$(2, n)$-Visual Cryptographic Schemes For Color Images With Low Pixel Expansion

Bhaswar B. Bhattacharya, Abhishek Chakrabortty, Shirshendu Ganguly, Shyamalendu Sinha

Indian Statistical Institute, Kolkata - 700 108, India,
bhaswar.bhattacharya@gmail.com

***Abstract*—In this paper we propose a $(2, n)$ visual cryptographic scheme for color images having low pixel expansion, when $n = 3t$, with $t \geq 3$. We use the Latin square aided construction of a $(2, n)$-VTS for black and white images of Adhikari and Bose [1] to improve upon the pixel expansion of the $(2, n)$-VTS for color images obtained by Adhikari and Sikdar [2]. The method has been applied to obtain $(2, n)$-color VTS with three and six colors, and finally generalized to k colors, where no two colors add up to give the third color. Our scheme reduces the pixel expansion dramatically and the the color ratios are reasonably good. Moreover, for small values on n our method is superior, both in terms of pixel expansion and color ratios.**

I. INTRODUCTION

In this paper we consider the problem of encrypting written material (printed text, hand- written notes, pictures, etc.) in a perfectly secure way which can be decoded directly by the human visual system. This is the famous concept of visual cryptography which was introduced by Naor and Shamir [12]. 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 [12] involved black and white images. Further research have extended the idea to gray-scale images [7], color images [2], [9], [10], [11], and general access structure [3]. Droste [8] considered the problem sharing multiple images among n participants. An alternative reconstruction method for $(2, n)$-VTS, which improves upon the contrast, was later proposed by by Noar and Shamir [13]. Blundo et al. [4], [5], [6] studied $(2, n)$-VTS for black and white images having optimal relative contrast.

In this paper we study the problem of $(2, n)$-VTS for color images. Using the Latin square aided construction of of Adhikari and Bose [1] and the construction of Adhikari and Sikdar [2] we obtain a $(2, n)$-VTS for color images having low pixel expansion. We obtain a $(2, n)$-color VTS with colors cyan, yellow, and green when $n = 3t$ with $t \geq 3$, having pixel expansion $4t(t - 1)$. This is a dramatic improvement over the scheme of Adhikari and Sikdar [2], where the pixel expansion is exponential in n. Naturally, we lose in terms of color ratios, however, the compromise seems to be reasonable. The color ratio of the colors cyan and yellow in our scheme is bounded from below by $1/4$ and that of green is $1/t$. We obtain similar results for a $(2, n)$-VTS with six colors. Moreover, the scheme generalizes to k colors such that no two colors can be combined to give the third color. The pixel expansion of our scheme is $2kt(t-1)$ and the color ratios of the all the colors are bounded below by $1/2k$. In comparison, the construction of Adhikari and Sikdar [2] has pixel expansion $2km$, where $m = \binom{n}{\lfloor n/2 \rfloor}$, and color ratios are bounded from below by $3/4k$.

In Section II we give the mathematical formulation of visual threshold schemes and introduce several relevant definitions. In Section III we review some of the major results in $(2, n)$-VTS for both black and white and color images obtained so far. Our results are presented in Section IV, where we obtain a series of results for $(2, n)$-VTS in color images with having low pixel expansion. In Section V we summarize and give some directions for future work.

II. PRELIMINARIES

A. The Model

Let $P = \{1, 2, \ldots, n\}$ be a set of elements called participants, and let 2^P denote the set of all subsets of P. Let Γ_{Qual} and Γ_{Forb} be subsets of 2^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 j-th subpixel in the i-th share is black. When the shares are stacked together, the perceived grey level is proportional to the number of ones 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 which is taken directly from Atienese, Blundo, De Santis, and Stinson [4]. Also, $OR\ V$ is used to denote the boolean operation OR of a set of vectors with result V. The Hamming weight $w(V)$ is the number of ones in the boolean vector V.

Definition 1: 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 cryptographic scheme $(\Gamma_{Qual}, \Gamma_{Forb}, m)$-VTS if there exists values $\alpha(m)$ and $\{t_X\}_{X \in \Gamma_{Qual}}$ satisfying:

(i) 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 the rows $\{i_1, i_2, \ldots, i_p\}$ satisfies $w(V) \leq t_X - m\alpha(m)$, whereas, for any $M \in C_1$ we have $w(V) \geq t_X$.

