

Journey of VCS from Black and White Images to Colored Images with their Performance Analysis

Neha Gupta
Assistant Professor
CS & IT Department
M.I.T. Moradabad

Manish Gupta
Assistant Professor
CS & IT Department
M.I.T. Moradabad

Abhishek Mishra
Assistant Professor
School of Computer Science
and Engineering,
IFTM University,

ABSTRACT

Visual Cryptography (VC), an emerging technology for secret sharing which allows visual information (pictures, text, etc.) to be encrypted in such a way that the decryption can be performed by the human vision system (HVS). Originally it was proposed by Naor and Shamir in 1994 for black and white images. Later this technique is extended for gray level images as well as for color images. This paper compares and analyze the performance of various VCS on various parameters such as pixel expansion, contrast, shares generated etc. The compared algorithms came into aura by rectifying limitations of one another.

Keywords

Visual cryptography, Pixel Expansion, Halftone technology, Color decomposition, Color Visual Cryptography.

1. INTRODUCTION

In the continually evolving world of secure image sharing, a growing number of people are becoming involved as new applications and business models are being developed all the time. This contributed volume gives academicians, researchers, and professionals the insight of well-known experts on key concepts, issues, trends, and technologies in this emerging field.

Visual Cryptography technology, proposed in 1994 by Naor and Shamir [1], used the characteristics of human vision to decrypt the encrypted image. Their scheme acts as a building block of other VCS schemes. They hide the secret image in n distinct images called shares and the secret image can then simply be revealed by stacking together k shares. This is called as (k, n) -threshold scheme (threshold is k , which means secret image is visible if and only if any k transparencies are stacked together). Here each share looked like a collection of random pixels. Naor and Shamir analyzed the case of (k, n) -threshold VCS for black and white secret image. Its major features:

From user point of view :- It needed neither cryptography knowledge nor complex computation.

From security point of view:- It ensures that hackers could not perceive any clue about a secret image from individual cover images.

Hou [2] proposed a VCS for color images. His methods are based on Halftone technique and color decomposition. All the methods given by Hou are based on the subtractive model. Afterwards, Yang-Chen [3] proposed another algorithm that uses additive model in a probabilistic way. Finally we compare Wu-Wong-Li [4] method which is the first one satisfying all the properties with no pixel expansion.

2. LITERATURE SURVEY

2.1 Naor-Shamir Black-and-White VCS

In the original encryption, the problem can be considered as a $(2, 2)$ secret sharing. The solution of the $(2, 2)$ black-and-white VCS scheme by either dividing one pixel into two subpixels or four subpixels in the two shares. So the size of the superimposed image is expanded by a factor of 4. Fig. 1 shows all the possible arrays of the four subpixels.

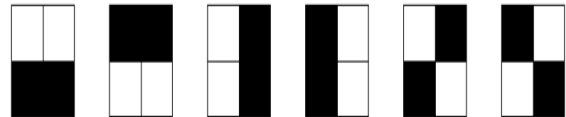


Fig 1: The Six Arrays of Four Subpixels

Randomly choose an array from Fig. 2.1 for a pixel in the secret image, as the first share. The second share is identical with the first one if the original pixel is white and if the original pixel is black, the second share is complementary with the first one. When we superimpose the two shares, the white color is recovered as medium gray and the black color is recovered as completely black. Secret sharing improves the reliability and robustness of secure key management.

Example: Consider the following situation: If the only key that provides access to some important data is lost somewhere, then that important data will become inaccessible. Thus this problem can be resolved by dividing the key into pieces and then distributing them to different persons so that any pre-specified set of persons can recover the key jointly.

2.2 VCS Schemes for Gray-Scale Images

Because of the limitation in black-and-white VCS schemes, Verheul and Tilborg [5] in 1997 proposed the k -out-of- n VCS for gray-scale images. To improve the pixel expansion of Verheul and Tilborg's VCS, in 2003 Lin and Tsai proposed another VCS scheme for gray-scale images by applying pre processing techniques such that the pixel expansion rate is the same as Naor-Shamir's black and white VCS.

