A new $(2, n)-$ visual threshold scheme for color images

Avishek Adhikari[1] and Somnath Sikdar[2]

[1] Applied Statistics Unit, Indian Statistical Institute,
203, B T Road, Calcutta 700 035, INDIA
avishek_r@isical.ac.in
[2] Department email@imsc.res.in

Abstract. In this paper we propose a new scheme for a $(2, n)$-visual threshold scheme (VTS) for color images. Our scheme achieves a better color ratio than the schemes proposed by Koga *et al* in 1998 and 2001. The pixel expansion of our scheme is reasonably good and we also give a lower bound on the color ratio of our scheme.

Keywords : secret sharing scheme, visual secret sharing scheme, visual cryptography.

1 Introduction

Visual cryptography was introduced by Naor and Shamir [9]. It is a new cryptographic paradigm that enables a secret image to be split into n shares, each share being printed on a transparency. The shares are distributed among n participants of whom only some are qualified to recover the original image. The secret image is reconstructed by stacking a certain number k $(2 \leq k \leq n)$ of these transparencies from the set of qualified participants. If fewer than k transparencies are superimposed, then it is impossible to decode the original image. The resulting cryptographic scheme is called a $(k, n)-$visual threshold scheme (VTS). Since the reconstruction is done by the human visual system, no computations are involved during decoding unlike traditional cryptographic schemes where a fair amount of computation is needed to reconstruct the plain text.

The schemes proposed by Naor and Shamir [9] involved black and white images. Further research [4], [6], [7], [8] extended the idea to gray-scale and color images. There are several efficient ways to encrypt black and white images but gray-scale and color images present problems. Color images are specially difficult to encrypt because of two reasons. Firstly, there seems to be no way of encrypting a color image using a reasonably small pixel expansion (a scheme has pixel expansion m if each pixel of the original image is encoded as m subpixels on each transparency) .

The second problem with encrypting color images relates to the brightness of colors in the reconstructed image. In all the schemes proposed on color visual cryptography so far, [6], [8], the brightness of the reconstructed image is poor.

This is because, on stacking the requisite number of transparencies, the number of subpixels that have the color of the original encoded pixel is very small compared to the total number of subpixels. Since, the ratio

$$\frac{\text{number of subpixels that possess the true color}}{\text{the total number of subpixels}} \tag{1}$$

influences the brightness of the reconstructed image, it deserves a separate definition.

Definition 1. *Let the (i,j)th pixel of the secret image have color c and suppose that we are working in a $(k,n)-$VTS for color images. The* **color ratio** *of the (i,j)th pixel in the reconstructed image is the ratio (1) above, when k transparencies from qualified participants are stacked together.*

It is conceivable that the encryption strategy is such that the color ratios of the different pixels in the reconstructed image are different. In this case,we could define the color ratio of a scheme to be the minimum value of the ratio defined in (1), the minimum being taken over all possible different colored pixels. On the other hand, the encryption strategy could be so regular that each pixel, irrespective of its color, has the same color ratio. In this case, we need not define the color ratio separately for each pixel of the reconstructed image. In such a case, if the color ratio of each pixel is R, we will say that the encoding scheme attains a color ratio R.

Koga *et al* ([8]) have proposed a construction of an $(n,n)-$VTS with colors $\{c_1, c_2, \ldots, c_k\}$. Their construction is defined over a bounded upper semilattice. From the basis matrices of a $(t,t)-$VTS for color images, they have constructed basis matrices of a $(t,n)-$VTS for color images. The disadvantage of their scheme is that when the number of shares (and also the number of colors) increases, the pixel expansion shoots up; the color ratio decreases correspondingly. Since their scheme has no positive lower bound on the color ratio, the reconstructed image becomes progressively darker as the number of shares increases.

In this paper, we propose a new scheme for a $(2,n)-$VTS for color images. Our scheme has the following advantages:

1. Our scheme provides a lower bound on the color ratio. For instance, if the secret image is composed of the colors cyan, yellow and green, then the color ratio of our scheme is lower bounded by $1/4$. This lower bound depends only on the number of colors in the secret image and is *independent* of the number of shares. Other schemes dealing with color images can provide no such lower bound ([6], [8]).
2. The color ratio of our scheme is very high compared to what other schemes provide. The result is that our images are brighter. If the secret image has the colors $\mathcal{C} = \{c_1, c_2, \ldots, c_k\}$ such that no two colors c_i and $c_j \in \mathcal{C}$ can be combined to produce a third color $c_l \in \mathcal{C}$, then the color ratio of our scheme is lower bounded by $1/2k$. Compare this with the color ratio $2/k \cdot n(n-1)$, which is what the scheme proposed by Koga ([6]) achieves. The scheme proposed by Koga in 2001, ([8]), achieves a color ratio of $2/kn$!

3. The pixel expansion of our scheme is reasonably good. If the secret image consists of colors cyan, yellow and green, then the pixel expansion is $4m$ where $m = \binom{n}{\lfloor n/2 \rfloor}$. In case, the secret image is composed of the colors red, green, blue, cyan, magenta and green, the pixel expansion is $6m$. Compare this with the pixel expansion given in [8], which for these same two color sets is $2n!$ and $3n!$ respectively. It can be easily seen that: $2n! > 4m \ , and \ 3n! > 6m \ , \ for \ n > 3$

This paper is organized as follows. Section 2 deals with some of the definitions and results on visual cryptography that we have made use of in this paper. In section 3, we construct a $(2, n)-$color VTS with three base colors. Finally, in section 4 we show how to construct a $(2, n)-$color VTS with six base colors. We also show how our scheme can be extended to an arbitrary number of colors.

