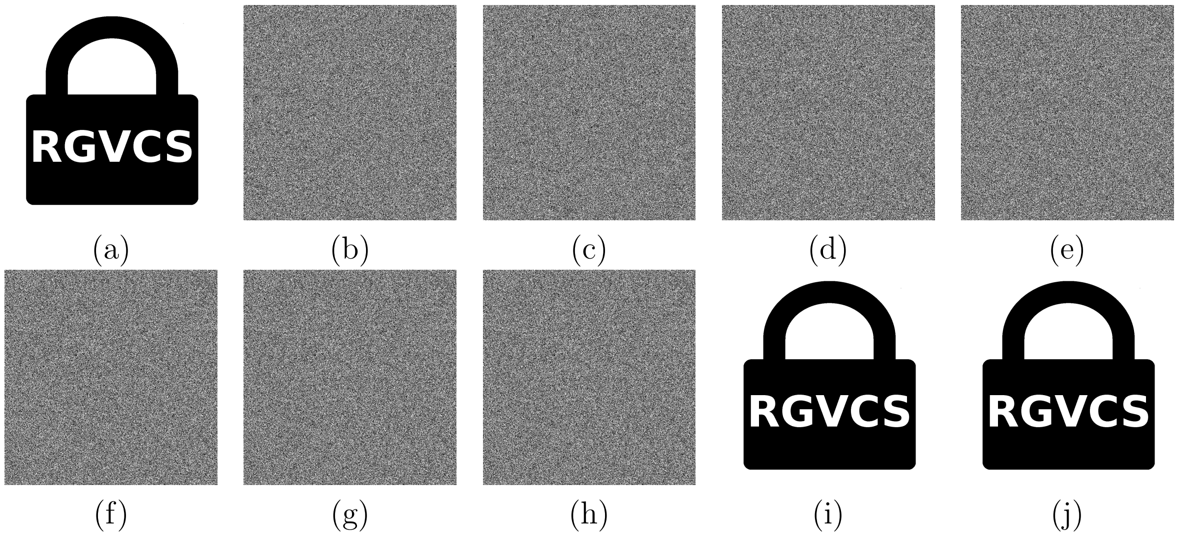
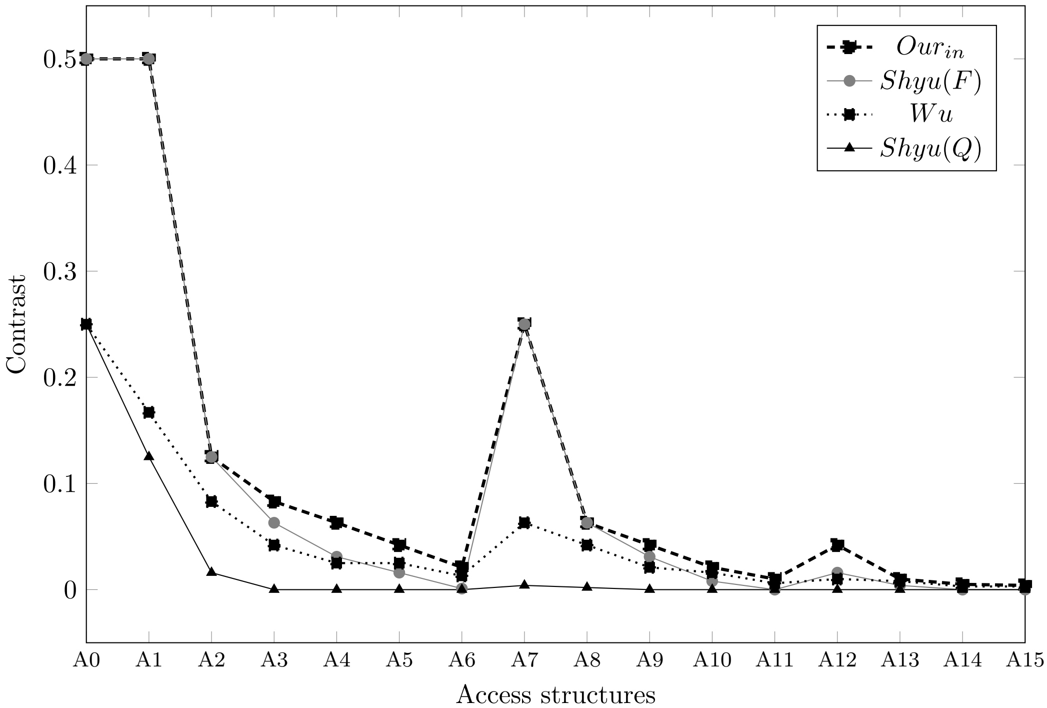


