Cheating Immune Visual Cryptographic Scheme with Reduced Pixel Expansion

Kanakkath Praveen and M. Sethumadhavan

Abstract One of the drawbacks in visual cryptography is cheating attacks, where the malicious adversaries can cheat the honest participant by submitting fake shares during reconstruction phase. Cheating immune visual cryptographic schemes are used for mitigating cheating attacks in visual cryptography. There are two types of cheating immune schemes: One is share authentication-based schemes, and the other is blind authentication-based schemes. For the existing blind authentication-based schemes, the pixel expansion value will increase in the order of $O(n)$. In this paper, a blind authentication-based cheating immune visual cryptographic scheme is proposed by modifying the existing scheme based on uniform codes where the pixel expansion value will increase in the order of $O(\log n)$.

Keywords Secret sharing · Visual cryptography · Cheating prevention
Cheating immune · Blind authentication

1 Introduction

Visual cryptography is an unconditionally secure secret splitting technique used to generate n shares from a secret image (SI). During the distribution phase, these shares are given to each of the n participants, and the secret image will be visible only during the reconstruction phase when sufficient participants combine their shares. In visual cryptographic scheme (VCS) for reconstruction, the Boolean operators OR, AND, NOT, XOR are used instead of complicated computation as in conventional cryptography. The quality of a VCS is quantified using pixel expansion m and contrast $\alpha.m$. A pixel in SI is converted to m sub pixels in all

K. Praveen (✉) · M. Sethumadhavan
TIFAC-CORE in Cyber Security, Amrita School of Engineering Coimbatore,
Amrita Vishwa Vidyapeetham, Amrita University, Coimbatore, India
e-mail: k_praveen@cb.amrita.edu

M. Sethumadhavan
e-mail: m_sethu@cb.amrita.edu

© Springer Nature Singapore Pte Ltd. 2018

K. Saeed et al. (eds.), *Progress in Advanced Computing and Intelligent Engineering*,
Advances in Intelligent Systems and Computing 563,
https://doi.org/10.1007/978-981-10-6872-0_24

shares. In the reconstructed image, gray levels of black and white pixel differ by α. m. The participants in the qualified (resp. forbidden) set can (resp. cannot) reconstruct the secret image. VCS are of different types namely (2, n), (k, n), and general access structure.VCS can also be classified into deterministic and probabilistic scheme depending upon the reconstruction of the secret. In 1994, Naor and Adi Shamir [1] developed deterministic VCS's, where OR (stacking) operation is used for reconstruction of secret image. The constructions of conventional VCS cannot resist against cheating attacks. So attacks (deterministic white to black (DWtB), deterministic black to white (DBtW) and region based) are possible against honest participants or victims by the malicious adversaries (collusive cheaters, malicious participant, and malicious outsider), by submitting fake shares during reconstruction process. There are two types of cheating immune visual cryptographic scheme (CIVCS): One is share authentication (SA)-based CIVCS, and the other is blind authentication (BA)-based CIVCS. In SA, apart from the shares of participants, extra information generated by the dealer or the participant is needed to verify cheating but in BA the shares are constructed in such a manner that the cheaters are not able to identify the structure of other participant's share. Two SA-based CIVCS are proposed by Yang and Laih [3] in 1999. The verification of shares is done with (resp. without) the help of an online trusted third party in the first (resp. second) CIVCS. The collusive cheating attack in (k, n)—VCS and its two mitigation techniques was developed by Horng et al. [4] in 2006. The first one is a SA technique, where each participant needed to carry extra verification transparencies, while the second technique is a (2, n) scheme based on BA, where (n + l) shares are generated in the sharing phase but only randomly selected n shares are used for distribution which makes cheaters hard to accomplish a successful attack. But, second technique protects only black pixels from cheating while white pixels are vulnerable to attack. Tsai et al. [5] in 2007 proposed a BA-based CIVCS using genetic algorithm by creating multiple homogeneous secret images. Here, the probability of successful cheating is highly decreased compared to [4] second scheme. Hu and Tzeg [6] in 2007 identified that cheating attack is possible by malicious participant or a malicious outsider if the VCS is not following perfect black criteria. The authors showed attacks on [3] first cheating method and on [4] scheme. The paper [6] also proposes SA-based CIVCS with reduced pixel expansion than [3] second method. De Prisco et al. [7] in 2010 proposed an (n, n) BA-based CIVCS and two (2, n) BA-based CIVCS. The first (2, n) scheme is a simple scheme but with a weakness that white pixels are not protected. The second scheme protects both white and black pixels by making use of larger m. Tsai et al. [8] in 2010 showed that the genetic algorithm-based CIVCS given in Tsai et al. [5] decodes the secret share incorrectly. Liu et al. [9] in 2011 proposed a SA-based CIVCS by disclosing t secret pixels to participants during the share distribution phase. The scheme is applicable to every VCS by verifying that the positions of randomly choosing t pixels in the secret are following the same color or not in the reconstructed image. Wang et al. [10] in 2011 proposed a SA-based tagged VCS for cheating prevention. Chen et al. [11] in 2011 showed a new variant of attack called Region cheating attack (RCA) which cheat human visual system (HVS), when for a