(ii) Any forbidden set $X = \{i_1, i_2, \ldots, i_p\} \in \Gamma_{Forb}$ has no information on the shared image. Formally, 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 reconstructible, 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 pixel expansion (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 $m\alpha$ is the contrast, which we want to be as large as possible. We require that $m\alpha \geq 1$ 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 (respectively black) pixel, the dealer randomly chooses one of the matrices in C_0 (respectively 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 C_0 (C_1). Finally, note that the size of the collections C_0 and C_1 need not be the same.

B. Definitions

Instead of working with the collections C_0 and C_1, it is convenient to consider only two $n \times m$ boolean matrices, S_0 and S_1 called basis matrices which satisfy the following definition:

Definition 2: Let $(\Gamma_{Qual}, \Gamma_{Forb})$ be a general access structure on a set of n participants. A $(\Gamma_{Qual}, \Gamma_{Forb}, m)$-VTS with pixel expansion m, 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:

(i) 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 $w(V) \leq t_X - m\alpha(m)$; whereas, for S_1 it results that $w(V) \geq t_X$.

(ii) 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 C_0 and C_1 are obtained by permuting the columns of the corresponding basis matrix (S_0 for C_0 and S_1 for C_1) in all possible ways. Note that, in this case, the sizes of the collections C_0 and C_1 are the same.

Now we modify the basis matrices S_0 and S_1 by a random permutation to ensure that the participants cannot decipher the actual color of pixel from less number of shares than required. For each pixel P, we generate a random permutation π of the set $\{1, 2, \ldots, m\}$. If P is a black pixel, then apply π to the columns of S_0. Otherwise, apply π to the columns of S_1. Call the resulting matrix T. For $1 \leq i \leq n$, row i of T comprises the m subpixels of P in the i-th share. This is called the *share distribution algorithm.*

A (k, n) threshold structure is any access structure $(\Gamma_{Qual}, \Gamma_{Forb})$ in which $\Gamma_{Qual} = \{B \subseteq P : |B| = k\}$ and $\Gamma = \{B \subseteq P : |B| \leq k - 1\}$. In any (k, n)-threshold VTS, 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 VTS, the image remains visible if more than k participants stack their transparencies.

The difference in the grey level of a black pixel and a white pixel in the recovered image determines the clarity of the recovered image. To measure this, the concept of relative contrast was first introduced in Naor and Shamir [12], who called it *relative difference*. For a $(2, n)$-VTS with pixel expansion m, for any pair of participants $i < j$, $(i, j = 1, 2, \ldots, n)$, let $H_0\{i, j\}$ (respectively $H_1\{i, j\}$) be the n-bit vector obtained by taking the component-wise OR of the rows i and j of S_0 (respectively S_1). Let $w(H_0\{i, j\})$ (respectively $w(H_1\{i, j\})$) denote the number of ones in $H_0\{i, j\}$ (respectively $H_1\{i, j\}$). The relative difference of the scheme is defined as

$$\min_{1 \leq i < j \leq n} \frac{[w(H_1\{i, j\}) - w(H_0\{i, j\})]}{m}$$

where the minimum is over all pairs of rows i and j of S_1.

III. Prior Work

After the publication of Naor and Shamir's [12] classical paper introducing the notion of visual cryptology, there has been a series of works on the different aspects of visual threshold schemes for black and white, gray level [7] and color images [2], [11].

In this section we discuss some of the important results obtained so far in the context both black and white and color $(2,n)$-VTS.

A. $(2,n)$ *Visual Threshold Scheme For Black and White Images*

As mentioned earlier the goodness of a visual threshold is determined largely by two parameters the pixel expansion m and the relative difference $\alpha(m)$. The problem of constructing VTS with best contrast has been extensively studied by Blundo et al. [4], [5], [6]. Blundo et. al [6] presented a $(2,n)$-VTS in which relative difference is optimal by constructing the $n \times m$ basis matrices S_0 and S_1. The columns of S_1 consist of all binary n vectors of weight $\lfloor n/2 \rfloor$. Hence, the pixel expansion $m = \binom{n}{\lfloor n/2 \rfloor}$ 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 weight $\binom{n-1}{\lfloor n/2 \rfloor -1}$. Then, they prove the following theorem:

Theorem 1: (Blundo, De Santis, and Stinson [6]) In any $(2,n)$-threshold visual cryptographic scheme with $n \geq 2$ and pixel expansion m, the relative contrast $\alpha(m)$ satisfies $\alpha(m) \leq \alpha^*(n) = \lfloor n/2 \rfloor \lceil n/2 \rceil / (n(n-1))$. Moreover, for any $n \geq 2$ there exists a strong $(2,n)$-visual cryptographic scheme with pixel expansion $m = \binom{n}{\lfloor n/2 \rfloor}$ and $\alpha(m) = \alpha^*(n)$.