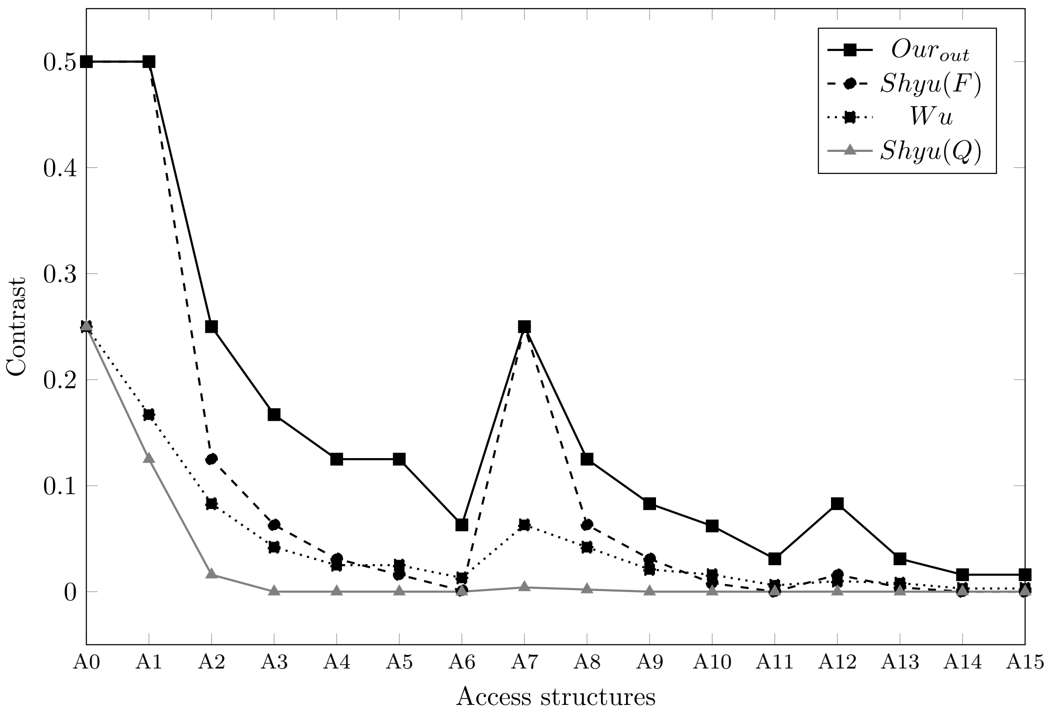
Figure 3: Implementation results for 2-$(3,5)^*$-XRGVCS, where "$\otimes$" stands for binary "OR" operation. Here (a) stands for the secret S. (b) stands for the random grid R_1. (c) R_2. (d) R_3. (e) R_4. (f) R_5. (g) Stands for the stacked image $R_1 \oplus R_2$. (h) $R_1 \oplus R_2 \oplus R_3 \oplus R_4$. (i) $R_1 \oplus R_2 \oplus R_3 \oplus R_4 \oplus R_5$. (j) $R_1 \oplus R_2 \oplus R_3$

Set of Participants	**Shyu(Q)**	**Shyu(F)**	**Wu**	**Our**	
				In	**Out**
S0 : $\{P_1\}$	0.000	0.000	0.000	0.000	0.000
S1 : $\{P_1, P_2\}$	0.000	0.000	0.000	0.000	0.000
S2 : $\{P_1, P_5\}$	0.000	0.000	0.000	0.000	0.000
S3 : $\{P_1, P_2, P_3\}$	0.000 $*_1$	0.063	0.042	0.167	0.667
S4 : $\{P_1, P_2, P_5\}$	0.000 $*_1$	0.063	0.042	0.083	0.333
S5 : $\{P_1, P_2, P_3, P_4\}$	0.000 $*_2$	0.063	0.063	0.167	NS
S6 : $\{P_1, P_2, P_3, P_5\}$	0.000 $*_2$	0.063	0.063	0.167	NA
S7 : $\{P_1, P_2, P_3, P_4, P_5\}$	0.000 $*_1$	0.063	0.042	0.250	NA

Table 5: Access Structure: 1-$(3,5)^*$, where $*_1$ and $*_2$ corresponds to the 3 digit approximations of the terms $\frac{1}{2048}$ and $\frac{1}{4096}$ respectively (See Fig.6(b)).