region in the secret image if there is a white pixel surrounded by lot of black pixels or a black pixel surrounded by lot of white pixels. The paper also shows that DWtB attack and RCA are possible in the second construction of [7] scheme even though the pixel expansion is high. Chen et al. [12] in 2011 also proposed a BA-based (2, n) scheme which is immune to RCA attack but still vulnerable to DWtB attack. Both Chen et al. [12] and Liu et al. [9] showed that scheme proposed by Hu and Tzeg [6] is not a CIVCS. Chen et al. [13] in 2012 suggested an improvement to [6] CIVCS. Chen et al. in 2012 [13] (resp. 2013 [14]) proposed SA-based (2, n) CIVCS, with (resp. without) extra verification transparency for each participant.

Here, this paper proposes a novel (2, n) CIVCS. The preliminaries for VCS are given in Sect. 2. In Sect. 3, the background for BA-based CIVCS and collusive cheating attacks on VCS is discussed. In Sect. 4, the novel construction of (2, n) CIVCS based on OR operation is explained.

2 Preliminaries

Let $PA = \{pa_1, pa_2, pa_3, \ldots, pa_n\}$ be the participant set and 2^{PA} is the cardinality of power set of PA. Then, the share S_i, $1 \leq i \leq n$ of SI is distributed to each pa_i. Let us denote Γ_{Qual} as a collection of qualified sets and Γ_{Forb} as a collection of forbidden sets, where $\Gamma_{\text{Qual}} \cup \Gamma_{\text{Forb}} = 2^{PA}$ and $\Gamma_{\text{Qual}} \cap \Gamma_{\text{Forb}} = \varphi$, then $\Gamma = (PA, \Gamma_{\text{Qual}}, \Gamma_{\text{Forb}})$ is called the access structure of VCS. Any set $C \in \Gamma_{\text{Qual}}$ can recover SI whereas any set $C \in \Gamma_{\text{Forb}}$ is not able to recover SI. Let $\Gamma_0 = \{C \in \Gamma_{\text{Qual}} : C' \notin \Gamma_{\text{Qual}}$ for all $C' \subseteq C$, $C' \neq C\}$ be the collection of minimal qualified subset of PA. Let B_1 and B_0 are two collections which consist of $n \times m$ Boolean matrices used for constructing n shares of SI. The row of each matrix in both B_1 and B_0 corresponds to m sub pixels. For sharing a 1 (resp. 0) pixel in SI, randomly choose a matrix T from B_1 (resp. B_0) and assign row i of T to the corresponding positions of share S_i, $1 \leq i \leq n$. The matrices in the two collections B_1 (resp. B_0) consist of all column permutations of T_1 (resp. T_0). The vector obtained by bitwise OR operation to the rows of T corresponding to the elements in PA is represented as T_{PA}. Let $w(T_{PA})$ denotes the Hamming weight of the vector T_{PA}. The stacking corresponds to the bitwise operation between sub pixels in the shares (S_i).

Definition 1 [2]: Let $\Gamma = (PA, \Gamma_{\text{Qual}}, \Gamma_{\text{Forb}})$ be an access structure. Two collections B_1 and B_0 constitute a (Γ, m)—VCS if there exists a value $\alpha(m) > 0$ and a set $\{(PA, t_{PA})\}_{PA \in \Gamma Qual}$ which satisfies the following conditions.

