(t, k, n)-Deterministic Extended Visual Secret Sharing Scheme Using Combined Boolean Operations

L. Chandana Priya and K. Praveen(✉)

TIFAC-CORE in Cyber Security, Amrita School of Engineering,
Amrita Vishwa Vidyapeetham, Coimbatore, India
k_praveen@cb.amrita.edu

Abstract. In Visual Cryptographic Scheme (VCS), the shares of the secret image are viewed as random whereas in Extended Visual Cryptographic Scheme (EVCS), the shares are viewed as meaningful images. When the number of participants increases the graying effect problem in deterministic VCS is caused due to high pixel expansion. This graying effect was resolved using ideal contrast constructions in VCS, but not in EVCS. In ideal contrast VCS; combinations of Boolean operations are used during reconstruction. Here in this paper, we designed a deterministic construction for (t, k, n) access structure using the existing VCS constructions with contrast one as building block. In existing EVCS constructions the relative contrast will vary depending on the access structure, but in the proposed EVCS construction it is 0.25, which is better than existing schemes.

Keywords: Secret sharing · Visual cryptography · Contrast · Extended visual cryptography · Essential access structure

1 Introduction

In Visual cryptographic scheme, dealer constructs random shares from a secret image (*SI*) and then distributes shares to participants. During sufficient participants join their shares, the reconstructed image (*RI*) will be produced. Based on the pixel expansion and the contrast value [1], the quality of a VCS is measured. XOR, OR, AND and NOT are the Boolean operations used for reconstruction in VCS. In deterministic VCS all the black and white pixels of *SI* will be reconstructed in *RI*, but in probabilistic VCS [11] the correct reconstruction cannot be assured. VCS was pioneered by Naor *et al.* [1] in 1994. The deterministic VCS for general access structures are introduced in papers [2, 3, 12]. The constructions given in papers [3, 4] reconstruct the black pixel without distortion. For VCS constructions with contrast value one, the secret *SI* is generated without loss of resolution using combined Boolean operations [5–7, 27]. EVCS is a type of VCS developed by Ateniese *et al.* [13] where the encoded shares of *SI* are viewed as meaningful image. Schemes given in papers [13–20] are EVCS with pixel expansion and constructions given in papers [21–26] are EVCS without pixel expansion.

K. R. Venugopal et al. (Eds.): ICInPro 2021, CCIS 1483, pp. 66–77, 2021.
https://doi.org/10.1007/978-3-030-91244-4_6

Table 1. Notations and its description

Symbol	Description
$\otimes$	OR operation
$\oplus$	XOR operation
Θ	AND operation
α_S	Relative contrast of meaningful share
α_{RI}	Relative contrast of reconstructed image
n	Total number of participants
m	Pixel expansion
k	Minimum participants needed to generate the secret in a (k, n) scheme
t	Number of mandatory participants needed to generate the secret in a (t, k, n) scheme
APE	Average pixel expansion [12]
$f(x) = \bar{x}$	NOT operation
Mp	Mp set contains distinct participants. For every $A \in \Gamma_{QM}$, at least one of the participant of $A \in Mp$
$COV_{(p_u,j)}(z, b)$	$n \times m$ Cover Images of size $p \times q$ where $1 \leq u \leq n$, $1 \leq j \leq m$, $1 \leq z \leq p$, $1 \leq b \leq q$, $p_u \in P$
$Sh_{(p_u,j)}(z, b, l)$	$n \times m$ Cover Shares of size $p \times 4q$ (generated using $n \times m$ Cover images) where $1 \leq z \leq p$, $1 \leq b \leq q$, $1 \leq l \leq 4$, $p_u \in P$
$M(z, b)$	Mask Cover Image of size $p \times q$ where $1 \leq z \leq p$, $1 \leq b \leq q$
$MS(z, b, l)$	Mask Cover share of size $p \times 4q$ (generated using Mask Cover Image) where $1 \leq z \leq p$, $1 \leq b \leq q$, $1 \leq l \leq 4$
S^0 and S^1	Basis matrices of a perfect black VCS
$D_{(p_u,j)}$	$D_{(p_u,j)}$ is a block of size 1×4 in $Sh_{(u,j)}$ generated for a pixel s in SI, $p_u \in P$
MD	MD is a block of size 1×4 in MS generated for a pixel s in SI