(i): Values corresponds to "In"



(ii): Values corresponds to "Out"

Figure 4: (i) and (ii) represent the graphical representation of the values from Table 2.

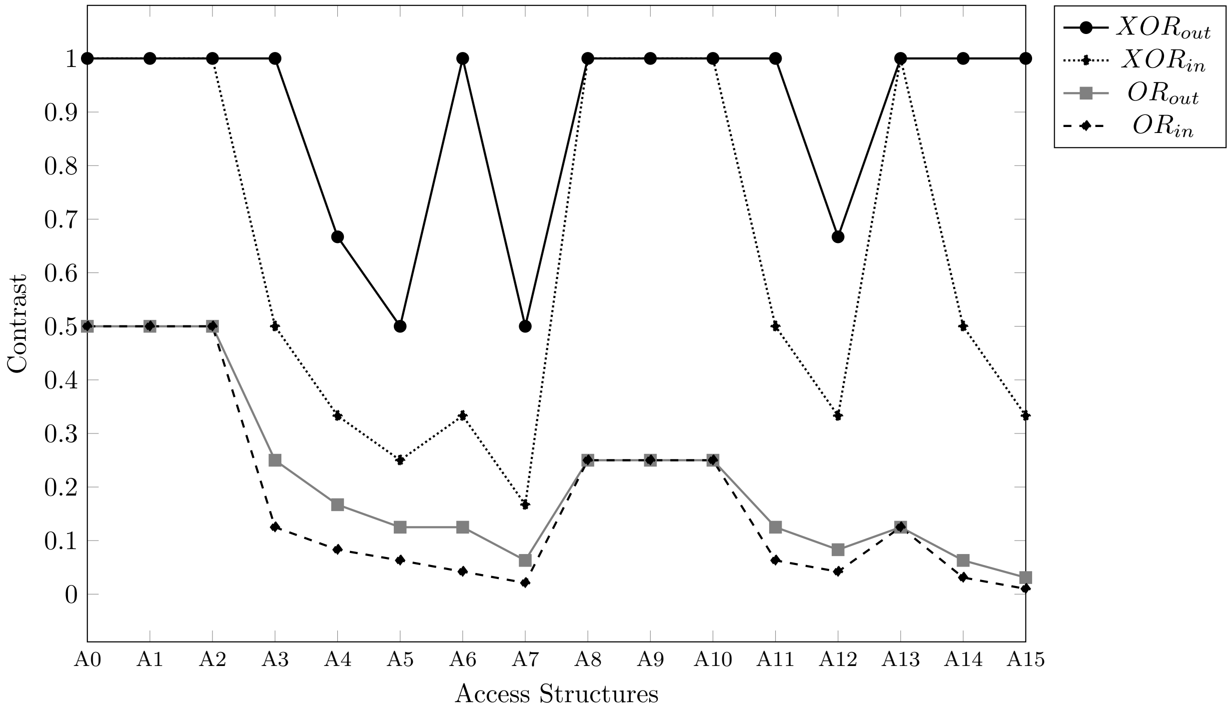
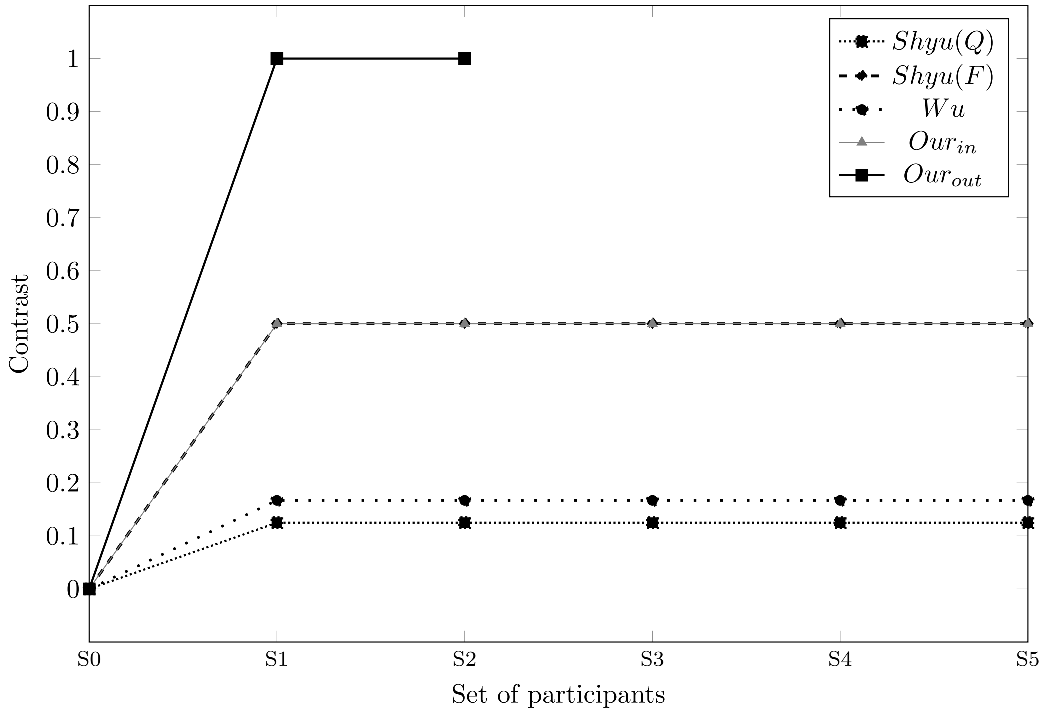