1. Any set $\{pai_1, pai_2, pai_3, \ldots, pai_q\} \in \Gamma_{Qual}$ can recover SI by stacking their shares. Formally, for any $T \in B_0$, $w(T_{PA}) \leq t_{PA} - \alpha.m$, whereas for any $T \in B_1$, $w(T_{PA}) \geq t_{PA}$.
2. Any set $\{pai_1, pai_2, pai_3, \ldots, pai_q\} \in \Gamma_{Forb}$ has no information on SI. Formally, the collections B_t, $t \in \{0, 1\}$ of $q \times m$ matrices obtained by restricting each

$n \times m$ matrix in $T \in B_t$ to rows $i_1, i_2, i_3, \ldots, i_q$ are indistinguishable in the sense that they contain the same matrices with the same frequencies.

The property 1 (resp. 2) ensures contrast (resp. security) of the scheme. The following is an example of (2, 3)—VCS with contrast $\alpha = \frac{1}{3}$ and $m = 3$, for $PA = \{pa_1, pa_2, pa_3\}$, where $\Gamma_{Qual} = \{\{pa_1, pa_2\}, \{pa_3, pa_2\}, \{pa_1, pa_3\}, \{pa_1, pa_2, pa_3\}\}$ and $\Gamma_{Forb} = \{\{pa_1\}, \{pa_2\}, \{pa_3\}\}$.

Example 1 Let the basis matrices be $T_0 = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}$ and $T_1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$. Then, when stacking the value of $w(T_{PA}) = 2$ is obtained for black pixel, and the value of $w(T_{PA}) = 1$ is obtained for white pixel.

3 A Review of Collusive Cheating Attacks and CIVCS's

3.1 DWtB and DBtW Attack—Horng et al. (2006) [4]

Let S_1, S_2, and S_3 are three distinct shares of SI, and they are distributed to each participant pa_1, pa_2, and pa_3, respectively. Let pa_1 and pa_2 are the adversaries, and pa_3 is the honest participant. During attack, pa_1 and pa_2 will create fake block F by predicting the share structure of pa_3. Let us explain a DWtB and DBtW attack using the basis matrices given in the example of Sect. 2. For 0 pixel, the block in the shares of pa_1, pa_2, and pa_3 is [1 0 0]. If the cheaters pa_1 and pa_2 collusively identify the structure of pa_3, they can create F using the blocks [0 1 0] and [0 0 1], respectively. The stacking of F and corresponding block in S_3 will result in a 1 pixel. This is DWtB attack. For the secret pixel 1, the blocks in the shares of pa_1, pa_2, and pa_3 are [1 0 0], [0 1 0], [0 0 1], respectively. If pa_1 and pa_2 collusively identify the structure of pa_3 to generate F as [0 0 1], the stacking of F with corresponding block in S_3 will results in a white pixel. This is DBtW attack.

3.2 CIVCS—Horng et al. (HCT) (2006) [4]

In this method instead of creating n shares and distribute it to each participants, $(n + l)$ shares are generated from SI, and randomly picked n shares are distributed to each participant. This scheme will protect pixel 1 but not pixel 0. The probability that adversaries can correctly guess the 1 pixel's in the honest participants share is $\frac{1}{l+1}$. This scheme can protect only DBtW attack, but not DWtB attack. Section 2.3 of paper [4] explains how complementary images can be used to make this scheme immune against DWtB attack.

3.3 Simple CIVCS—de Prisco et al. (DD1) (2010) [7]

Let T_1 (resp. T_0) be the basis matrices shown in example of Sect. 2, then the basis matrices for CIVCS are given by A_1 (resp. A_0) for 1 (resp. 0) pixel are

$$A_0 = \left[\begin{array}{c|c} \begin{matrix}0\\.\\0\end{matrix} & T_0 \end{array}\right] \text{ and } A_1 = \left[\begin{array}{c|c} \begin{matrix}0\\.\\0\end{matrix} & T_1 \end{array}\right]$$

respectively. This scheme also can protect only DBtW attack, but not DWtB attack.

3.4 Better CIVCS—de Prisco et al. (DD2), 2010

Let A_1 (resp. A_0) be the basis matrices of $DD1$ scheme given above. Let D be a matrix which contain all possible 2^n column vectors, then the basis matrices B_1 (resp. B_0) for 1 (resp. 0) pixel for better scheme are $[D \quad A_0]$ (resp.$[D \quad A_1]$). But it is shown in Sect. 4 of paper [11] that, this scheme is also vulnerable to collusive cheating.