2 Preliminaries

2.1 The Model

The model that we describe here is taken nearly verbatim from Blundo, De Santis, and Stinson [3]. Let $\mathcal{P} = \{1, \ldots, n\}$ be a set of elements called *participants*, and let $2^{\mathcal{P}}$ denote the set of all subsets of $\mathcal{P}$. Let Γ_{Qual} and Γ_{Forb} be subsets of $2^{\mathcal{P}}$, where $\Gamma_{Qual} \cap \Gamma_{Forb} = \emptyset$. We will refer to members of Γ_{Qual} as *qualified sets* and the members of Γ_{Forb} as *forbidden sets*. The pair $(\Gamma_{Qual}, \Gamma_{Forb})$ is called the *access structure* of the scheme.

We assume that the secret image consists of a collection of black and white pixels, each pixel being encrypted separately. To understand the encryption process consider the case where the secret image consists of just a single black or white pixel. On encryption, this pixel appears in the n shares distributed to the participants. However, in each share the pixel is subdivided into m *subpixels* (m is the pixel expansion), each of which is either black or white. It is important to note that the shares are printed on transparencies, and that a "white" subpixel is actually an area where nothing is printed, and therefore left transparent. We assume that the subpixels are sufficiently small and close enough so that the eye averages them to some shade of grey. We can represent this with an $n \times m$ boolean matrix $S[i, j]$, where $S[i, j] = 1$ if and only if the jth subpixel in the ith share is black. When the shares are stacked together, the perceived grey level is proportional to the number of 1's in the boolean OR of the $m-$vectors representing the shares of each participant. When the secret image consists of more than one pixel, we encrypt each pixel separately.

We give the following definition of a visual cryptography scheme for a general access structure. The phrasing is taken directly from Atienese, Blundo, De Santis, and Stinson [1]. We use $OR\ V$ to denote the boolean operation OR of a set of vectors with result V. The *Hamming weight* $w(V)$ is the number of 1's in the boolean vector V.

Definition 2. *Let* $(\Gamma_{Qual}, \Gamma_{Forb})$ *be an access structure on a set of* n *participants. Two collections (multisets) of* $n \times m$ *Boolean matrices* C_0 *and* C_1 *constitute a visual cryptography scheme* $(\Gamma_{Qual}, \Gamma_{Forb}, m)-VCS$ *if there exists values* $\alpha(m)$ *and* $\{t_X\}_{X \in \Gamma_{Qual}}$ *satisfying:*

1. *Any qualified set* $X = \{i_1, i_2, \ldots, i_p\} \in \Gamma_{Qual}$ *can recover the shared image by stacking their transparencies.*
   Formally, for any $M \in C_0$*, the "or"* V *of rows* $i_1, \ldots, i_p$ *satisfies* $w(V) \leq t_X - \alpha(m) \cdot m$*; whereas, for any* $M \in C_1$ *it results that* $w(V) \geq t_X$*.*
2. *Any forbidden set* $X = \{i_1, i_2, \ldots, i_p\} \in \Gamma_{Forb}$ *has no information on the shared image.*
   Formaly, the two collections of $p \times m$ *matrices* D_t*, with* $t \in \{0, 1\}$*, obtained by restricting each* $n \times m$ *matrix in* C_t *to rows* $i_1, \ldots, i_p$ *are indistinguishable in the sense that they contain the same matrices with the same frequencies.*

In order that the recovered image is clearly discernible, it is important that the grey level of a black pixel be darker than that of a white pixel. Informally, the difference in the grey levels of the two pixel types is called *contrast*. We want the contrast to be as large as possible. Three variables control the perception of black and white regions in the recovered image: a threshold value (t), a relative difference (α), and the pixelexpansion (m). The *threshold value* is a numeric value that represents a grey level that is perceived by the human eye as the color black. The value $\alpha \cdot m$ is the contrast, which we want to be as large as possible. We require that $\alpha \cdot m \geq 1$ to ensure that black and white areas will be distinguishable.

Each pixel of the original image will be encrypted into n pixels, each of which consist of m subpixels. To share a white (resp. black) pixel, the dealer randomly chooses one of the matrices in $\mathcal{C}_0$ (resp. $\mathcal{C}_1$), and distributes row i to participant i. Thus the chosen matrix defines the m subpixels in each of the n transparencies. Note that in the definition above we allow a matrix to appear more than once in $\mathcal{C}_0$ ($\mathcal{C}_1$). Finally, note that the size of the collections $\mathcal{C}_0$ and $\mathcal{C}_1$ need not be the same.

2.2 Basis Matrices

Instead of working with the collections $\mathcal{C}_0$ and $\mathcal{C}_1$, it is convenient (in terms of memory requirements) to consider only two $n \times m$ boolean matrices, S^0 and S^1 called *basis matrices* which satisfy the following definition.

Definition 3. *Let* $(\Gamma_{Qual}, \Gamma_{Forb})$ *be an access structure on a set* $\mathcal{P}$ *of* n *participants. A* $(\Gamma_{Qual}, \Gamma_{Forb}, m)$*-VCS with relative difference* $\alpha(m)$ *and a set of thresholds* $\{t_X\}_{X \in \Gamma_{Qual}}$ *is realized using the* $n \times m$ *basis matrices* S^0 *and* S^1 *if the following two conditions hold:*

1. *If* $X = \{i_1, i_2, \ldots, i_p\} \in \Gamma_{Qual}$*, then the OR* V *of the rows* $i_1, i_2, \ldots, i_p$ *of* S^0 *satisfies* $w(V) \leq t_X - \alpha(m) \cdot m$*; whereas, for* S^1 *it results that* $w(V) \geq t_X$*.*
2. *If* $X = \{i_1, i_2, \ldots, i_p\} \in \Gamma_{Forb}$*, the two* $p \times m$ *matrices obtained by restricting* S^0 *and* S^1 *to rows* $i_1, i_2, \ldots, i_p$ *are equal up to a column permutation.*

The collections $\mathcal{C}_0$ and $\mathcal{C}_1$ are obtained by permuting the columns of the corresponding basis matrix (S^0 for $\mathcal{C}_0$ and S^1 for $\mathcal{C}_1$) in all possible ways. Note that, in this case, the sizes of the collections $\mathcal{C}_0$ and $\mathcal{C}_1$ are the same.