Let $P = \{p_1, p_2, p_3, \ldots, p_t, p_{t+1}, p_{t+2}, \ldots, p_n\}$ be the set of participants, and 2^P denotes the power set of P. Let us 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 $\Gamma_{QM} = \{A \in \Gamma_{Qual} : A' \notin \Gamma_{Qual}$ for all $A' \subseteq A, A' \neq A\}$ be the set of minimal qualified subset of P. Let Γ_{FM} be denoted as the maximum forbidden set of P. Then the pair $\Gamma = (\Gamma_{Qual}, \Gamma_{Forb})$ is denoted as the access structure of the scheme. Let S be a $n \times m$ Boolean matrix and $A \subseteq P$. The vector obtained by applying the Boolean operation (e.g.: OR) using rows of S corresponding to the elements of A is denoted by S_A. Then $w(S_A)$ is denoted as the Hamming weight of vector S_A. The definition for contrast and security of the VCS are given in [3].

Define two sets $L = \{p_1, p_2, p_3, \ldots, p_t\}$ and $R = \{p_{t+1}, p_{t+2}, \ldots, p_n\}$ which contains t respectively $(n-t)$ participants. For a (t, k, n)-EVCS the minimal qualified set is

represented as $\Gamma_{QM} = \{A: A \subseteq P, L \in A \text{ and } |A| = k\}$. It is mandatory that all the participants in the set L and any k participants from set R need to involve in the reconstruction phase of a (t, k, n)-EVCS [8–10].

In this paper, we propose a deterministic EVCS for (t, k, n) access structure with a related contrast of 0.25. Our scheme is applicable only for sharing binary images. In the deterministic EVCS given in papers [13, 14, 16–20], each of the participants carry single meaningful image as share. Our proposed constructions are similar to the deterministic EVCS given in paper [15], where each of the participants carries multiple meaningful images as shares. Our EVCS has better reconstruction image quality than the deterministic EVCS constructions given in papers [13–20]. Table 1 describes the notations used in our algorithm.

2 A (t, k, n)-EVCS with Reduced Pixel Expansion

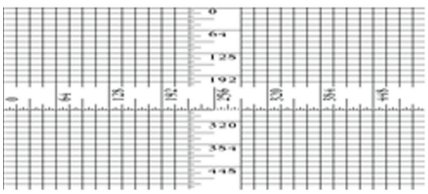
Let us define a set $L = \{p_1, p_2, p_3, \ldots, p_t\}$ which contains t essential participants and $R = \{p_{t+1}, p_{t+2}, \ldots, p_n\}$ which contains $(n - t)$ remaining participants. For a (t, k, n)-EVCS the minimal qualified set is represented as $\Gamma_{QM} = \{A: A \subseteq P, L \in A \text{ and } |A| = k\}$. It is mandatory that all the participants in the set L and any k participants from set R need to involve in the reconstruction phase of (t, k, n)-EVCS.

In today's world, there is a need for storing user's valuable private data like texts, images, passwords, or keys, on his/her computer or on any other electronic device. But in the current computing world all devices can fall prey to viruses, spyware, Trojan horses and other types of malware, exposing user data and breaching his/her privacy. Under such circumstances, it becomes paramount for a user or company to ensure the confidentiality of his/her data. One of the applications of essential access structure $(1, k, n)$-VCS in this scenario is that, user can store copies of the essential share in each of his/her own devices (home computer, mobile phones etc.) and outsource the remaining $n - 1$ shares to $n - 1$ trusted servers. So, an event of corruption or loss of his/her own single device will not result in the loss of data. Even on compromise of $k - 1$ servers, it will not expose the private information of user to public. A $(1, k, n)$ scheme is a (t, k, n) scheme where the value of t is 1. Figure 1 shows the experimental results and implies that our scheme has better contrast than Ateniese et al. [13] scheme. The following section shows our proposed algorithm for share generation and secret reconstruction for (t, k, n)-EVCS.