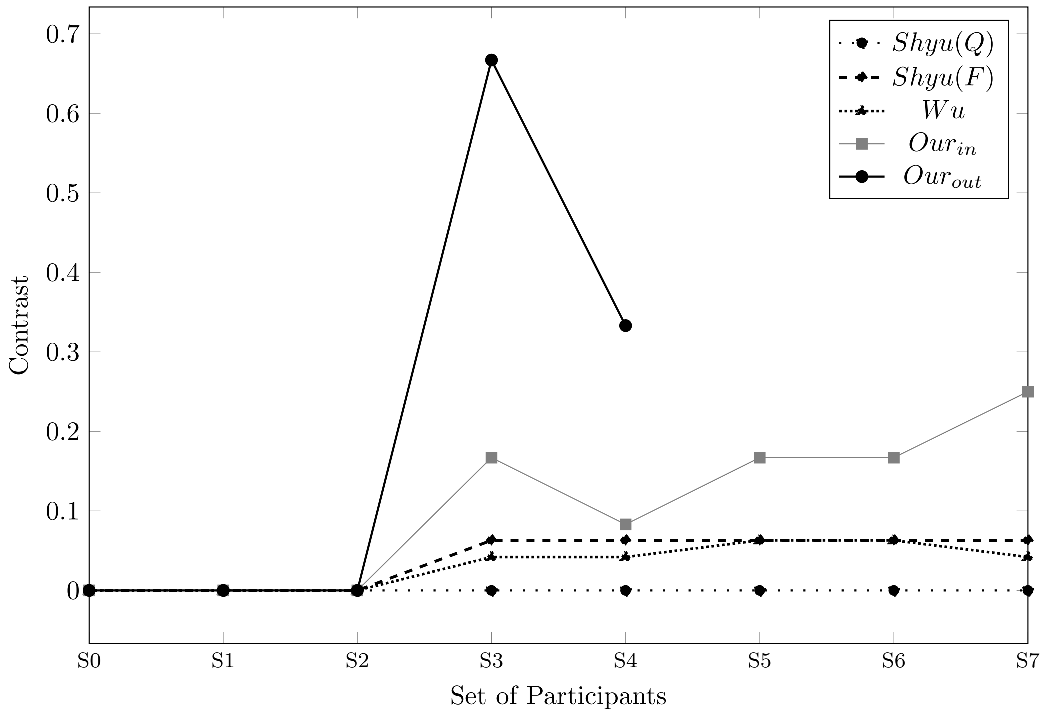
Figure 5: Graphical representation of values for our "OR" and "XOR" based schemes as shown in Table 3.

Set of Participants: H	α_{OR}^{H}	$e\alpha_{OR}^{H}$	α_{XOR}^{H}	$e\alpha_{XOR}^{H}$
$\{P_1, P_2\}$	0.5000	0.5004	1.0000	1.0000
$\{P_1, P_4\}$	0.5000	0.5004	1.0000	1.0000
$\{P_2, P_3\}$	0.000	0.0000	0.0000	0.0000
$\{P_1, P_2, P_3\}$	0.5000	0.5000	NA	NA
$\{P_1, P_2, P_4\}$	0.5000	0.5000	NA	NA
$\{P_2, P_3, P_4\}$	0.0000	0.0000	NA	NA
$\{P_1, P_2, P_3, P_4\}$	0.5000	0.5004	NA	NA

Table 6: 1-$(2,4)^{*}$-RGVCS



(a)



(b)

Figure 6: (a) 1-$(2,4)^*$ RGVCS (See Table 4), (b) 1-$(3,5)^*$ RGVCS (See Table 5).