2.3 Share Distribution Algorithm

Now that we will be working with the basis matrices S^0 and S^1, we need to modify the encryption process slightly as described below.

For each pixel P, do the following:

1. Generate a random permutation π of the set $\{1, 2, \ldots, m\}$.
2. If P is a black pixel, then apply π to the columns of S^0; else apply π to the columns of S^1. Call the resulting matrix T.
3. For $1 \leq i \leq n$, row i of T comprises the m subpixels of P in the ith share.

2.4 Threshold Schemes

A $(k, n)-$threshold structure is any access structure $(\Gamma_{Qual}, \Gamma_{Forb})$ in which $\Gamma_0 = \{B \subseteq \mathcal{P} : |B| = k\}$ and $\Gamma_{Forb} = \{B \subseteq \mathcal{P} : |B| \leq k-1\}$. In any $(k, n)-$threshold VCS, the image is visible if any k of the n participants stack their transparencies, but totally invisible if fewer than k transparencies are stacked together or analyzed by any other method. In a strong $(k, n)-$threshold VCS, the image remains visible if more than k participants stack their transparencies.

2.5 A $(2, n)-$threshold VCS with optimal contrast

We now present a $(2, n)-$threshold VCS due to Blundo, De Santis, and Stinson [3] in which the relative difference is optimal.

The $n \times m$ basis matrices S^0 and S^1 are constructed as follows: The columns of S^1 consist of all binary $n-$vectors of weight $\lfloor n/2 \rfloor$. Hence, $m = \binom{n}{\lfloor n/2 \rfloor}$ and any row in S^1 has weight equal to $\binom{n-1}{\lfloor n/2 \rfloor - 1}$. S^0 is constructed from n identical row vectors of length m, and of weight $\binom{n-1}{\lfloor n/2 \rfloor - 1}$.

Theorem 1. *Let $n \geq 2$. In any $(2, n)-$threshold visual cryptography scheme with pixel expansion $m = \binom{n}{\lfloor n/2 \rfloor}$, it holds that $\alpha(m) \leq \alpha^*(n) = \lfloor n/2 \rfloor \lceil n/2 \rceil / n(n-1)$.*

Theorem 2. *For any $n \geq 2$, there exists a strong $(2, n)-$threshold visual cryptography scheme with pixel expansion $m = \binom{n}{\lfloor n/2 \rfloor}$ and $\alpha(m) = \alpha^*(n)$.*

2.6 Lattice-based color VTS

In this section we present constructions for lattice based visual cryptography schemes for color images due to Koga *et al* [6–8].We begin with a few definitions.

A poset $(L, \leq)$ is called a *lattice* if for all $a, b \in L$, the set $\{a, b\}$ has both a l.u.b and a g.l.b. A poset $(L, \leq)$ is called an *upper semi-lattice* if for all $a, b \in L$ the set $\{a, b\}$ has a l.u.b. If $(L, \leq)$ is an upper semi-lattice then the *join* (denoted by $\sqcup$) of L is a binary operation on L defined as follows: For $x, y \in L$, $x \sqcup y =$ least upper bound of $\{x, y\}$. An upper semi-lattice is said to be *bounded* if it contains the least element 0 and the greatest element 1 such that $x \sqcup 0 = x$ and $x \sqcup 1 = 1$ for all $x \in L$.

Let L be a bounded upper semi-lattice of colors and let $m \geq 2$ be an integer. Define $\mathcal{C} = \{c_1, \ldots, c_K\} \subseteq L$ to be the set of colors that the secret image contains. This subset need not be a sublattice of L. Let $\mathcal{P}$ be a set of n participants. We can view an element of $(L^m)^n$ as an $n \times m$ matrix S whose entries are elements of L. For $1 \leq p \leq n$ and $A = \{i_1, \ldots, i_p\} \subseteq \mathcal{P}$ define $S[A]$ to be the $p \times m$ matrix obtained by restricting S to rows $i_1, \ldots, i_p$. For such a p and A define the mapping $h : (L^m)^n \rightarrow L^m$ as $h(S[A]) = \bar{s}_{i_1} \sqcup_m \bar{s}_{i_2} \sqcup_m \ldots \sqcup_m \bar{s}_{i_p}$ where $\bar{s}_{i_j}$ denotes the i_j-th row of matrix S and $\sqcup_m$ denotes the join of L^m defined previously. Note that h describes the physical operation of stacking the shares of the i_1th$, \ldots, i_p$th participants.

A lattice-based visual cryptography scheme for an access structure Γ is defined as follows:

Definition 4. *Let $\Gamma = (\Gamma_{Qual}, \Gamma_{Forb})$ be an access structure on a set $\mathcal{P}$ of participants. Let L be a bounded upper semi-lattice of colors and $\mathcal{C} = \{c_1, \ldots, c_K\}$ a subset of L. Let $\mathcal{X}_{c_i}$ $(1 \leq i \leq K)$ denote a collection of $n \times m$ matrices with elements from L. The set $\{\mathcal{X}_{c_i}\}_{i=1}^K$ is called a lattice-based visual cryptography scheme for the access structure Γ with colors $\mathcal{C}$ and pixel expansion m if the following two properties hold:*

1. *For each $1 \leq i \leq K$, if $A \in \Gamma^*_{Qual}$ and $S \in \mathcal{X}_{c_i}$, then $h(S[A]) \in L^m$ contains only 1s and at least one c_i. Γ^*_{Qual} is a minimum qualified set of Γ_{Qual}.*
2. *If $A \in \Gamma^*_{Forb}$, then the sets $\mathcal{X}_{c_i}[A]$ $(1 \leq i \leq K)$ are indistinguishable in the sense that they contain the same elements with the same frequencies. $\mathcal{X}_{c_i}[A]$ is defined as $\mathcal{X}_{c_i}[A] = \{S[A] : S \in \mathcal{X}_{c_i}\}$. Γ^*_{Forb} refers to the maximal forbidden sets of Γ_{Forb}.*

2.7 (2,n)-Lattice-based VTS

Before we describe the construction, let us set up our notation. For $j = 1, 2, \ldots, n$, define $M_{n,n-j}(x)$ as the matrix obtained by permuting a column containing one x, $n - j$ 0's, and $j - 1$ 1's in all possible ways.