2.1 Share Generation and Distribution Phase

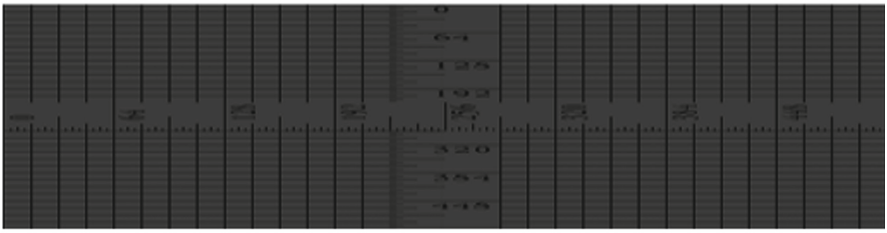
Input:

1. SI and a random image K of size $p \times q$.
2. The t cover images $COV_{(p_r,1)}$ of size $p \times q$, where $p_r \in L$, $1 \leq r \leq t$.
   ($COV_{(p_r,1)}$, used for generating meaningful shares for t mandatory participants in L).
3. The $(n-t) \times m$ cover images $COV_{(p_u,j)}$ of size $p \times q$, where $p_u \in R$, $(t+1) \leq u \leq n$.



Secret Image (*SI*)

Probabilistic Yang *et.al.* [11]



Our Deterministic EVCS

Deterministic EVCS by Ateniese *et al.*[13]

Fig. 1. Reconstructed image for (2, 3) scheme

($COV_{(p_u,j)}$, used for generating meaningful shares for remaining $(n-t)$ participants where $1 \leq j \leq m$, pixel expansion of a perfect black $(k-t, n-t)$ scheme is m).

4. S^0 and S^1 are basis matrices of a perfect black $(k-t, n-t)$-VCS of size $(n-t) \times m$.
5. Let *Odd* (resp. *Even*) be column vectors of size $(t \times 1)$ which contain odd (resp. even) number of ones.
6. Set *Mp* (*Mp* contains any one essential participant, $|Mp| = 1$).

Algorithm:

Step 1. Let $E(z,b) = SI(z,b) \oplus K(z,b)$;

Step 2. Based on share generation given in [5, 6 and 7]

$$H_{(p_r,1)}(z,b) = \begin{cases} Odd(r) & if\ E(z,b) == 1 \\ Even(r) & if\ E(z,b) == 0 \end{cases} \text{ and}$$

$$H_{(p_u,j)}(z,b) = \begin{cases} S^0(p_u,j) & if\ K(z,b) == 0 \\ S^1(p_u,j) & if\ K(z,b) == 1 \end{cases}$$

where, $1 \le r \le t, (t+1) \le u \le n, 1 \le j \le m$. While encoding each pixel, S^0 or S^1 is updated with same column permutation.

Step 3.

for z = 1 to p

for b = 1 to q

for r = 1 to t

If $H_{(p_r,1)}(z,b) = 0$ and $COV_{(p_r,1)}(z,b) = 0$

Set $Q_{(p_r,1)}(1) = 0; Q_{(p_r,1)}(2) = 1; Q_{(p_r,1)}(3) = 0; Q_{(p_r,1)}(4) = 0;$

If $H_{(p_r,1)}(z,b) = 0$ and $COV_{(p_r,1)}(z,b) = 1$

Set $Q_{(p_r,1)}(1) = 0; Q_{(p_r,1)}(2) = 1; Q_{(p_r,1)}(3) = 0; Q_{(p_r,1)}(4) = 1;$

If $H_{(p_r,1)}(z,b) = 1$ and $COV_{(p_r,1)}(z,b) = 0$

Set $Q_{(p_r,1)}(1) = 0; Q_{(p_r,1)}(2) = 0; Q_{(p_r,1)}(3) = 1; Q_{(p_r,1)}(4) = 0;$

If $H_{(p_r,1)}(z,b) = 1$ and $COV_{(p_r,1)}(z,b) = 1$

Set $Q_{(p_r,1)}(1) = 0; Q_{(p_r,1)}(2) = 1; Q_{(p_r,1)}(3) = 1; Q_{(p_r,1)}(4) = 0;$

end

for j = 1 to m

for $u = t+1$ to n

If $H_{(p_u,j)}(z,b) = 0$ and $COV_{(p_u,j)}(z,b) = 0$

Set $Q_{(p_u,j)}(1) = 0; Q_{(p_u,j)}(2) = 1; Q_{(p_u,j)}(3) = 0; Q_{(p_u,j)}(4) = 0;$

If $H_{(p_u,j)}(z,b) = 0$ and $COV_{(p_u,j)}(z,b) = 1$

Set $Q_{(p_u,j)}(1) = 0; Q_{(p_u,j)}(2) = 1; Q_{(p_u,j)}(3) = 0; Q_{(p_u,j)}(4) = 1;$