Set of Participants: H	α_{OR}^{H}	$e\alpha_{OR}^{H}$	α_{XOR}^{H}	$e\alpha_{XOR}^{H}$
$\{P_2, P_3\}$	0.0000	0.0000	0.0000	0.0002
$\{P_1, P_2, P_3\}$	0.1669	0.1667	0.6667	0.6658
$\{P_1, P_2, P_5\}$	0.0833	0.0831	0.3333	0.3330
$\{P_2, P_3, P_4\}$	0.0000	0.0000	0.0000	0.0001
$\{P_1, P_2, P_3, P_4\}$	0.1666	0.1669	NA	NA
$\{P_1, P_2, P_3, P_5\}$	0.1666	0.1669	NA	NA
$\{P_2, P_3, P_4, P_5\}$	0.0000	0.0000	NA	NA
$\{P_1, P_2, P_3, P_4, P_5\}$	0.2500	0.2498	NA	NA

Table 7: 1-$(3, 5)^*$-RGVCS

Set of Participants: H	α_{OR}^{H}	$e\alpha_{OR}^{H}$	α_{XOR}^{H}	$e\alpha_{XOR}^{H}$
$\{P_1, P_2\}$	0.0000	0.0004	0.0000	0.0003
$\{P_1, P_2, P_3\}$	0.2500	0.2495	1.0000	1.0000
$\{P_1, P_2, P_5\}$	0.2500	0.2495	1.0000	1.0000
$\{P_2, P_3, P_4\}$	0.0000	0.0002	0.0000	0.0007
$\{P_1, P_2, P_3, P_4\}$	0.2500	0.2495	NA	NA
$\{P_1, P_2, P_3, P_5\}$	0.2500	0.2495	NA	NA
$\{P_2, P_3, P_4, P_5\}$	0.0000	0.0002	NA	NA
$\{P_1, P_2, P_3, P_4, P_5\}$	0.2500	0.2495	NA	NA

Table 8: 2-$(3, 5)^*$-RGVCS

Acknowledgments

Research of the third author is partially supported by National Board for Higher Mathematics, Department of Atomic Energy, Government of India,
Grant No. 2/48(10)/2013/NBHM(R.P.)/R&D II/695.

Acknowledgment

References

[1] Adhikari, A. (2014). 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.

[2] Adhikari, A. and Bose, M. (2004). A new visual cryptographic scheme using latin squares. *IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences*, 87(5):1198–1202.

[3] Adhikari, A., Bose, M., Kumar, D., and Roy, B. K. (2007). Applications of partially balanced incomplete block designs in developing (2, n) visual cryptographic schemes. *IEICE Transactions*, 90-A(5):949–951.

[4] Adhikari, A., Dutta, T. K., and Roy, B. K. (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, December 20-22, 2004, Proceedings*, pages 399–413.

[5] Adhikari, A. and Roy, B. (2008). On some constructions of monochrome visual cryptographic schemes. In *Information Technology, 2008. IT 2008. 1st International Conference on*, pages 1–6. IEEE.

[6] Adhikari, A. and Sikdar, S. (2003). A new (2, n)-visual threshold scheme for color images. In *Progress in Cryptology - INDOCRYPT 2003, 4th International Conference on Cryptology in India, New Delhi, India, December 8-10, 2003, Proceedings*, pages 148–161.

[7] Adhikari, M. R. and Adhikari, A. (2014). *Basic modern algebra with applications.* Springer.

[8] Ateniese, G., Blundo, C., De Santis, A., and Stinson, D. R. (1996a). Constructions and bounds for visual cryptography. In *Automata, Languages and Programming, 23rd International Colloquium, ICALP96, Paderborn, Germany, 8-12 July 1996, Proceedings*, pages 416–428.

[9] Ateniese, G., Blundo, C., Santis, A. D., and Stinson, D. R. (1996b). Visual cryptography for general access structures. *Inf. Comput.*, 129(2):86–106.

[10] Blundo, C., Bonis, A. D., and Santis, A. D. (2001). Improved schemes for visual cryptography. *Designs, Codes and Cryptography*, 24(3):255–278.

