Design of Visual Cryptography Scheme Using C(m, w) Combinations

Anindya Kr. Biswas, S. Mukhopadhyay and G.P. Biswas

Abstract VCS is a perfect secure technique that allows easy concealment of images without any cryptographic computation, however, the encrypted image can be recovered by human visual system. The scheme is proposed by Naor and Shamir for binary images, called *k-out-of-n* VCS, where $k \leq n$ participants can recover images. Subsequently, a number of efficient VCS models are proposed that enhanced different VCS features. This work proposes a new model for $k = 2, 3$ that generates shares using *C(m, w)*, where a bit string of length m with $w < m$ number of 1's is taken for constructing a share. On analysis, it has been found that our scheme realizes *2-out-of-n* VCS more efficiently than the scheme proposed by Naor et al. Also our design for *3-out-of-n* VCS shows improvement as well as supports access structure similar to Ateniese et al. On simulation, it has been found that our VCS performs satisfactorily.

Keywords Visual cryptography scheme (VCS) · Access structure · Basis matrices · Image contrast and resolution

1 Introduction

The visual cryptographic scheme (VCS) is a new cryptographic paradigm, in which a secret binary image is concealed simply by encoding into multiple invisible shares. And during decoding, a set of predefined shares are stacked together for

A.Kr. Biswas (✉)
Department of Information Technology, MAKAU (WBUT), Kolkata, West Bengal, India
e-mail: anindya.kr.bws@gmail.com

S. Mukhopadhyay · G.P. Biswas
Department of Computer Science and Engineering, Indian School of Mines, Dhanbad, Jharkhand, India
e-mail: msushanta2001@gmail.com

G.P. Biswas
e-mail: gpbiswas@gmail.com

S.C. Satapathy et al. (eds.), *Proceedings of the 5th International Conference on Frontiers in Intelligent Computing: Theory and Applications*, Advances in Intelligent Systems and Computing 516, DOI 10.1007/978-981-10-3156-4_46

reconstruction of the input image through human vision system. It does not involve any cryptographic knowledge and computation as required in any other security design and applications. Its implementation is easy, however the security level is perfect as the scheme is not breakable even with brute-force attack and infinite computation without having adequate shares. In 1995, Naor and Shamir introduced VCS in a seminal paper [1], where without through powerful computers, a technique similar to the security checking by human beings is proposed. It is known as *k-out-of-n* VCS and the secret image is reconstructed if at least any k shares out of $n \geq k$, are combined together.

In general, three major approaches for concealing image and/or data are followed and they are *encryption*, *information hiding* and *secret sharing*. In encryption, the messages are encrypted using known symmetric or public-key methods, where the corresponding private keys are kept secret [2, 3]. In information hiding, the watermarking techniques are used, in which the secret data are hidden into cover images such that the visibility of latter ones are not disturbed [4]. In secret sharing, Naor and Shamir proposed a cryptography scheme for sharing of secret among any of $k \leq n$ *for* n participants [1]. In recovery, any k or more can combine their shares to reconstruct the secret whereas any $k - 1$ or fewer get no information. The basic VCS model has been extended by different researchers including Ateniese et al. [5], Tzeng and Hu [6] and so on. In [5], authors have analyzed the structure of VCS and provided an efficient technique for realizing different VCSs. It is shown that this construction is better with the pixel expansion than the one proposed in [1]. Also the graph based access structure for VCS is described in [5], in which a qualified set contains an edge of a given graph corresponding to the participant of the scheme.

The VCS presented in [6] has in some cases better pixel expansion than previous results. Also the authors proposed an improved VCS based on the fact that human visual system cares about the contrast only and thus, it is not necessary that the recovered image must be always darker than background as in those works followed by Naor and Shamir's VCS model. There are other works on VCS that contribute to the improvement of the contrast of the recovered image. Hofmeister et al. in [7] proposed a VCS for *k-out-of-n* threshold access structure that achieves the best contrast by solving a simple linear problem. Droste proposed a very general method to construct an extended VCS for an arbitrary access structure, however, the scheme is not necessarily monotonic [8]. The access structure of negative images is developed by Kim et al. [9]. The VCSs for color images are proposed in [10–12]. The current work describes and analyzes three existing VCS models and explains their tangible features. In addition, a new design paradigm for $k = 2$ and 3 VCS is proposed that generates and implements participants' shares using combination rule $C(m, w)$, where w is number of 1 s in a share having size m known as pixel expansion value.