If M is a matrix and $\alpha \geq 1$ an integer, $M^{[\alpha]}$ denotes the matrix obtained by concatenating M with itself α times i.e $M^{[\alpha]} = \underbrace{M \circ M \circ \ldots \circ M}_{\alpha \text{ times}}$.

In the paper [6] if the color set is $\mathcal{C} = \{c_1, \ldots, c_K\}$, the basis matrices S_{c_i} ($c_i \in \{c_1, \ldots, c_K\}$) are defined as follows: $S_{c_i} = A(c_i) \circ D(c_1) \circ \ldots \circ D(c_{i-1}) \circ D(c_{i+1}) \circ \ldots \circ D(c_K)$ where $A(x) = M_{n,1}(x)$ and $D(x) = M_{n,0}^{[n-1]}(x)$. Here the pixel expansion is $kn(n-1)$ and the color ratio is $2/kn(n-1)$.

In the paper [8] ,they first construct the basis matrices for $(2,2)$-color VTS. If the color set is $\mathcal{C} = \{c_1, \ldots, c_K\}$,then the basis matrices X_{c_i} ($c_i \in \{c_1, \ldots, c_K\}$) of $(2,2)$-color VTS are defined as follows: $X_{c_i} = A(c_i) \circ D(c_1) \circ \ldots \circ D(c_{i-1}) \circ D(c_{i+1}) \circ \ldots \circ D(c_K)$ where $A(X) = M_2(X, 0)$ and $D(X) = M_2(X, 1)$ and $M_n(a_1, \ldots, a_n)$ is an $n \times n!$ matrix consisting of all permutations of the vector $(a_1, \ldots, a_n)^t$. To construct the basis matrices S_{c_i} of a $(2,n)$-color VTS with a set of colors $\mathcal{C} = \{c_1, \ldots, c_K\}$,they just replace $M_2(X, Y)$ of X_{c_i} by $M_n(X, Y, 1, \ldots, 1)$. So they have pixel expansion $kn!$ and color ratio $2/kn!$.

3 A new construction of a $(2, n)-$color VTS with three base colors

Before we describe our scheme, we define what we mean by a color visual threshold scheme.

Definition 5. *Let us suppose we can generate all the colors in the secret image using the color set $\mathcal{C} = \{c_1, c_2, \ldots, c_J\}$. A set of J $n \times m$ matrices G_i with entries from the set $\{0, 1, c_1, c_2, \ldots, c_J\}$ form a (k, n) visual threshold scheme if the following properties are satisfied:*

1. *For any i, ($1 \leq i \leq J$), the $m-$vector obtained by "superimposing" any k rows of G_i has at least L_i entries which are c_i; each of the remaining colors c_j appear at most U_i^j times in this $m-$vector.*
2. *For any subset $\{i_1, i_2, \ldots, i_j\} \subset \{1, \ldots, n\}$, the submatrices G_i' obtained by restricting each G_i to the rows $i_1, \ldots, i_j$ are identical up to a column permutation.*

Here the L_i's signify lower bounds and the U_i^j's signify upper bounds. The true color c_i must appear at least L_i times when two shares for a pixel of color c_i are combined; other colors c_j may appear on superimposing two arbitrary shares for c_i, but they do so at most U_i^j times. The second property is related to security and it ensures that no set of $k-1$ participants or fewer can decipher the secret image.

suppose that the original image is composed of only three colors, namely Cyan (C), Yellow (Y) and Green (G). We will first construct a $(2,2)-$VTS with the color set $\mathcal{C} = \{C, Y, G\}$. To do this, it is sufficient to construct the basis matrices S_C, S_Y, S_G corresponding to the colors C, Y and G respectively. These basis matrices are given below:
$S_C = \begin{bmatrix} C & 0 & Y & 1 \\ 0 & C & 1 & Y \end{bmatrix}$, $S_Y = \begin{bmatrix} Y & 0 & C & 1 \\ 0 & Y & 1 & C \end{bmatrix}$ *and* $S_G = \begin{bmatrix} C & Y & 1 & 0 \\ Y & C & 0 & 1 \end{bmatrix}$
To construct a $(2,n)-$color VTS ($n \geq 3$) with base colors C, Y, and G, we first consider the basis matrix S^1 of the $(2,n)-$VTS for black and white images as

described in [3]. S^1 is an $n \times m$ Boolean matrix which is realized by considering all binary $n-$vectors of weight $\lfloor n/2 \rfloor$, where $m = \binom{n}{\lfloor n/2 \rfloor}$.

To construct our $(2,n)-$ color VTS ($n \geq 3$), we will use the basis matrices of the (2,2) scheme as templates in the construction of the basis matrices of the $(2,n)$ scheme. From here on, we will denote the basis matrix S_{col} of the (2,2) scheme by X_{col}. Therefore, S_C, S_Y, S_G defined above will be denoted as X_C, X_Y, and X_G respectively. S_C, S_Y and S_G, the basis matrices for the $(2,n)$ scheme, are defined below.

> S_C is an $n \times 4m$ matrix defined in terms of S^1 as follows:
> Replace a 0 in S^1 by the first row of X_C and a 1 in S^1 by the second row of X_C.

S_Y and S_G are constructed in a similar fashion. One can verify that the ith rows ($1 \leq i \leq n$) of the matrices S_C, S_Y and S_G thus obtained are identical up to a column permutation.