[11] Blundo, C., De Santis, A., and Stinson, D. R. (1999). On the contrast in visual cryptography schemes. *Journal of Cryptology*, 12(4):261–289.

[12] Chen, T.-H. and Tsao, K.-H. (2011a). Threshold visual secret sharing by random grids. *Journal of Systems and Software*, 84(7):1197 – 1208.

[13] Chen, T.-H. and Tsao, K.-H. (2011b). User-friendly random-grid-based visual secret sharing. *IEEE Transactions on Circuits and Systems for Video Technology*, 21(11):1693–1703.

[14] Chen, Y., Chen, L., and Shyu, S. J. (2016). Secret image sharing with smaller shadow sizes for general access structures. *Multimedia Tools Appl.*, 75(21):13913–13929.

[15] Dutta, S. and 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, December 16-17, 2014, Revised Selected Papers*, pages 230–242.

[16] Dutta, S., Bhore, T., and Adhikari, A. (2016a). Efficient construction of visual cryptographic scheme for compartmented access structures. *IACR Cryptology ePrint Archive*, 2016:1113.

[17] Dutta, S., Rohit, R. S., and Adhikari, A. (2016b). Constructions and analysis of some efficient t -$(k,n)^*$-visual cryptographic schemes using linear algebraic techniques. *Des. Codes Cryptography*, 80(1):165–196.

[18] Dutta, S., Roy, P. S., Adhikari, A., and Sakurai, K. (2016c). On the robustness of visual cryptographic schemes. In *Digital Forensics and Watermarking - 15th International Workshop, IWDW 2016, Beijing, China, September 17-19, 2016, Revised Selected Papers*, pages 251–262.

[19] Fu, Z. and Yu, B. (2014). Optimal pixel expansion of deterministic visual cryptography scheme. *Multimedia Tools Appl.*, 73(3):1177–1193.

[20] Hou, Y.-C. (2003). Visual cryptography for color images. *Pattern Recognition*, 36(7):1619 – 1629.

[21] Kafri, O. and Keren, E. (1987). Encryption of pictures and shapes by random grids. *Opt. Lett.*, 12(6):377–379.

[22] Lakshmanan, R. and Arumugam, S. (2017). Construction of a (k, n)-visual cryptography scheme. *Des. Codes Cryptography*, 82(3):629–645.

[23] Naor, M. and Shamir, A. (1995). *Visual cryptography*, pages 1–12. Springer Berlin Heidelberg, Berlin, Heidelberg.

[24] Ryo ITO, H. K. and TANAKA, H. (1999). Image size invariant visual cryptography. *IEICE TRANS. FUNDAMENTALS*, E82A(10):2172–2177.

[25] Shen, G., Liu, F., Fu, Z., and Yu, B. (2017). Visual cryptograms of random grids via linear algebra. *Multimedia Tools and Applications.*

[26] Shyu, S. and Chen, M. (2011). Optimum pixel expansions for threshold visual secret sharing schemes. *IEEE Transactions on Information Forensics and Security*, 6(3 PART 2):960–969.

[27] Shyu, S. J. (2007). Image encryption by random grids. *Pattern Recognition*, 40(3):1014–1031.

[28] Shyu, S. J. (2009). Image encryption by multiple random grids. *Pattern Recognition*, 42(7):1582 – 1596.

[29] Shyu, S. J. (2013). Visual cryptograms of random grids for general access structures. *IEEE Trans. Circuits Syst. Video Techn.*, 23(3):414–424.

[30] Shyu, S. J. (2015). Visual cryptograms of random grids for threshold access structures. *Theor. Comput. Sci.*, 565:30–49.

[31] Shyu, S. J. and Chen, M. C. (2015). Minimizing pixel expansion in visual cryptographic scheme for general access structures. *IEEE Trans. Circuits Syst. Video Techn.*, 25(9):1557–1561.

[32] Tsao, K., Shyu, S. J., Lin, C., Lee, Y., and Chen, T. (2015). Visual multiple-secret sharing for flexible general access structure by random grids. *Displays*, 39:80–92.

[33] Verheul, E. R. and van Tilborg, H. C. A. (1997). Constructions and properties of k out of n visual secret sharing schemes. *Designs, Codes and Cryptography*, 11(2):179–196.

[34] Wu, X. and Sun, W. (2012). Visual secret sharing for general access structures by random grids. *IET information security*, 6(4):299–309.

[35] Yang, C. (2004). New visual secret sharing schemes using probabilistic method. *Pattern Recognition Letters*, 25(4):481–494.