If $H_{(p_u,j)}(z,b) = 1$ and $COV_{(p_u,j)}(z,b) = 0$

Set $Q_{(p_u,j)}(1) = 0; Q_{(p_u,j)}(2) = 0; Q_{(p_u,j)}(3) = 1; Q_{(p_u,j)}(4) = 0;$

If $H_{(p_u,j)}(z,b) = 1$ and $COV_{(p_u,j)}(z,b) = 1$

Set $Q_{(p_u,j)}(1) = 0; Q_{(p_u,j)}(2) = 1; Q_{(p_u,j)}(3) = 1; Q_{(p_u,j)}(4) = 0;$

end

end

Apply same column permutation for all the $Q_{(p_u,j)}$ matrices and *MD* matrix of size 1×4.

for $j = 1$ to m

for $u = t+1$ to n

for $l = 1$ to 4

$Sh_{(p_u,j)}(z,b,l) = Q_{(p_u,j)}(l)$;

end

end

end

for $l = 1$ to 4

$MS(z,b,l) = MD(l)$;

for $r = 1$ to t

$Sh_{(p_r,1)}(z,b,l) = Q_{(p_r,1)}(l)$;

end

end

end

end

Output:

1. Shares $\{Sh_{(p_r,1)}: 1 \le r \le t\}$. The t meaningful shares of size $p \times 4q$ are distributed to t mandatory participants in set L.
2. Shares $\{Sh_{(p_u,j)}: (t+1) \le u \le n, 1 \le j \le m\}$. The $(n-t) \times m$ meaningful shares of size $p \times 4q$ are distributed to remaining participants in set R.
3. Share MS of size $p \times 4q$ is distributed to participants in the set Mp.

2.2 Secret Reconstruction Phase

Step 1. λ_j's are generated by OR-ing shares $Sh_{(p_u,j)}$ of any $(k-t)$ out of $(n-t)$ participants in $R = \{p_{t+1}, p_{t+2}, \ldots, p_n\}$, where $1 \le j \le m$.

Step 2.

The construction of K can be done using any one of the following schemes

a) Cimato *et al.* [5] (OR and NOT operation) **b)** Wang *et al.* [6] (OR and XOR operation) and **c)** Praveen *et al.* [7] (OR and AND operation).

a) Cimato *et al.* [5]

for $z = 1$ to p

for $b = 1$ to q

for $l = 1$ to 4

1. $\sigma(z,b,l) = \overset{m}{\underset{j=1}{\otimes}} f(\lambda_j(z,b,l)$

2. $K(z,b,l) = f(\sigma(z,b.,l))$;

end

end

end

b) Wang *et al.* [6]

for $z = 1$ to p

for $b = 1$ to q

for $l = 1$ to 4

$K(z,b,l) = \overset{m}{\underset{j=1}{\oplus}} \lambda_j(z,b,l)$;

end

end

end

c) Praveen *et al.* [7]

for $z = 1$ to p

for $b = 1$ to q

for $l = 1$ to 4

$K(z,b,l) = \overset{m}{\underset{j=1}{\Theta}} \lambda_j(z,b,l)$;

end

end

end

Step 3. XOR-ing the shares of all the participants in the set L along with K will generate RI. Then AND-ing RI with MS will reconstruct the secret OI.

for $z = 1$ to p
  for $b = 1$ to $4q$
    for $l = 1$ to 4
$$RI(z,b) = K(z,b) \oplus Sh_{(p_1,1)}(z,b) \oplus \ldots\ldots\ldots \oplus Sh_{(p_r,1)}(z,b)$$
$$OI(z,b,l) = RI(z,b,l) \quad \Theta \quad MS(z,b,l)$$
    end
  end
end

Tables 2, 3 and 4 shows the comparison results.

Table 2. Reconstruction operations count for (t, k, n)

Operation	Cimato *et al.* [5]	Wang *et al.* [6]	Praveen *et al.* [7]
OR	$4 \times (m(k-t)+(m-1))$	$4 \times (m(k-t)))$	$4 \times (m(k-t))$
NOT	$4 \times (m+1)$	0	0
AND	4	4	$4m$
XOR	$4t$	$4t + 4(m-1)$	$4t$

Table 3. Comparison of deterministic (1, 3, 4) scheme

Scheme	Operations	APE	α_{RI}
Ateniese *et al.* [13]	OR	10	0.100
Liu *et al.* [14]	OR	16	0.062
Wang *et al.* [16]	OR	16	0.062
Yan *et al.* [19]	OR	16	0.062
Our scheme (Sect. 2.1)	OR, XOR, AND	11	0.250

2.3 Analysis on the Pixel Expansion, Contrast and Security

The matrices S^0 (resp. S^1) are constructed based on the Definition 1. The proposed (t, k, n)-perfect black EVCS is valid only when the following three conditions meet.