Recall that a (v,k,λ)-BIBD (*balanced incomplete block design*) is a pair $(\mathcal{X}, \mathcal{B})$, where $\mathcal{X}$ is a set of v elements (called *points*) and $\mathcal{B}$ is a collection of subsets of $\mathcal{X}$ (called *blocks*), such that each block contains exactly k points and each pair of points is a subset of exactly λ blocks. In a (v,k,λ)-BIBD, each point occurs in exactly $r = \lambda(v-1)/(k-1)$ blocks, and the total number of blocks is $b = vr/k$ The number r is called the *replication number* of the BIBD.

Blundo et al. [6] also proves the following two theorems which indicates that a suitable BIBD, if it exists, can be used to obtain $(2,n)$-VTS for black and white images.

Theorem 2: (Blundo, De Santis, and Stinson [6]) Suppose n is even. Then there exists a $(2,n)$-threshold VTS with pixel expansion m and (optimal) relative difference $\alpha(m) = \alpha^*(n)$ if and only if there exists an $(n, n/2, m(n-2)/(4n-4))$-BIBD.

Theorem 3: (Blundo, De Santis, and Stinson [6]) If a (n,k,λ)-BIBD exists, then there exists $(2,n)$-VTS scheme with pixel expansion $m = b = \lambda(n^2-n)/(k^2-k)$ and relative difference $\alpha(n) = (r-\lambda)/b = k(n-k)/n(n-1)$.

The problem of obtaining $(2,n)$-VTS with reduced pixel expansion was first addressed by Adhikari and Bose [1]. They constructed a $(2,n)$ VTS for black and white images with very low pixel expansion whenever $n = 3t$, with $t \geq 3$, using properties of Latin squares. Though the relative difference in this case is far from optimal, it is reasonably good in a practical situation.

Theorem 4: (Adhikari and Bose [1]) For any n of the form $n = 3t$, with $t \geq 3$, there exists a $(2,n)$-VTS with pixel expansion $t(t-1)$ and relative difference $1/t - 1/(t(t-1))$.

The basis matrix S_1 that is constructed for proving the above theorem has two important properties. Firstly, every row in S_1 has exactly $t-1$ ones, the rest are zeros. Moreover, the hamming weight of boolean OR of any two rows is $2(t-1)-\lambda$, where λ is either 0 or 1.

B. $(2,n)$ *Visual Threshold Schemes For Color Images*

Construction of a visual threshold for color images is a challenging problem. We begin with the definition of a color VTS.

Definition 3: Let us suppose we can generate all the colors in the secret image using the color set $C = \{c_1, c_2, \ldots, c_J\}$. 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:

(i) 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.

(ii) For any subset $\{i_1, i_2, \ldots, i_j\} \subset \{1, 2, \ldots, n\}$, the submatrices G'_i obtained by restricting each G_i to the rows $\{i_1, i_2, \ldots, i_j\}$ 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.

The notion of relative difference in black and white schemes gets modified into the notion of color ratio for color images, which measures the contrast of every color separately. The formal definition is as follows:

Definition 4: 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 of the number of subpixels that possess the true color by the total number of subpixels, 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 above, 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. [11] 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 semi-lattice. 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 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.

Adhikari and Sikdar [2] propose a new $(2, n)$ threshold schemes which attains a reasonably good lower bound on the color ratios which depends only on the number of colors and not on the number of shares n. Moreover, their color ratios are significantly more than those obtained by Koga and Iwamoto [9] and Koga et al. [11]. They proved the following two results for a $(2, n)$ VTS having three or six colors:

Theorem 5: (Adhikari and Sikdar [2]) 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 $4\alpha^*(n)$ and color ratios

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

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

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

Theorem 6: (Adhikari and Sikdar [2]) 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 $6\alpha^*(n)$ and color ratios

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

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

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

They also proved that if the secret image has the colors $C = \{c_1, c_2, \ldots, c_k\}$ such that no two colors c_i and c_j in C can be combined to produce a third color c_l in C, then the color ratio of their scheme is lower bounded by $3/4k$. However, since their construction uses the basis matrix for the optimal relative difference [6], the pixel expansion of their scheme is, exponential in n.