3.1 An example of a $(2,4)-$color VTS with base colors C, Y and G

To construct a $(2,4)-$color VTS with base colors C, Y, and G we first look at the basis matrix S^1 of a $(2,4)-$VTS for black and white images. The matrix S^1 is shown below.

$$\begin{bmatrix} 1\,0\,0\,1\,0\,1 \\ 1\,1\,0\,0\,1\,0 \\ 0\,1\,1\,1\,0\,0 \\ 0\,0\,1\,0\,1\,1 \end{bmatrix}.$$

Since $X_C = \begin{bmatrix} C & 0 & Y & 1 \\ 0 & C & 1 & Y \end{bmatrix}$, $X_Y = \begin{bmatrix} Y & 0 & C & 1 \\ 0 & Y & 1 & C \end{bmatrix}$ and $X_G = \begin{bmatrix} C & Y & 1 & 0 \\ Y & C & 0 & 1 \end{bmatrix}$ we have

S_C:

$$\begin{bmatrix} 0 & C & 1 & Y & C & 0 & Y & 1 & C & 0 & Y & 1 & 0 & C & 1 & Y & C & 0 & Y & 1 & 0 & C & 1 & Y \\ 0 & C & 1 & Y & 0 & C & 1 & Y & C & 0 & Y & 1 & C & 0 & Y & 1 & 0 & C & 1 & Y & C & 0 & Y & 1 \\ C & 0 & Y & 1 & 0 & C & 1 & Y & 0 & C & 1 & Y & 0 & C & 1 & Y & C & 0 & Y & 1 & C & 0 & Y & 1 \\ C & 0 & Y & 1 & C & 0 & Y & 1 & 0 & C & 1 & Y & C & 0 & Y & 1 & 0 & C & 1 & Y & 0 & C & 1 & Y \end{bmatrix}$$

S_Y:

$$\begin{bmatrix} 0 & Y & 1 & C & Y & 0 & C & 1 & Y & 0 & C & 1 & 0 & Y & 1 & C & Y & 0 & C & 1 & 0 & Y & 1 & C \\ 0 & Y & 1 & C & 0 & Y & 1 & C & Y & 0 & C & 1 & Y & 0 & C & 1 & 0 & Y & 1 & C & Y & 0 & C & 1 \\ Y & 0 & C & 1 & 0 & Y & 1 & C & 0 & Y & 1 & C & 0 & Y & 1 & C & Y & 0 & C & 1 & Y & 0 & C & 1 \\ Y & 0 & C & 1 & Y & 0 & C & 1 & 0 & Y & 1 & C & Y & 0 & C & 1 & 0 & Y & 1 & C & 0 & Y & 1 & C \end{bmatrix}$$

S_G:

$$\begin{bmatrix} Y & C & 0 & 1 & C & Y & 1 & 0 & C & Y & 1 & 0 & Y & C & 0 & 1 & C & Y & 1 & 0 & Y & C & 0 & 1 \\ Y & C & 0 & 1 & Y & C & 0 & 1 & C & Y & 1 & 0 & C & Y & 1 & 0 & Y & C & 0 & 1 & C & Y & 1 & 0 \\ C & Y & 1 & 0 & Y & C & 0 & 1 & Y & C & 0 & 1 & Y & C & 0 & 1 & C & Y & 1 & 0 & C & Y & 1 & 0 \\ C & Y & 1 & 0 & C & Y & 1 & 0 & Y & C & 0 & 1 & C & Y & 1 & 0 & Y & C & 0 & 1 & Y & C & 0 & 1 \end{bmatrix}$$

Here $R_C = 10/24$, $R_Y = 10/24$ and $R_G = 8/24$. Note that the color ratio of the above scheme is $1/3$.

3.2 Share distribution algorithm

We use the following algorithm to encode the secret image.

For each pixel P in the secret image do the following:

1. Generate a random permutation π of the set $\{1, 2, \ldots, 4m\}$.
2. If P is a cyan pixel, apply π to the columns of S_C. Call the resulting matrix T_C. If P is Y or G, apply π to the columns of the matrices S_Y or S_G respectively to form T_Y or T_G.
3. For $1 \leq i \leq n$, row i of T_X, where $X \in \{C, Y, G\}$, describes the color distribution among the $4m$ subpixels of the ith share.

If $n = 2$, we do the same thing as above by taking $m = 1$.

We next show that the color ratio attained by this encryption scheme is bounded below by $1/4$. To prove this result we need the following lemmas:

Lemma 1. *For any distinct $i, j = 1, 2, \ldots, n$ let $S^1\{i, j\}$ denote the $2 \times m$ matrix obtained by restricting S^1 to rows i and j. Then the submatrix $S^1\{i, j\}$ has equal number of patterns of the forms: $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$ and $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ and this number is equal to $m \cdot \alpha(m)$. Also the total number of patterns of the forms $\begin{bmatrix} 0 \\ 0 \end{bmatrix}$ and $\begin{bmatrix} 1 \\ 1 \end{bmatrix}$ is given by $m - 2 \cdot m \cdot \alpha(m)$. Here $\alpha(m)$ is given by $\alpha(m) = \begin{cases} 1/4 + 1/4(n-1), & \text{if } n \text{ is even} \\ 1/4 + 1/4n, & \text{if } n \text{ is odd} \end{cases}$*

Proof. Choose two distinct rows i and j and suppose that $i < j$. The number of $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ patterns in $S^1\{i, j\}$ is equal to the number of ways of distributing the remaining $\lfloor n/2 \rfloor - 1$ 1's among the remaining $n - 2$ rows. This can be done in $\begin{pmatrix} n-2 \\ \lfloor n/2 \rfloor - 1 \end{pmatrix}$ ways. It so happens that the contrast $\alpha(m) \cdot m$ of the $(2, n)$ scheme of which S^1 is a basis matrix is equal to the above number. By a similar argument, there is an equal number of $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$ patterns in $S^1\{i, j\}$. Since S^1 has m columns, the total number of patterns of the forms $\begin{bmatrix} 0 \\ 0 \end{bmatrix}$ and $\begin{bmatrix} 1 \\ 1 \end{bmatrix}$ must be $m - 2 \cdot m \cdot \alpha(m)$. □

Note. From here on whenever we use the term $\alpha(m)$, we will use it as defined above in Lemma 1. To see how $\alpha(m)$ is obtained, consult reference [3].