Condition 1: It should not be possible for any $(k-t)$ participant in the set R out of $(n-t)$ participants to identify SI in the absence of participants in the set L.

Table 4. Comparison of deterministic (2, 4, 5) scheme

Scheme	Operations	APE	α_{RI}
Ateniese *et al.* [13]	OR	18	0.055
Liu *et al.* [14]	OR	25	0.040
Wang *et al.* [16]	OR	32	0.031
Yan *et al.* [19]	OR	32	0.031
Our scheme (Sect. 2.1)	OR, XOR, AND	9.6	0.250

Condition 2: It should not be possible for any participant less than $(k-t)$ in the set R out of $(n-t)$ participants to identify SI with participants in the set L.

Condition 3: It should be possible for any $(k-t)$ in the set R out of $(n-t)$ participants to identify SI in the presence of all participants in the set L. The first two conditions are for the security of the scheme and the third is for the correctness of reconstruction. Assume that variables q, b, b_1, b_2, z take the values either 0 or 1. Let $Pbr(q = b)$ denote the probability of occurrence of q equal to b. Let b_1 and b_2 be the two independent bits and $q = b_1 \oplus b_2$. Let $Pbr((q = b_2)/(b_1 = z))$ be the probability of $q = b_2$ given bit b_1 equal to z.

Lemma 1: Let b_1 (resp. b_2) be known (resp. unknown) bit and $q = b_1 \oplus b_2$ then

$$Pbr((q = b_2)/(b_1 = 0)) = Pbr((q = b_2)/(b_1 = 1)) = \frac{1}{2}.$$

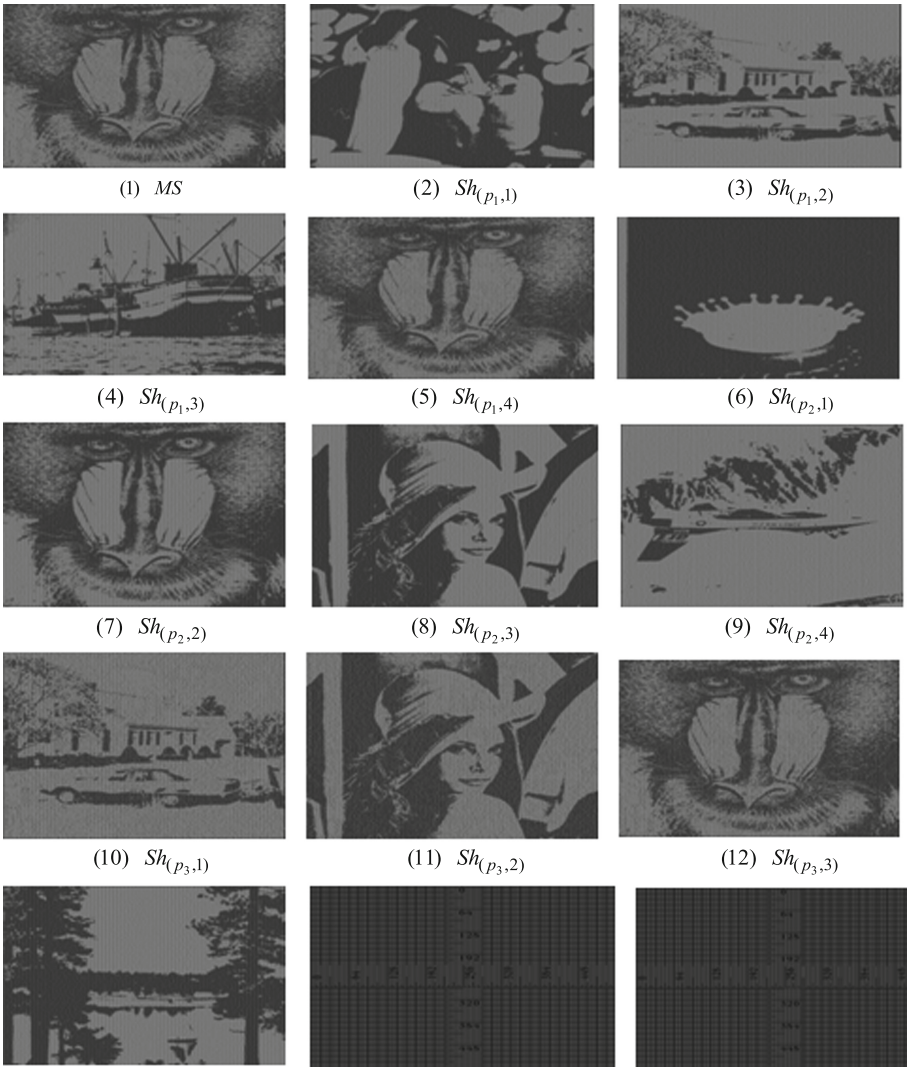
Proof: Here the given information is b_1 and $q = b_1 \oplus b_2$. But b_2 is unknown then, $Pbr((q = 0)/(b_1 = 0)) = Pbr((q = 1)/(b_1 = 0)) = \frac{1}{2}$ and $Pbr((q = 0)/(b_1 = 1)) = Pbr((q = 1)/(b_1 = 1)) = \frac{1}{2}$ accordingly,$Pbr((q = b_2)/(b_1 = 0)) = Pbr((q = b_2)/(b_1 = 1)) = \frac{1}{2}$.