The rest of the paper is organized as follows. Three important VCSs including their models are presented in Sect. 2. In Sect. 3, the proposed VCS designs and their implementation are described. A simulation result carried out on a sample binary image is given in this section. Finally, the concluding remarks are given in Sect. 4.

2 Preliminaries of Three VCS Models for Binary Images

There are several important VCS models available in the literature, however, three of them including the scheme proposed by Naor et al. [1] are presented in this section.

2.1 VCS Model Proposed by Naor and Shamir [1]

In [1], an input binary image is encrypted using VCS and distributed among a set of $n > 1$ participants $P = \{1, 2 \ldots n\}$. For this, two basis matrices of order $n \times m$ with *0* and *1* pixels are taken and each input pixel after VCS encryption appears in n shares as a collection of m white and black pixels. A *k-out-of-n* VCS consists of two collections of $n \times m$ Boolean matrices (C_i for $i = 1$ or *2*) generated from basis matrices and one from each is chosen in generating the shares. In VCS, the following three conditions are to be satisfied, where *H(V)* is the Hamming-weight of m-vector V obtained by logical *OR*-ing of k rows of a matrix selected from C_i:

1. For $S_0 \in C_0$, any k of n rows satisfies $H(V) \leq d - \beta$, where $1 \leq d \leq m$ and $\beta = \alpha(m) \times m$, called image contrast ($\alpha(m)$ is the relative difference and $\alpha(m) = (H(V)$ *for* $S_1 - H(V)$ *for* $S_0)/m$).
2. For $S_1 \in C_1$, any k of n rows satisfies $H(V) \geq d$.
3. For any subset $\{i_1, i_2 \ldots i_q\}$ with $q < k$, two collections of $q \times m$ matrices obtained by limiting each matrix to rows $i_1, i_2 \ldots i_q$ are indistinguishable.

The conditions 1 and 2 are called *image contrast* while the condition 3 defines *VCS security*. In fact, no one by stacking fewer than k shares and even with endless computation get any benefit in deciding whether the shared pixel was black or white.

2.2 VCS Model Proposed by Ateniese et al. [5]

An optimal VCS model proposed in [5] is briefly described. For given qualified (Γ_{Qual}) and forbidden (Γ_{Forb}) sets, a *(Γ_{Qual}, Γ_{Forb}, m)-VCS* with a set of threshold $\{(X, t_X)\}_{X \in \Gamma_{Qual}}$ is realized using two $n \times m$ basis matrices B_0 and B_1 if two conditions given below are satisfied:

1. *Construction condition:* Any subset $X = \{i_1, i_2, \ldots, i_p\} \in \Gamma_{Qual}$ can recover the secret image by combining their shares. That is, for any matrix $M \in C_0$, $H(V)$ of $i_1, i_2, \ldots, i_p$ satisfies $H(V) \leq t_X - \beta$, whereas for $M \in C_1$, $H(V) \geq t_X$., where t_X is the threshold used to identify the reconstructed pixels as black or white.

2. *Security condition:* Any subset $X = \{i_1, i_2, \ldots, i_p\} \in \Gamma_{Forb}$ has no information of secret. That is, two matrices of size $p \times m$ obtained by limiting each $n \times m$ matrix, are indistinguishable.

This model incorporates and satisfies all the characteristics defined in VCS proposed in [1], and provides a systematic formal presentation. It's a generalization of VCS as each set $X \in \Gamma_{Qual}$ is possibly associated with a different threshold t_X. Also the access structure of [5] is not as strong as presented in [1].

2.3 VCS Model Proposed by Tzeng and Hu [6]

An efficient VCS with different features is proposed in [6], where a new access structure for VCS is provided. An access structure $\Gamma = (P, Q, F)$ with $Q \cap F = \varnothing$ is presented in [6], where Q and F are respectively qualified and forbidden sets of participants P. Here Q is monotonically increasing if $X \in Q$ implies for all $X' \supseteq X$, $X' \in Q$ and F is monotonically decreasing if $X \in F$ implies for all $X' \subseteq X$, $X' \in F$. Two collections C_0 and C_1 of $n \times m$ Boolean matrices constitute a visual cryptography scheme if there exist value $\alpha(m) > 0$ and a set $\{(X, t_X)\}$ $X \in Q$ satisfying:

1. Any set $X = \{i_1, i_2 \ldots i_q\} \in Q$ can recover the secret image by combining their shares. That is, for any $M \in C_0$, $w(M, X) = t_X$ and any $M' \in C_1$, $w(M', X) \geq t_X + \alpha(m) \times m$ or $M' \in C_1$, $w(M', X) \leq t_X - \alpha(m) \times m$, where $w(M, X) = H(V)$.
2. Any set $X = \{i_1, i_2 \ldots i_q\} \in F$ contains no information of secret. That is, two matrices of size $q \times m$ obtained by limiting each $n \times m$ matrix such that
   (a) If X is not a qualified set in Q, are indistinguishable.
   (b) If X is a qualified set in Q, the collections obtained by *OR*-ing all rows of each $q \times m$ matrix are indistinguishable.