Lemma 2. *For each cyan (or yellow) pixel in the original image, the total number of cyan (or yellow) colored subpixels in the image formed by superimposing two arbitrary shares is given by*

$$m[1 + 2 \cdot \alpha(m)].$$

For each green pixel in the original image, the total number of green colored subpixels in the superimposed image is given by $4m \cdot \alpha(m)$.

Proof. Recall that we defined X_C as follows: $X_C = \begin{bmatrix} C & 0 & Y & 1 \\ 0 & C & 1 & Y \end{bmatrix}$. First note that each one of the patterns $\begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ in S^1 contributes two C's in S_C. Each one of the patterns $\begin{bmatrix} 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \end{bmatrix}$ in S^1 contributes one C in S_C. So for each cyan colored pixel in the original image, the total number of cyan colored subpixels in the image obtained by superimposing two arbitrary shares, is given by (by using lemma 1) $2m \cdot \alpha(m) + 2m \cdot \alpha(m) + m - 2m \cdot \alpha(m)$ which simplifies to $m[1 + 2 \cdot \alpha(m)]$ One can verify that this result holds for a yellow pixel also.

Next we will work this out for a green pixel. Recall that we defined X_G as follows $X_G = \begin{bmatrix} C & Y & 1 & 0 \\ Y & C & 0 & 1 \end{bmatrix}$ Note that each one of the patterns $\begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ in S^1 contributes two G's in S_G. The patterns $\begin{bmatrix} 0 \\ 0 \end{bmatrix}$ and $\begin{bmatrix} 1 \\ 1 \end{bmatrix}$ contribute no G's in S_G. Thus for each green pixel in the original image, the total number of green colored subpixels in the superimposed image is given by (by using lemma 1)
$2m \cdot \alpha(m) + 2m \cdot \alpha(m) + 0 + 0 = 4m \cdot \alpha(m)$. □

Now we come to the main theorem.

Theorem 3. *For any* $n \geq 3$*, there exists a* $(2, n)-$*color VTS with base colors Cyan (C), Yellow(Y), and Green (G) with pixel expansion* $4m$ *and color ratios*

$$R_C = \begin{cases} 3/8 + 1/8(n-1), & \text{if } n \text{ is even} \\ 3/8 + 1/8n, & \text{if } n \text{ is odd} \end{cases}$$

$$R_Y = \begin{cases} 3/8 + 1/8(n-1), & \text{if } n \text{ is even} \\ 3/8 + 1/8n, & \text{if } n \text{ is odd} \end{cases}$$

$$R_G = \begin{cases} 1/4 + 1/4(n-1), & \text{if } n \text{ is even} \\ 1/4 + 1/4n, & \text{if } n \text{ is odd} \end{cases}$$

For $n = 2$*, the color ratio of the* $(2, n)-$*color VTS is 1/2 and the pixel expansion is 4.*

Proof. That for $n = 2$, the color ratio is $1/2$ and the pixel expansion is 4 can be seen by examining the basis matrices of the (2,2) scheme.

Therefore, consider the case when $n \geq 3$. The number of columns in each S_X, $X \in \{C, Y, G\}$ is $4m$. To find out the color ratios R_C, R_Y and R_G we need to examine the construction of the basis matrix S^1. The color ratio depends on the patterns $\begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \end{bmatrix}$ that appear in the matrix $S^1\{i, j\}$ for any $i, j = 1, 2, \ldots, n$. Now by using lemma 2, the color ratio R_C is given by

$$R_C = [m \cdot (2 \cdot \alpha(m) + 1)]/4m = 1/4 + \alpha(m)/2$$

From [3] we know that $\alpha(m)$ is given by,

$$\alpha(m) = \begin{cases} 1/4 + 1/4(n-1), & \textit{if } n \textit{ is even} \\ 1/4 + 1/4n, & \textit{if } n \textit{ is odd} \end{cases}$$

Therefore, R_C is given by

$$R_C = \begin{cases} 3/8 + 1/8(n-1), & \textit{if } n \textit{ is even} \\ 3/8 + 1/8n, & \textit{if } n \textit{ is odd} \end{cases}$$

R_Y can be derived in a similar fashion. One can verify that R_Y is given by:

$$R_Y = \begin{cases} 3/8 + 1/8(n-1), & \textit{if } n \textit{ is even} \\ 3/8 + 1/8n, & \textit{if } n \textit{ is odd} \end{cases}$$

The color ratio R_G is given by

$$R_G = 4m \cdot \alpha(m)/4m = \alpha(m) = \begin{cases} 1/4 + 1/4(n-1), & \textit{if } n \textit{ is even} \\ 1/4 + 1/4n, & \textit{if } n \textit{ is odd} \end{cases}$$

$\square$

Observe that each share contains the original base colors C, Y, and G along with white (0) and black (1). If the encoded pixel is colored cyan then on superimposing any two shares, the resulting reconstructed pixel will have the colors cyan, yellow, black, and white. Note that the color yellow is unwanted here, because too many yellow subpixels may fool the visual system into thinking this as a yellow pixel. We will call such unwanted colors *nuisance colors*.