Lemma 2: Given two bits b_1, b_2 and $q = b_1 \oplus b_2$ then $Pbr((q = b_2)/(b_1 = 0)) = 1$ and $Pbr((q = b_2)/(b_1 = 1)) = 0$.

Proof: Here the given information is b_1, b_2 and $q = b_1 \oplus b_2$ then, $Pbr((q = 0)/(b_1 = 0)) = Pbr((q = 1)/(b_1 = 0)) = 1$ and $Pbr((q = 0)/(b_1 = 1)) = Pbr((q = 1)/(b_1 = 1)) = 0$ accordingly, $Pbr((q = b_2)/(b_1 = 0)) = 1$ and $Pbr((q = f(b_2))/(b_1 = 1)) = 1$.
which implies that $Pbr((q = b_2)/(b_1 = 1)) = 0$.

Let x be a bit obtained by combining the shares (MS is not taken) of any $(k-t)$ out of $(n-t)$ participants from the set R. Let y be a bit obtained by combining all the shares of participants in the set $L$and s is the secret bit in RI. Then $s = x \oplus y$.The security for Condition 1 and 2 can be proved using Lemma 1.

Condition 1: Here $b_1 = y$ (is given), $b_2 = x$ (is unknown bit either 0 or 1) and $q = s$ (either 0 or 1). $Pbr((s = x)/(y = 0)) = Pbr((s = x)/(y = 1)) = \frac{1}{2}$ (Lemma 1).