IV. $(2, n)$-VTS For Color Images With Low Pixel Expansion

In this paper we improve upon the pixel expansions, albeit at the cost of color ratios, obtained in Theorem 5 and Theorem 6. The construction is very much similar that of Adhikari and Sikdar [2], and also uses the $(2, n)$-VTS of Adhikari and Bose [1], which uses Latin square design.

The results are presented in three different subsections. In the first section a $(2, n)$-VTS with three base colors is obtained. Several optimality criteria, including pixel expansion, color ratios, and presence of nuisance colors, are studied. The next section contains a similar result with six colors, and in the final section we generalize our scheme to k colors, whenever no two colors can be combined to give a third color.

A. $(2, n)$-VTS With Three Base Colors

Suppose that the original image is composed of only three colors, namely *Cyan (C), Yellow (Y)* and *Green (G)*, with $C + Y = G$. We will first construct a $(2, 2)$-VTS with the color set $C = \{C, Y, G\}$. To do this, it is sufficient to construct the basis matrices corresponding to the colors C, Y and G respectively. These basis matrices are given below:

$$X_C = \begin{pmatrix} C & 0 & Y & 1 \\ 0 & C & 1 & Y \end{pmatrix},$$

$$X_Y = \begin{pmatrix} Y & 0 & C & 1 \\ 0 & Y & 1 & C \end{pmatrix},$$

$$X_G = \begin{pmatrix} C & Y & 0 & 1 \\ Y & C & 0 & 1 \end{pmatrix}.$$

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 any $(2, n)$-VTS for black and white images. To construct our $(2, n)$-color VTS, 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. 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 obtained in terms of S_1 by replacing 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 i-th 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.

In Theorem 5, Adhikari and Sikdar take S_1 to be the matrix for obtaining optimal relative contrast as described by Blundo et al. [6].

In the following theorem, we prove the existence of $(2, n)$-VTS for three colors with low pixel expansion and reasonably good color ratios, by taking S_1 to be the matrix obtained from the proof of Theorem 4. This matrix was constructed by Adhikari and Bose [1] using the properties of a Latin square.

Theorem 7: For any $n = 3t$ ($t \geq 3$), there exists a $(2, n)$ color VTS with base colors Cyan (C), Yellow (Y), and Green (G) with pixel expansion $4t(t-1)$ and color ratios $R_C = R_Y = 1/4 + 1/2t$ and $R_G = 1/t$.

Proof: Take S_1 to be the basis matrix obtained by the $(2, n)$-VTS using Latin Squares in Theorem 4. The pixel expansion of their scheme is $t(t-1)$, where $n = 3t$, with $t \geq 3$. The existence of a $(2, n)$ VTS with three colors and the required pixel expansion now follows from the construction of the basis matrices S_C, S_Y, and S_G with the matrices X_C, X_Y, and X_G as templates and starting with S_1.

Now, observe that the number of $(1, 1)'$ pairs in $S_1\{i, j\}$ is λ, where λ =0 or 1. The number of $(1, 0)'$ pairs in $S_1\{i, j\} = t - 1 - \lambda$. From symmetry, the number of $(0, 1)'$ pairs in $S_1\{i, j\} = t - 1 - \lambda$. Each $(1, 1)'$ or $(0, 0)'$ pair in $S_1\{i, j\}$ gives one Cyan (or one Yellow) pixel, and each $(0, 1)'$ or $(1, 0)'$ gives two Cyan (or two Yellow) pixels each.

Since X_C and $X_Y$are symmetric we get,

$$R_C = R_Y =$$

$$\frac{2(t-1-\lambda)+2(t-1-\lambda)+\{t(t-1)-2(t-1-\lambda)\}}{4t(t-1)}$$

$$\approx 1/4+1/2t$$

For X_G, only the patterns $(0,1)'$ or $(1,0)'$ gives two Green pixels. Thus, we have $R_G = \frac{4(t-1-\lambda)}{4t(t-1)} \approx 1/t$. ■

Nuisance Colors: 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 $N(c_j, c_i)$.