4 Proposed (2, *N*)—CIVCS's

4.1 MS CIVCS—Modified (Sreekumar and Babusundar 2008) [15]

A uniform code of length t consists of precisely $\lceil \frac{t}{2} \rceil$ 1's and $\lfloor \frac{t}{2} \rfloor$ 0's. Let N_t denote the number of uniform codes of length t, where $N_t = \binom{t}{\lfloor \frac{t}{2} \rfloor}$. In the construction of (2, n)—VCS based on OR operation by Sreekumar and Babusundar [15], the $n \leq N_t$ shares are generated using uniform codes. The scheme [15] is vulnerable to DWtB in the case of more than two collusive adversaries for any value of n and vulnerable to DBtW attack in the case of $n - 1$ collusive adversaries only when $n == N_t$. But, in the case of 2 to $n - 2$ collusive adversaries, the scheme [15] is immune to DBtW attack when $n == N_t$. The following shows an example of vulnerability of the scheme [15].

Example 2 For constructing a (2, 6)-VCS using uniform codes [15], let us select the value of $t = 4$, which satisfies the condition $n \leq N_t$. The ($N_t = 6$) distinct uniform codes for the value of $t = 4$ are given in $UC = \{1100, 0110, 0011, 1001, 1010,$

0101}. Let $M = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}$ be a matrix constructed using *UC*. For sharing a pixel 1, a randomly selected row from M is distributed to all the six participants. For sharing a pixel 0, each row of M is distributed to six corresponding participants. Here, DWtB attack is possible because when any $n-1$ cheaters (here 5) collude, they can predict the block of the victim as [1 0 0 1], if the matrix used for sharing a pixel 0 is $\begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix}$.The five cheaters can conduct a DWtB attack by generating the fake matrix $\begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}$. Here, DBtW attack is possible because when any $n-1$ cheaters (here 5) collude, they can predict the block of the victim as [1 0 0 1], if the matrix used for sharing a pixel 1 is $\begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}$.The five cheaters can conduct a DBtW attack by generating the fake matrix $\begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix}$. Here, in this example, the value of $n = 6$ and the value of $N_t = 6$. So when $n == N_t$, DBtW attack is possible by $n-1$ (here 5) cheaters.

Proposed construction: The following are the steps done by the dealer.

Step1: **If** the value of $n == N_t$, then M be the basis matrix of order $N_{t+1} \times (t+1)$ and each element in the matrices is different vectors of length $(t+1)$.
Else M be the basis matrix of order $N_t \times t$, and each row in the matrices is different vectors of length t.

Step2: Construct a set G which is a collection of different row permuted matrix of M.

Step3: This step is applicable to all pixels in SI. The dealer randomly selects a matrix from G and constructs another matrix K of order $n \times (t+1)$ or $n \times t$ based on the value of n. For sharing 1, the dealer uses any row permuted matrix K, and for sharing 0 the dealer selects any one row of matrix K and distribute to all n participants.

Theorem 1: The MS—(2, n) CIVCS is vulnerable to DWtB attack but immune to DBtW attack.

Proof Let TS be the share of honest participant, and let B be the block corresponding to 1 of SI, and W is a block corresponding to 0 of SI. The dealer selects a matrix M of order $N_m \times m$, where $m = \begin{Bmatrix} t+1 & if \quad n==N_t \\ t & Otherwise \end{Bmatrix}$, $n \geq 2$ and $t \geq 2$. Here, when any d collusive participants (cheaters) combine, the probability for correctly guessing B in TS is $\frac{1}{N_m - d}$, and the probability for correctly guessing W in TS is 1.

This scheme is used as a BA-based CIVCS which can resist both DWtB and DBtW attack, if the shares of complementary secret image are also distributed to participants analogous to (2, $n + l$)—CIVCS constructed by Horng et al. [4]. Assume that SI = [1 0] be the secret image to be shared using (2, 3)—CIVCS. For constructing a CIVCS, we need to generate a complementary matrix of SI, say $SI^{'}$ = [0 1]. Both SI and $SI^{'}$ are shared among the three participants.