Here, the scheme changes image contrast as the revealed images become darker or lighter than the background if *condition*-1 is satisfied. Note that the revealed images in [5] are always darker than background. VCS model in [6] is non-monotonic in nature.

3 Proposed VCS Model

A new VCS design for hiding image visibility is proposed. It considers $C(m, w)$ combinations to generate binary strings of length m with w number of 1's for $1 \leq w < m$, and uses them to represent participants' shares. These strings are

suitable as each share in VCS is encoded using an m-length equal weight binary string.Two basis matrices used for designing 2-*out-of*-3 VCS in [1] as

$$B_0 = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix} \quad B_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Three shares are generated for three participants, where each input pixel is expanded by three subpixels ($m = 3$). Since each row of the matrices has weight $w = 1$, the basis matrices can be simply generated using $C(3, 1)$. For smaller n, a generalization for 2-*out-of-n* VCS is proposed, where the following basis matrices are used [1]:

$$B_0 = \begin{pmatrix} 100 & \cdots & 0 \\ 100 & & 0 \\ \vdots & \ddots & \vdots \\ 100 & \cdots & 0 \end{pmatrix} \quad B_1 = \begin{pmatrix} 100 & \cdots & 0 \\ 010 & & 0 \\ \vdots & \ddots & \vdots \\ 000 & \cdots & 1 \end{pmatrix}$$

The design of 2-*out-of-n* VCS in [1] is not efficient for two reasons—(i) a unique encryption pattern (using binary string of weight 1) for generating shares is followed and (ii) size of basis matrices become large for large n. This paper proposes an efficient design for 2-*out-of-n* VCS, which is described below in Sect. 3.1.

3.1 Design of 2-out-of-n *Threshold VCS*

The design of *2-out-of-n* VCS in [1] that uses n-length binary strings of $w = 1$, can be generalized as

$$B_0 = (n \textit{ repetitions of a string} \in C(n, 1)) B_1 = (\textit{all strings} \in C(n, 1))$$

Since $C(n, 1) = n$, this scheme has a limitation that the number of participants can never be increased more than n. However, if w is increased ($n/2 \geq w > 1$), the value of $C(n, w)$ becomes greater than n. Thus, the following three improvements over the scheme in [1] can be made if $C(m, w)$ is used:

1. Increase number of participants without increasing the size of basis matrices
2. Support multiple implementations for a given threshold VCS (m remains smaller, enhances image contrast)
3. Contrast of the revealed images can be increased (β increases for some of the qualified subsets)

For instance, the design of 2-*out-of*-4 VCS in addition to using $C(4, 1) = 4$, can also be done by using $C(4, 2) = 6$ and thus, six participants instead of four could be involved without increasing matrix-size. After reconstruction, the image contrast

becomes $\beta = 1$ or 2 whereas $\beta = 1$ in [1]. The proposed VCS for 2-*out-of-n* VCS can be generalized as

1. Adjust pixel expansion parameter m and string-weight w such that the number of combinations in $C(m, w)$ is equal to n, i.e. $C(m, w) = n$, where $1 \leq w < m$.
2. Out of multiple designs, select one having lesser m and higher β values.

An alternative design for 2-*out-of*-3 VCS can be done by considering $m = 3$ and $w = 2$, where the following basis matrices are taken:

$$B_0 = (3\ repetitions\ of\ a\ string \in C(3,2)) B_1 = (all\ strings \in C(3,2))$$

That is, $B_0 = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 0 \end{pmatrix}$ $B_1 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}$

Its simulation results are shown in Fig. 1.