In this case, yellow is a nuisance color for cyan and we denote the number of yellow subpixels in a cyan pixel by $N(Y,C)$. Similarly for a yellow pixel, the nuisance color is cyan and we denote the number of cyan subpixels by $N(C,Y)$. Finally, a green pixel has as nuisance colors both cyan and yellow and we denote their numbers by $N(C,G)$ and $N(Y,G)$, 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.

Now, we shall compute the value of $N(Y,C)$. Observe that when the i-th and j-th rows of S_C are superimposed the nuisance color yellow occurs when patterns $(1,1)'$ or $(0,0)'$ occurs in $S_1\{i,j\}$, each of which contributes one yellow pixel to he superimposed image. When the basis matrix S_1 is from the Latin Square design of Theorem 4 the pattern $(0,0)'$ occurs λ times where λ =0 or 1. The pattern $(0,0)'$ occurs $t(t-1)-2(t-1-\lambda)-\lambda$ times. Therefore, we get $N(Y,G) = t(t-1)-2(t-1-\lambda)$. The fraction of the subpixel which have color yellow is $N(Y,C)/m \leq 1/4$. From symmetry, it follows that $N(Y,C) = N(C,Y)$. For the green pixel the number of cyan or yellow colored pixels is $t(t-1)-2(t-1-\lambda)$. Therefore, $(N(C,G)+N(Y,G))/m \leq 1/2$.

B. $(2,n)$-Color VTS with Six Base Colors

Now, 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)*, such that Note that $C+Y=G$, $C+M=B$, and $Y+M=R$. Consider the following six matrices as templates:

$$X_Y = \begin{pmatrix} Y & 0 & C & M & 1 & 1 \\ 0 & Y & 1 & 1 & C & M \end{pmatrix},$$

$$X_C = \begin{pmatrix} C & 0 & M & Y & 1 & 1 \\ 0 & C & 1 & 1 & M & Y \end{pmatrix}$$

$$X_M = \begin{pmatrix} M & 0 & Y & C & 1 & 1 \\ 0 & M & 1 & 1 & Y & C \end{pmatrix}$$

$$X_R = \begin{pmatrix} Y & M & C & 1 & 1 & 0 \\ M & Y & 1 & C & 0 & 1 \end{pmatrix}$$

$$X_G = \begin{pmatrix} Y & C & M & 1 & 1 & 0 \\ C & Y & 1 & M & 0 & 1 \end{pmatrix}$$

$$X_B = \begin{pmatrix} M & C & Y & 1 & 1 & 0 \\ C & M & 1 & Y & 0 & 1 \end{pmatrix}.$$

Let S_1 be a basis matrix for any $(2,n)$ black and white VTS. 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 by replacing 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 i-th 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.

Adhikari and Sikdar [2] take S_1 to be the matrix for obtaining optimal relative contrast as described by Blundo et al. [6] in Theorem 6 to get a $(2,n)$-VTS for six colors.

In the following theorem, we prove the existence of $(2,n)$-VTS for six colors with low pixel expansion, by taking S_1 to be the matrix obtained by Adhikari and Bose [1] using Latin squares design (Theorem 4). The proof is exactly similar to that of Theorem 7.

Theorem 8: For any $n = 3t$ ($t \geq 3$), 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 $6t(t-1)$ and color ratios $R_Y = R_C = R_M = 1/6+1/3t$ and $R_R = R_G = R_B = 2/3t$.

C. Generalization To Arbitrary Number of Colors

If the secret image has the colors $C = \{c_1, c_2, \ldots, c_k\}$ such that no two colors c_i and $c_j \in C$ can be combined to produce a third color $c_l \in C$, then for each color $c_i \in C$ we define matrix X_{c_i} as shown in Equation 1.

Note that X_{c_i} has $2k$ columns. We define S_{c_i} in terms of X_{c_i} and the basis matrix of any $(2,n)$ black and white S_1 as follows: S_{c_i} is an $n \times 2mk$ matrix obtained by replacing the zeros of S_1 by the first row of X_{c_i} and the the ones of S_1 by the second row of X_{c_i}.

Again, in the same way as in Theorems 7 and 8 we obtain the following theorem for arbitrary number of colors by using S_1 as in Adhikari and Bose [1].