Suppose that the encoded pixel has color c_i, and on superimposing two arbitrary shares, we find some subpixels with color c_j ($c_j \neq$ black, white). Then we define c_j to be a nuisance color for c_i and we denote the *number* of such subpixels in a reconstructed pixel for c_i by $N_{c_i}^{c_j}$. In this case, yellow is a nuisance color for cyan and we denote the number of yellow subpixels in a cyan pixel by N_C^Y. Similarly for a yellow pixel, the nuisance color is cyan and we denote the number of cyan subpixels by N_Y^C. Finally, a green pixel has as nuisance colors both cyan and yellow and we denote their numbers by N_G^C and N_G^Y respectively.

Note that we have not defined white or black as nuisance colors. This is because the presence of white subpixels serve to make the image lighter, but they do not hinder the visual system from discerning the true color of a pixel. Black subpixels darken the image, but again, they do not hinder the visual system from discerning the color of a pixel.

We will next determine the numbers N_C^Y, N_Y^C, N_G^Y, and N_G^C. Note that in the (2,2) color VTS with color set $\{C, Y, G\}$ there are no nuisance colors. Let the encoded pixel be a cyan colored one. When the ith and jth ($1 \leq i < j \leq n$) shares are superimposed, the nuisance color yellow appears due to the patterns $\begin{bmatrix} 0 \\ 0 \end{bmatrix}$ and $\begin{bmatrix} 1 \\ 1 \end{bmatrix}$ in $S^1\{i,j\}$. Each of the above patterns contributes one yellow subpixel in the superimposed image. Recall that the total number of such patterns is given by $m - 2 \cdot m \cdot \alpha(m)$. Hence the number of yellow subpixels N_C^Y for each cyan pixel in the original image is given by

$$N_C^Y = m - 2 \cdot m \cdot \alpha(m) = \begin{cases} m[\frac{1}{2} - \frac{1}{2(n-1)}], & \text{if } n \text{ is even} \\ m[\frac{1}{2} - \frac{1}{2n}], & \text{if } n \text{ is odd} \end{cases}$$

Note that $N_C^Y < m/2$. The pixel expansion, in this case, is $4m$. Out of these $4m$ subpixels, less than $m/2$ subpixels are yellow. That is, less than 1/8th of the subpixels will be nuisance colored. One can show that $N_Y^C = N_C^Y$. Therefore, these observations hold for cyan colored pixels also. For each green pixel in the secret image, the number of cyan and yellow colored subpixels are each less than $m/2$. Hence, $N_G^C + N_G^Y < m$. That is, for each green pixel in the reconstructed image the total number of nuisance colored subpixels $< m$ and the fraction of such subpixels $< m/4m = 1/4$.

Although, the reconstructed image has nuisance colors, they will not affect the quality of the reconstructed image significantly. Nuisance colors do not produce any diminution of brightness, as the overwhelming majority of black subpixels do in [6] and [8].

4 Construction of a $(2, n)-$color VTS with six base colors

Suppose that the original image is made up of exactly six colors namely Red (R), Green (G), Blue (B), Cyan (C), Yellow (Y) and Magenta (M). To construct a $(2, n)-$color VTS with base colors R, G, B, Y, C, and M we first consider the basis matrix S^1 of the $(2, n)-$ VTS for black and white images that was described earlier. Recall that S^1 is an $n \times m$ Boolean matrix which is realized by considering all binary n-vectors of weight $\lfloor n/2 \rfloor$, where $m = \binom{n}{\lfloor n/2 \rfloor}$. Now for each of the six colors we construct a 2×6 matrix as shown below.

$$X_Y = \begin{bmatrix} Y & 0 & C & M & 1 & 1 \\ 0 & Y & 1 & 1 & C & M \end{bmatrix}, X_C = \begin{bmatrix} C & 0 & M & Y & 1 & 1 \\ 0 & C & 1 & 1 & M & Y \end{bmatrix}, X_M = \begin{bmatrix} M & 0 & Y & C & 1 & 1 \\ 0 & M & 1 & 1 & Y & C \end{bmatrix}$$

$$X_R = \begin{bmatrix} Y & M & C & 1 & 1 & 0 \\ M & Y & 1 & C & 0 & 1 \end{bmatrix}, X_G = \begin{bmatrix} Y & C & M & 1 & 1 & 0 \\ C & Y & 1 & M & 0 & 1 \end{bmatrix}, X_B = \begin{bmatrix} M & C & Y & 1 & 1 & 0 \\ C & M & 1 & Y & 0 & 1 \end{bmatrix}$$

Note that C + Y = G, C + M = B and Y + M = R. To construct a $(2, n)-$color VTS it is sufficient to construct the basis matrices S_R, S_G, S_B, S_C, S_Y, and S_M for the colors R, G, B, C, Y, and M respectively. For $n = 2$, we have $S_P = X_P$ where P = C, Y, M, R, G, B. Now we consider our $(2, n)-$color VTS with $n \geq 3$.

We define S_R as an $n \times 6m$ matrix that is constructed as follows:

> Replace each occurrence of a 0 in S^1 by the first row of X_R and that of a 1 by the second row of X_R.

S_G, S_B, S_C, S_Y and S_M are constructed in a similar fashion. Note that the ith rows of the matrices S_R, S_G, S_B, S_C, S_Y, and S_M thus obtained are identical up to a column permutation.

4.1 Share distribution algorithm

The share distribution algorithm is exactly the same as the one given for three colors. The proof is similar to the proof of Theorem 3.