Example 3 For constructing a (2, 6)—CIVCS, let us select a matrix $K = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{bmatrix}$ which satisfies the following criteria $n \leq N_t$. Here, if any five collusive adversaries combine, they cannot predict the block corresponding to pixel 1. So the scheme is immune to DBtW attack. If complementary secret is also shared with the original secret, the scheme resists DWtB attack also.

4.2 Comparison of CIVCS's

Below Tables 1 and 2 show the comparison of proposed MS CIVCS with related works which are reported as secure in the paper [14] (CTH).

Table 1 Comparison of secure (2, n)—CIVCS's

Scheme	HCT	DD1	CTH	MS
Reconstruction operation	OR	OR	OR	OR
Type of CIVCS	BA	BA	SA	BA
Complimentary secret image	YES	YES	NO	YES
Complexity	$O(n)$	$O(n)$	$O(n)$	$O(\log n)$

Table 2 Pixel expansion of secure (2, n)—CIVCS's

N	HCT($l = 1$) $2 \times (n+l)$	DD1 $2 \times (n+1)$	CTH $(2 \times n) + 1$	MS $2 \times m$
2	6	6	5	6 ($t = 3$)
4	10	10	9	8 ($t = 4$)
6	14	14	13	10 ($t = 5$)
8	18	18	17	10 ($t = 5$)
10	22	22	21	12 ($t = 6$)
15	32	32	31	12 ($t = 6$)
18	38	38	37	12 ($t = 6$)

5 Conclusion

The order of pixel expansion for the existing secure blind authentication based (2, n)—CIVCS's is $O(n)$. Here, we proposed a (2, n)—CIVCS which can prevent $n - 1$ cheaters by modifying Sreekumar and Babusundar [15] uniform code scheme in which the order of pixel expansion is $O(\log n)$.

References

1. Naor, M., Shamir, A.: Visual cryptography. In: EUROCRYPT. Lecture Notes in Computer Science, vol. 950, pp. 1–12. Springer, Berlin Heidelberg (1994)
2. Ateniese, G., Blundo, C., DeSantis, A., Stinson, D.R.: Visual cryptography for general access structures. Inf. Comput. **129**(2), 86–106 (1996)
3. Yang, C.N., Laih, C.S.: Some new type of visual secret sharing schemes. In: National computer symposium, vol. 3, pp. 260–268 (1999)
4. Horng, G., Chen, T.H., Tsai, D.S.: Cheating in visual cryptography. Des. Codes Crypt. **38**(2), 219–236 (2006)
5. Tsai, D.S., Chen, T.H., Horng, G.: A cheating prevention scheme for binary visual cryptography with homogeneous secret images. Pattern Recogn **40**(8), 2356–2366 (2007)
6. Hu, C.M., Tzeng, W.G.: Cheating prevention in visual cryptography. IEEE Trans. Image Process. **16**(1), 36–45 (2007)
7. DePrisco, R., DeSantis, A.: Cheating immune threshold visual secret sharing. Comput J **53**, 1485–1496 (2010)

8. Tsai, D.S., Huang, C.C.: A new deterministic algorithm based cheating prevention scheme for visual cryptography. Hsiuping J. **20** (2010)
9. Liu, F., Wu, C., Lin, X.: Cheating immune visual cryptographic scheme. IET Inf. Secur. **5**(1), 51–59 (2011)
10. Wang, R.Z., Hsu, S.F.: Tagged visual cryptography. IEEE Sig. Process. Lett. **18**(11), 627–630 (2011)
11. Chen, Y.C., Horng, G., Tsai, D.S.: Cheating human vision in visual secret sharing. https://eprint.iacr.org/2011/631.pdf (2011)
12. Chen, Y.C., Horng, G., Tsai, D.S.: Comment on cheating prevention in visual cryptography. IEEE Trans. Image Process. **21**(7), 3319–3323 (2012)
13. Chen, Y.C., Tsai, D.S., Horng, G.: A new authentication based cheating prevention scheme in Naor-Shamir's visual cryptography. J. Vis. Commun. Image Representation **23**(8), 1225–1233 (2012)
14. Chen, Y.C., Tsai, D.S., Horng, G.: Visual secret sharing with cheating prevention revisited. Digit. Sig. Process. **23**(5), 1496–1504 (2013)
15. Sreekumar, A., Babusundar, S.: Uniform secret sharing scheme for (2, *n*) threshold using visual cryptography. Int. J. Inf. Process. **2**(4) (2008)