In 2007, Chen et al. [3] extended the results to gray-scale images and proposed a gray-scale VCS scheme with the goal of no pixel expansion. Although, their scheme does not support colored images and only supports (k, k) threshold setting. Also it needs to do preprocessing before secret sharing on the original images.

3. PREVIOUS WORK

3.1 (k,n) Threshold Scheme

In this a secret is divided into n number of shares and distributed among n persons. When any k or more of these persons ($k \leq n$) bring their shares together, the secret can be recovered. However, if $(k-1)$ persons attempt to reconstruct the secret, they will fail. Due to this threshold scheme, it is referred as a (k, n) threshold secret sharing scheme.

3.2 Fundamentals of Color Models

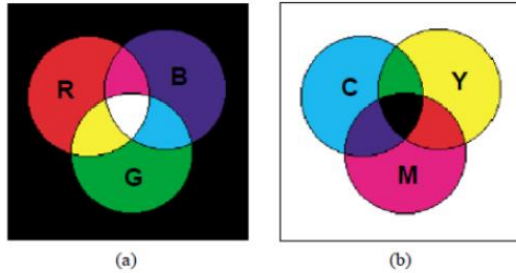


Fig 2: (a) Additive model (b) Subtractive model

3.3 Basic Concepts for handling VCS Schemes for Color Images

Basic Terminologies used in encrypting Colored Images via Visual Cryptographic method are discussed below.

Halftoning: This method uses the density of the net dots to simulate the gray level is called “Halftone” and transforms an image with gray level into a binary image before processing.

Color Decomposition: In this, every color on a color image can be decomposed into three primary colors: C, M, Y (if subtractive model is used) or R, G, B (if additive model is used). This method expands every pixel of a color secret image into a 2×2 block in the sharing images and keeps two colored and two transparent pixels in the block.

Pixel expansion: Pixel expansion m refers to the number of subpixels in the generated shares that represents a pixel of the original input image. Smaller pixel expansion results in smaller size of the share. It represents the loss in resolution from the original picture to the shared one.

4. VARIOUS METHODS FOR CVCS

4.1 CVCS Scheme Proposed by Y.C. Hou

For Color VCS schemes, Hou's schemes are believed to be the first set of color VCS Schemes. Hou proposed three methods and a subtractive model is used in all the three methods.

Hou's Method 1: This method produces four shares, namely black mask, C, M, and Y share. The reconstructed image can be shown by superimposing these shares.

Step 1. Color Decomposition: The original colored image is firstly decomposed into three primary-color images under the subtractive model, namely, C (Cyan), M (Magenta) and Y (Yellow). The size of the three images is equal to that of the original one.

Step 2. Halftoning: Transform each primary color image into three C, M, and Y halftone images so that each image will have two color levels. The principle is to pack pixels in higher

density for representing darker colors and distribute the pixels sparsely for representing lighter colors.

Step 3. Black Mask: Design a randomly generated half black-and-white mask to shade unexpected colors on the stacked sharing images so that only the expected colors show up. Since the black mask is randomly generated, for each block, there are six possible patterns in total.

Step 4. Share Creation: To create the C, Y and M shares, the halftoned C, M and Y primary-color images of the original secret image are scanned pixel by pixel. 0 and 1 are used to represent the two conditions of a primary color where 0 represents absence of the primary color while 1 represents the opposite condition.