For $m = 4$ and $w = 2$, we have $C(4, 2) = 6$ combinations as 1100, 0110, 0011, 1001, 1010 and *0101*. One way of designing the basis matrices is

$$B_0 = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix} \quad B_1 = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$

Or, $B_0 = (6\ repetitions\ of\ a\ string \in C(4,2))\ B_1 = (all\ 6\ strings \in C(4,2))$

Here, $t_X = 3$ or 4 for $X \in Q$, relative difference and contrast are $\alpha(m) = 1/4$ or 1/2 and $\beta = 1$ or 2, respectively. Thus, the qualified subset $\{1, 3\}$ with $t_{\{1,\ 3\}} = 4$ reconstructs images with better contrast than the subset $\{1, 2\}$ having $t_{\{1,\ 3\}} = 3$. Also our scheme requires 6×4 basis matrices than 6×6 as in [1]. Although the design has similarity to the scheme in [5], the approach is different.

Our scheme for 2-*out-of-n* VCS is better than the scheme presented in [1] as the values of n and m could be reduced. Also it has been found that the proposed

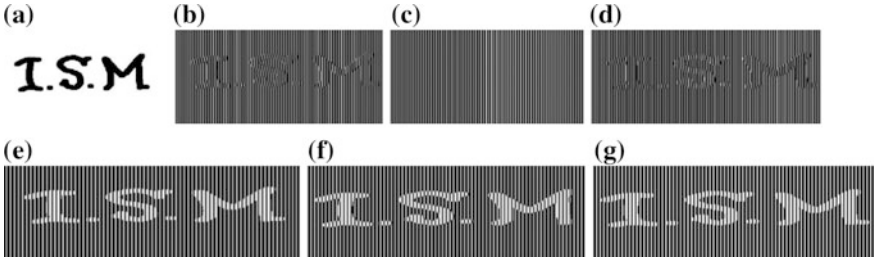

Fig. 1 Results for *2-out-of-3* VCS **a** Input image **b** Share s_1 **c** Share s_2 **d** Share s_3 **e** Combination of s_1 and s_2 **f** Combination of s_2 and s_3 **g** Combination of s_3 and s_1

Table 1 Comparison of proposed *2-out-of-n* threshold VCS with [1]

m	Values of r	Number of participants, $n = \binom{m}{r}$	Basis matrix-size in proposed scheme	Basis matrix-size in [1]	Improvement in bits over [1]
4	1, 3	4	4 × 4	4 × 4	Nil
	2	5–6	5 × 4 – 6 × 4	5 × 5 – 6 × 6	10–24
5	1, 4	5	5 × 5	5 × 5	Nil
	2, 3	6–10	6 × 5 – 10 × 5	6 × 6 – 10 × 10	12–100
6	1, 5	6	6 × 6	6 × 6	Nil
	2, 4	7–15	7 × 6 – 15 × 6	7 × 7 – 15 × 15	14–270
	3	7–20	7 × 6 – 20 × 6	7 × 6 – 20 × 20	14–560
…	…	…	…	…	…
10	1, 9	10	10 × 10	10 × 10	Nil
	2, 8	11–45	11 × 10 – 45 × 10	11 × 11 – 45 × 45	22–3150
	3, 7	11–120	11 × 10 – 120 × 10	11 × 11 – 120 × 120	22–26400
	4, 6	11–210	11 × 10 – 210 × 10	11 × 11 – 210 × 210	22–84000
	5	11–252	11 × 10 – 252 × 10	11 × 11 – 252 × 252	22–121968

scheme requires *2n(n-m)* bits lesser than in [1]. A comparison of the proposed 2-*out-of-n* VCS with the scheme presented in [1] for $m = 4, 5, 6$ *and* 10 is given in Table 1, where $1 \leq w \leq m\text{-}1$.

3.2 *Design* 3-out-of-n *Threshold VCS*

In this section, VCS design for *3-out-of-n* using *C(m, w)* is discussed and compared with Naor and Shamir's scheme [1]. The design in [1] is briefly presented. Consider two binary matrices C and I of order $n \times (n–2)$ and $n \times n$ respectively, where C contains all 1's and I is an identity matrix. Their concatenation $B||I$ becomes a matrix of order $n \times 2n - 2$. The basis matrices for *3-out-of-n* are $B_0 = \left(\overline{C||I}\right)$ and $B_1 = (C||I)$, where $\left(\overline{C||I}\right)$ is the complementation of $C||I$. For illustration, the basis matrices of *3-out-of-4* VCS are as follows:

$$B_0 = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix} \quad B_1 = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Note that the size of the basis matrices for *3-out-of-n* VCS is increased rapidly, which would be infeasible for practical applications. Our design procedure based on *C(n, w)* is better than it. Before presenting the proposed scheme, an illustration is given. The design of 3-*out-of*-3 VCS could be done using (0)‖*C*(3, 2) and *C*(4, 2) for B_0 and B_1 respectively, where (0) is a zero column matrix i.e.,

$$B_0 = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} || C(3,2) = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix} \quad B_1 = C(4,2) = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix}$$