(1) MS (2) $Sh_{(p_1,1)}$ (3) $Sh_{(p_1,2)}$

(4) $Sh_{(p_1,3)}$ (5) $Sh_{(p_1,4)}$ (6) $Sh_{(p_2,1)}$

(7) $Sh_{(p_2,2)}$ (8) $Sh_{(p_2,3)}$ (9) $Sh_{(p_2,4)}$

(10) $Sh_{(p_3,1)}$ (11) $Sh_{(p_3,2)}$ (12) $Sh_{(p_3,3)}$

(13) $Sh_{(p_3,4)}$ (14) $RI(p_1, p_2, p_3)$ (15) $OI(p_1, p_2, p_3)$

Fig. 2. Experimental results for our (2, 3) EVCS

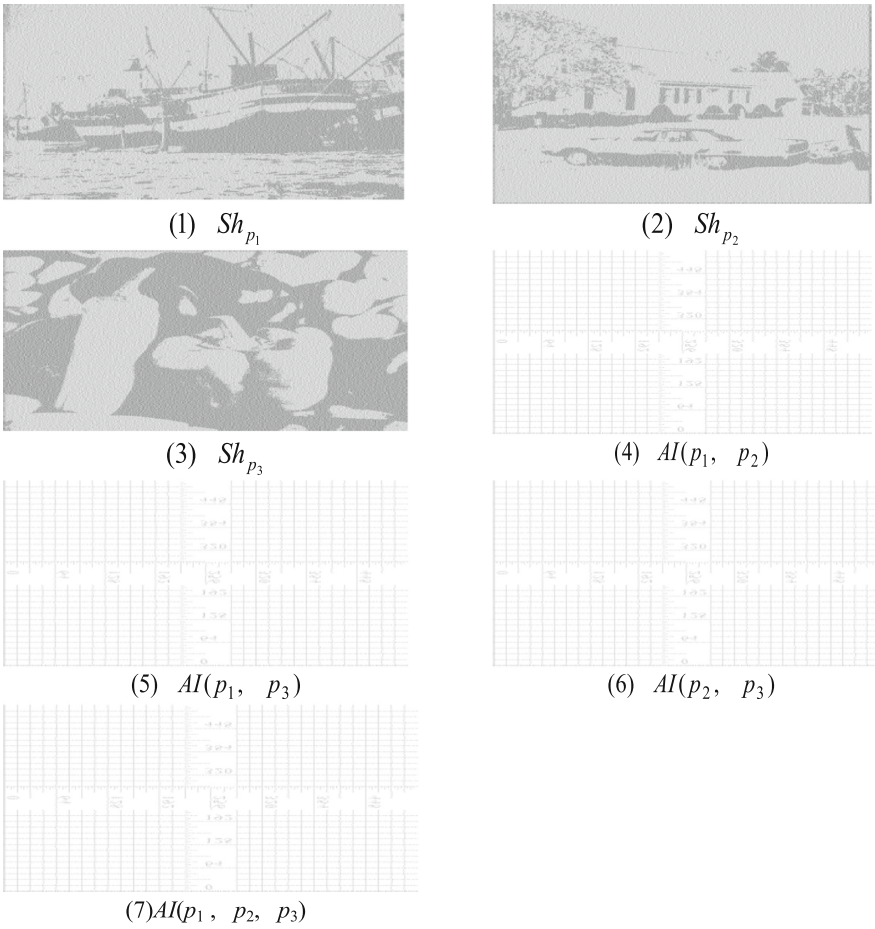


Fig. 3. Experimental results for (2,3) EVCS by Ateniese *et al.* [13]

Condition 2: Here $b_1 = x$ (is given), $b_2 = y$ (is unknown bit either 0 or 1) and $q = s$ (either 0 or 1). $Pbr((s = y)/(x = 0)) = Pbr((s = y)/(x = 1)) = \frac{1}{2}$ (Lemma 1).

Condition 3: Here $b_1 = y$, $b_2 = x$ (is given) and $q = s$. $Pbr((s = x)/(y = 0)) = 1$, $Pbr((s = x)/(y = 1)) = 0$ (Lemma 2).

Figure 2 shows the experimental results of our scheme with meaningful shares (*Sh*) and reconstructed images (*RI* and *OI*). Figure 3 shows the experimental results of Ateniese *et al.* [13] scheme with meaningful shares (*Sh*) and reconstructed images (*AI*). It is clear that the contrast of *AI* is less than *OI*.

3 Conclusion

Even though deterministic schemes need huge amount of data, it guarantees reconstruction of all the secret data correctly. In the case of probabilistic scheme there is no such guarantee. So constructions of deterministic schemes with high relative contrast and less pixel expansion are of great demand. In this paper a deterministic EVCS for (t, k, n) access structure is proposed. It is true that in our constructions OR, XOR and AND Boolean operations are used for reconstruction instead of only OR operation as in existing EVCS constructions. But the experimental results show that, the quality of reconstructed image for our EVCS is better when compared to other related EVCS.