Theorem 4. *For any $n \geq 3$, there exists a $(2, n)-$color VTS with base colors Red (R), Green (G), Blue (B), Cyan (C), Yellow (Y), and Magenta (M) with pixel expansion 6m and color ratios*

$$R_Y = \begin{cases} 1/4 + 1/12(n-1), & \textit{if } n \textit{ is even} \\ 1/4 + 1/12n, & \textit{if } n \textit{ is odd} \end{cases}$$

$$R_C = \begin{cases} 1/4 + 1/12(n-1), & \textit{if } n \textit{ is even} \\ 1/4 + 1/12n, & \textit{if } n \textit{ is odd} \end{cases}$$

$$R_M = \begin{cases} 1/4 + 1/12(n-1), & \textit{if } n \textit{ is even} \\ 1/4 + 1/12n, & \textit{if } n \textit{ is odd} \end{cases}$$

$$R_R = \begin{cases} 1/6 + 1/6(n-1), & \textit{if } n \textit{ is even} \\ 1/6 + 1/6n, & \textit{if } n \textit{ is odd} \end{cases}$$

$$R_G = \begin{cases} 1/6 + 1/6(n-1), & \textit{if } n \textit{ is even} \\ 1/6 + 1/6n, & \textit{if } n \textit{ is odd} \end{cases}$$

$$R_B = \begin{cases} 1/6 + 1/6(n-1), & \textit{if } n \textit{ is even} \\ 1/6 + 1/6n, & \textit{if } n \textit{ is odd} \end{cases}$$

If $n = 2$, then the pixel expansion is 6 and the color ratio of the scheme is 1/3.

5 Generalization to an arbitrary number of colors

Our scheme can be generalized to an arbitrary number of colors. If the secret image has the colors $\mathcal{C} = \{c_1, c_2, \ldots, c_k\}$ such that no two colors c_i and $c_j \in \mathcal{C}$ can be combined to produce a third color $c_l \in \mathcal{C}$, then for each color $c_i \in \mathcal{C}$ we define matrix X_{c_i} as follows :

$$X_{c_i} = \begin{bmatrix} c_i & 0 & c_1 & \ldots & c_{i-1} & c_{i+1} & \ldots & c_k & 1 & \ldots & 1 & 1 & \ldots & 1 \\ 0 & c_i & 1 & \ldots & 1 & 1 & \ldots & 1 & c_1 & \ldots & c_{i-1} & c_{i+1} & \ldots & c_k \end{bmatrix}$$

Note that X_{c_i} has $2k$ columns. We define S_{c_i} in terms of X_{c_i} and S^1 as follows:

S_{c_i} is an $n \times 2 \cdot m \cdot k$ matrix obtained by replacing the 0's of S^1 by the first row of X_{c_i} and the the 1's of S^1 by the second row of X_{c_i}.

On combining any two rows of S_{c_i}, the number of columns with color c_i is $m[1 + 2 \cdot \alpha(m)]$. The proof of this is similar to the proof of Lemma 2. The color ratio X_{c_i} is therefore:

$$\begin{aligned} X_{c_i} &= \frac{m[1 + 2 \cdot \alpha(m)]}{2mk} \\ &= \frac{1}{2k} + \frac{\alpha(m)}{k} \end{aligned}$$

This lower bound is independent of the number of shares and depends only on the number of colors in the secret image. In case colors can be combined, we will get a better lower bound for the color ratio.

6 Conclusion

In this paper we have proposed a new construction for a $(2, n)-$VTS with the color sets $\mathcal{C}_1 = \{C, Y, G\}$ and $\mathcal{C}_2 = \{C, Y, M, R, G, B\}$. For the first color set $\mathcal{C}_1$, our scheme achieves a color ratio that is lower bounded by $1/4$; for the second color set $\mathcal{C}_2$, the lower bound on the color ratio is $1/6$. The color ratio that we obtain is also much higher than those obtained from the schemes in [6] and [8]. The pixel expansion is quite good, and is certainly better than the one in [8]. We have also shown that our scheme can be extended to an arbitrary number of colors and that the pixel expansion of our scheme does not depend on the number of shares but only on the number of base colors. Extending this scheme to a $(k, n)-$VTS remains an open problem.

References

1. G. Ateniese, C. Blundo, A. De Santis, and D.R. Stinson, *Visual Cryptography for General Access Structures* Information and Computation, vol.129, pp.86-106, 1996.
2. G. Ateniese, C. Blundo, A. De Santis, and D.R. Stinson, *Constructions and Bounds for Visual Cryptography*, in "23rd International Colloquim on Automata, Languages and Programming" (ICALP '96), F.M. auf der Heide and B. Monien Eds., Vol. 1099 of "Lecture Notes in Computer Science", Springer-Verlag, Berlin, pp. 416-428,1996.
3. C. Blundo, A.De Santis, and D.R. Stinson, *On the Contrast in Visual Cryptography Schemes*, J. Cryptology, vol.12, no.4, pp.261-289, 1999.
4. C. Blundo, A.De Santis and M. Naor, *Visual Cryptography for gray Level Images*, Inf. Process. Lett., Vol. 75, Issue. 6, pp.255-259, 2001.
5. S. Droste, *New Results on Visual Cryptography*, Advance in Cryptography-CRYPT'96, Lecture Notes in Computer Science, 1109, pp. 401-415, Springer-Verlag, 1996.
6. H. Koga and H. Yamamoto, *Proposal of a Lattice-Based Visual Secret Sharing Sceme for Color and Gray-Scale Images*, IEICE Trans. Fundamentals, Vol. E81-A, No. 6 June 1998.
7. H. Koga and T. Ishihara, *New Constructions of the Lattice-Based Visual Secret Sharing Scheme Using Mixture of Colors*, IEICE Trans. Fundamentals, Vol. E85-A, No. 1 January 2002.
8. H. Koga, M. Iwamoto and H. Yamamoto, *An Analytic Construction of the Visual Secret Scheme for Color Images*, IEICE Trans. Fundamentals, Vol. E84-A, No.1 January 2001.
9. M. Naor and A. Shamir, *Visual Cryptography*, Advance in Cryptography, Eurocrypt'94, Lecture Notes in Computer Science 950, pp. 1-12, Springer-Verlag, 1994.
10. V. Rijmen and B. Preneel, *Efficient Colour Visual Encryption or "Shared Colors of Benetton"*, presented at EUROCRYPT '96 Rump Session. Available at `http://www.iacr.org/conferences/ec96/rump/preneel.ps`.