It is identical to the design presented in [1]. Although similar design for any 3-*out-of-n* ($n > 3$) using *C(n, w)* exist, it supports the access structure (not strong) presented in [5]. For instance, the design of 3-*out-of-4* VCS using (0)‖ *C*(4, 3) and *C*(5, 3) basis matrices B_0 and B_1 respectively, would be feasible. Here B_0 is fixed, however, B_1 has multiple options as out of *C(5, 3)* = 10, four are taken. A simple design procedure for B_1 is—(i) one of five columns contains all 1*s* and the remaining four columns must contain exactly two 0*s*. The design is shown below:

$$B_0 = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \end{pmatrix} \quad B_1 = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 \end{pmatrix}$$

Here, each of the basis matrices has size 4 × 5, which requires lesser pixel expansion ($m = 5$) than 4 × 6 ($m = 6$) as in [1]. The qualified set is $Q = \{\{3\text{-}out\text{-}of\text{-}4\}, \{1, 4\}, \{2, 3\}\}$. Some other designs for 3-*out-of-n* and comparison with [1] are shown in Table 2.

Table 2 Comparison of proposed *3-out-of-n* threshold VCS with [1]

3-out-of-n VCS	Proposed scheme			Matrix size in [1]	Improvement in bits
	B_0Matrix	B_1Matrix	Matrix Size		
3-out-of-3	(0) ‖ C(3, 2)	C(4, 2)	3 × 4	3 × 4	Nil
3-out-of-4	(0) ‖ C(4, 3)	C(5, 3)	4 × 5	4 × 6	4
3-out-of-5	(0) ‖ C(5, 4)	C(6, 4)	5 × 6	5 × 8	10
3-out-of-6	(0) ‖ C(6, 5)	C(7, 5)	6 × 7	6 × 10	18
…	…	…	…	…	…
3-out-of-10	(0) ‖ C(10, 9)	C(11, 9)	10 × 11	10 × 18	70

4 Conclusions

A new VCS design based on *C(m, w)* framework for $k = 2, 3$ is presented. Our scheme for 2-*out-of-n* is far better than the VCS presented by Naor and Shamir, however, 3-*out-of-n* VCS although better than [1], supports access structure similar to one presented in [5]. A comparative study with [1] and a sample simulation are provided that are found to be satisfactory.

References

1. M. Naor, A. Shamir, Visual cryptography, in *Proceedings of Eurocrypt 94*, LNCS 950 (Springer, 1994), pp. 1–12
2. J. Daemen, V. Rijmen, Rijndael: the advanced encryption standard. Fr. Dobb's J. (2001)
3. M. Bellare, A. Boldyreva, S. Micali, Public-key encryption in multiuser setting: security proofs and improvements, in *Advances in Cryptology-Eurocrypt-2000* (2000)
4. Cox et al., *Digital Water Marking* (Morgan Kaufmann Publishers, 2000)
5. G. Ateniese, C. Blundo, A. De Santis, D.R. Stinson, Visual cryptography for general access structure. J. Inf. Comput. **129**(2), 86–106 (1996)
6. W.G. Tzeng, C.M. Hu, A new approach for visual cryptography. J Des. Codes Crypt. **27**, 707–727 (2002)
7. Hofmeister et al., Contrast-Optimal *k-out-of-n* Secret Sharing Schemes in Visual cryptograph COCOON 97, LNCS, vol. 1276 (1997)
8. S. Droste, New results on visual cryptography, in *Proceedings of Advances in Cryptology-CRYPTO 96*, LNCS, vol. 1109 (1996), pp. 401–415
9. K. Kim et al., Human-machine identification using visual cryptography, in *Proceedings of IEEE International Workshop on Intelligent Signal Processing and Communication Systems* (1998), pp. 178–182
10. D. Naccache, Colorful cryptography—a purely physical secret-sharing scheme based on chromatic filters, in *Coding and Information Integrity, French-Israeli Workshop* (1994)
11. V. Rijmen, B. Preneel, Efficient colour visual encryption or shared colors of Benetton, in *UROCRYPT 96* (1996)
12. Y.C. Hou, Visual cryptography for color images. Pattern Recognit. **36**, 1619–1629 (2003)