Theorem 9: For any $n = 3t$ where $t \geq 3$, there exists a $(2,n)$ color VTS with a set C of k colors, such that no two of C can be combined to obtain a third color, having pixel expansion $2kt(t-1)$ and color ratios $R(C_i) = 1/2k + 1/kt \approx 1/2k$.

$$X_{c_i} = \begin{pmatrix} c_i & 0 & c_1 & \dots & c_{i-1} & c_{i+1} & \dots & c_k & 1 & \dots & 1 & 1 & \dots & 1 \\ 0 & c_i & 1 & \dots & 1 & 1 & \dots & 1 & c_1 & \dots & c_{i-1} & c_{i+1} & \dots & c_k \end{pmatrix}. \quad (1)$$

Note that the color ratios of all the colors in this setup is bounded below by $1/2k$. This is unlike the situations in Theorems 7 and 8, where the color ratios of some of the colors decreases as the number of shares increase. Moreover, the analogous result obtained by Adhikari and Sikdar [2] using S_1 as in Blundo et al. [6] is bounded below by $3/4k$. Therefore, we lose the contrast only by a factor of $1/4k$, but dramatically improve upon the pixel expansion.

V. Conclusions

In this paper we study the problem of constructing $(2, n)$-VTS schemes with low pixel expansion and reasonably good contrasts. A construction of a $(2, n)$-VTS for black and white pixels using Latin squares has been used to extend the results of Adhikari and Sikdar [2] for $(2, n)$-VTS for color images, to obtain schemes with low pixel expansion and reasonable color ratios.

Similar results can also be obtained with the help of BIBD's. Careful interpretation of such results needs to be done to understand its implications on color ratios and pixel expansion. These results may also be helpful in the construction of $(2, n)$-color VTS with optimal color ratios. Generalizing the scheme to (k, n)-VTS for color images is another interesting problem.

Acknowledgment

We would like to thank Prof. Bimal K. Roy and Prof. G. M. Saha for proposing the problem to us, and for their inspirational guidance.

References

[1] A. Adhikari and M. Bose, A New Visual Cryptographic Scheme Using Latin Squares, *IEICE Transactions Fundamentals*, Vol. E87-A, No.5, 1998-2002, May 2004.

[2] A. Adhikari and S. Sikdar, A New $(2, n)$-Visual Threshold Scheme For Color Images, *Indocrypt 2003*, LNCS, 2904, 148-161, 2003.

[3] A. Adhikari, T.K. Dutta, and B. Roy, A New Black and White Visual Cryptographic Scheme For General Access Structures, *Indocrypt 2004*, LNCS, 3348, 399-413, 2004.

[4] G. Ateniese, C. Blundo, A. De Santis, and D.R. Stinson, Visual Cryptography for General Access Structures, *Information and Computation*, Vol. 129, 86-106, 1996.

[5] G. Ateniese, C. Blundo, A. De Santis, and D.R. Stinson, Constructions and Bounds for Visual Cryptography, *Proc. 23rd International Colloquim on Automata, Languages and Programming (ICALP 1996)*, LNCS 1099, 416-428,1996.

[6] C. Blundo, A.De Santis, and D.R. Stinson, On the Contrast in Visual Cryptography Schemes, *Journal of Cryptology*, Vol. 12 (4), 261-289, 1999.

[7] C. Blundo, A.De Santis, and M. Naor, Visual Cryptography for gray Level Images, *Information Processing Letters*, Vol. 75 (6), 255-259, 2001.

[8] S. Droste, New Results on Visual Cryptography, *Advance in Cryptography- CRYPT 1996*, LNCS 1109, 401-415, 1996.

[9] H. Koga and H. Yamamoto, Proposal of a Lattice-Based Visual Secret Sharing Sceme for Color and Gray-Scale Images, *IEICE Transactions Fundamentals*, Vol. E81-A, No. 6, June 1998.

[10] H. Koga and T. Ishihara, New Constructions of the Lattice-Based Visual Secret Sharing Scheme Using Mixture of Colors, *IEICE Transactions Fundamentals*, Vol. E85- A, No. 1, January 2002.

[11] H. Koga, M. Iwamoto, and H. Yamamoto, An Analytic Construction of the Visual Secret Scheme for Color Images, *IEICE Transactions Fundamentals*, Vol. E84-A, No. 1, January 2001.

[12] M. Naor and A. Shamir, Visual Cryptography, *Advance in Cryptography, Eurocrypt 1994*, LNCS 950, 1-12, 1994.

[13] M. Noar and A. Shamir, Visual Cryptography II: Improving the Contrast Via the Cover Base, *presented at Security in Communications Networks*, Italy, September 1996.