References

1. Naor, M., Shamir, A.: Visual cryptography. In: De Santis, A. (ed.) Eurocrypt 1994. LNCS, vol. 950, pp. 1–12. Springer, Heidelberg (1994). https://doi.org/10.1007/BFb0053419
2. Adhikari, A.: 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 (2014)
3. Ateniese, G., Blundo, C., De Santis, A., Stinson, D.R.: Visual cryptography for general access structures. Inf. Comput. **129**(2), 86–106 (1996)
4. Blundo, C., De Bonis, A., De Santis, A.: Improved schemes for visual cryptography. Des. Codes Cryptogr. **24**(3), 255–278 (2001)
5. Cimato, S., De Santis, A., Ferrara, A.L., Masucci, B.: Ideal contrast visual cryptography schemes with reversing. Inf. Process. Lett. **93**(4), 199–206 (2005)
6. Wang, D.S., Song, T., Dong, L., Yang, C.N.: Optimal contrast grayscale visual cryptography schemes with reversing. IEEE Trans. Inf. Forensics Secur. **8**(12), 2059–2072 (2013)
7. Praveen, K., Sethumadhavan, M.: Ideal contrast visual cryptography for general access structures with AND operation. In: Nagar, A., Mohapatra, D.P., Chaki, N. (eds.) Proceedings of 3rd International Conference on Advanced Computing, Networking and Informatics. SIST, vol. 44, pp. 309–314. Springer, New Delhi (2016). https://doi.org/10.1007/978-81-322-2529-4_32
8. Arumugam, S., Lakshmanan, R., Nagar, A.K.: On (k, n) *-visual cryptographic scheme. Des. Codes Cryptogr. **71**(1), 153–162 (2014)
9. Guo, T., Liu, F., Wu, C.K., Ren, Y.W., Wang, W.: On (k, n) visual cryptography scheme with t essential parties. In: Padró, C. (ed.) ICITS 2013. LNCS, vol. 8317, pp. 56–68. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-04268-8_4
10. Dutta, S., Rohit, R.S., Adhikari, A.: Constructions and analysis of some efficient t-(k, n)* - visual cryptographic schemes using linear algebraic techniques. Des. Codes Cryptogr. 1–32 (2016)
11. Yang, C.N.: New visual secret sharing schemes using probabilistic method. Pattern Recogn. Lett. **25**, 481–494 (2004)
12. Liu, F., Wu, C., Lin, X.: Step construction of visual cryptographic schemes. IEEE Trans. Inf. Forensics Secur. **5**(1), 25–34 (2010)
13. Ateniese, G., Blundo, C., De Santis, A., Stinson, D.R.: Extended capabilities for visual cryptography. Theor. Comput. Sci. **250**(1), 143–161 (2001)
14. Liu, F., Wu, C.: Embedded extended visual cryptography schemes. IEEE Trans. Inf. Forensics Secur. **6**(2), 307–322 (2011)
15. Zhou, Z., Arce, G.R., Di Crescenzo, G.: Halftone visual cryptography. IEEE Trans. Image Process. **15**(8), 2441–2453 (2006)

16. Wang, Z., Arce, G.R., Di Crescenzo, G.: Halftone visual cryptography with error diffusion. IEEE Trans. Inf. Forensics Secur. **4**(3), 383–396 (2009)
17. Wang, D., Yi, F., Li, X.: On general construction for extended visual cryptography schemes. Pattern Recogn. **42**(11), 3071–3082 (2009)
18. Yang, C.N., Yang, Y.Y.: New extended visual cryptography schemes with clearer shadow images. Inf. Sci. **271**, 246–263 (2014)
19. Yan, X., Wang, S., Niu, X., Yang, C.N.: Halftone visual cryptography with minimum auxiliary black pixels and uniform image quality. Digit. Sig. Process. **38**, 53–65 (2015)
20. Lu, S., Manchala, D., Ostrovsky, R.: Visual cryptography on graphs. J. Comb. Optim. **21**(1), 47–66 (2011)
21. Lee, K.H., Chiu, P.L.: An extended visual cryptography algorithm for general access structures. IEEE Trans. Inf. Forensics Secur. **7**(1), 219–229 (2012)
22. Guo, T., Liu, F., Wu, C.: k out of k extended visual cryptography scheme by random grids. Sig. Process. **94**, 90–101 (2014)
23. Chiu, P.L., Lee, K.H.: User-friendly threshold visual cryptography with complementary cover images. Sig. Process. **108**, 476–488 (2015)
24. Ou, D., Sun, W., Wu, X.: Non-expansible XOR-based visual cryptography scheme with meaningful shares. Sig. Process. **108**, 604–621 (2015)
25. Yan, X., Wang, S., Niu, X., Yang, C.N.: Generalized random grids-based threshold visual cryptography with meaningful shares. Sig. Process. **109**, 317–333 (2015)
26. Wang, S., Yan, X., Sang, J., Niu, X.: Meaningful visual secret sharing based on error diffusion and random grids. Multimedia Tools Appl. **75**(6), 3353–3373 (2016)
27. Praveen, K., Sethumadhavan, M., Krishnan, R.: Visual cryptographic schemes using combined Boolean operations. J. Discrete Math. Sci. Cryptogr. **20**(2), 413–437 (2017)