Mask	Revealed color (C,M,Y)	Share1(C)	Share2(M)	Share3(Y)	Stacked image	Revealed color quantity (C,M,Y)
	(0, 0, 0)					(1/2, 1/2, 1/2)
	(1, 0, 0)					(1, 1/2, 1/2)
	(0, 1, 0)					(1/2, 1, 1/2)
	(0, 0, 1)					(1/2, 1/2, 1)
	(1, 1, 0)					(1, 1, 1/2)
	(0, 1, 1)					(1/2, 1, 1)
	(1, 0, 1)					(1, 1/2, 1)
	(1, 1, 1)					(1, 1, 1)

Fig 3: Four separating shared transparencies and result of stacking

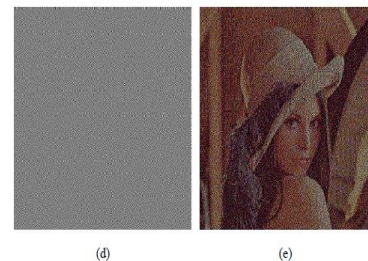
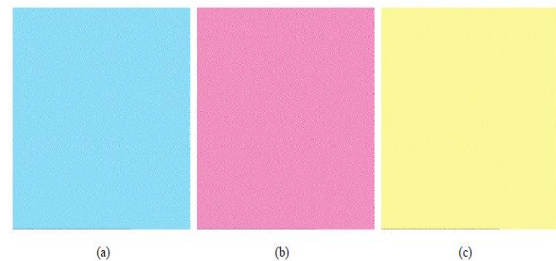


Fig 4: (a) Share 1(C), (b) Share 2(M), (c) Share 3(Y), (d) Mask, and (e) Stacked Image

Hou's Method 2:

Share Creation: The second method expands every pixel of a halftone image into a 2×2 block on two sharing images and fills the block with cyan, magenta, yellow and transparent, respectively. Two stacked images can generate various colors by using these four colors, by different permutations.

Method: According to the values of C, M, Y and Share 1, generate a 2x2 block as Share 2. The block in Share 2 is the permutation of the four colors of the block in Share 1. Repeat this step until every pixel of the decomposed image is dealt with. Hence, two visual Cryptography transparencies to share the secret image are obtained.

Example: Fig. 5 shows the two sharing transparencies and their stacked effect:

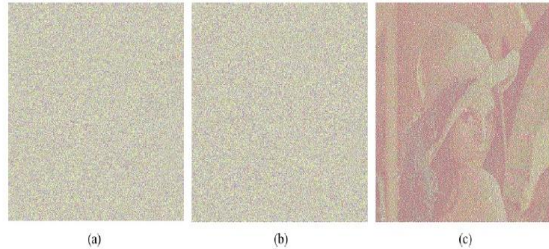


Fig 5: (a) Share 1 (b) Share 2 (c) Stacked Image

Hou's Method 3:

After transforming a color secret image into three halftone images C, M, and Y, it generates six temporary sharing images C1, C2, M1, M2, Y1, and Y2. Each of these sharing images will have two white pixels and two color pixels in every 2x2 block. The method then combines C1, M1, and Y1 to form a colored halftone Share 1 and to form colored halftone share2, combine C2, M2, and Y2.

Fig. 6 shows how to decompose a blue pixel (1; 1; 0) into two sharing blocks and how to reconstruct the blue-like block.

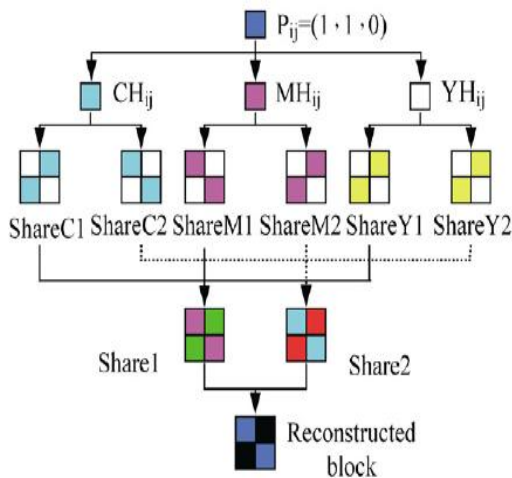


Fig. 6: Color (blue) pixel decomposition and reconstruction

4.2 CVCS Scheme Proposed by Yang-Chen

In all the previous methods given by Hou, a secret pixel is represented by several color subpixels and the number of these subpixels is referred to as the pixel expansion. Generally, they require a larger pixel expansion to produce more colors and hence increases the share size. Therefore Yang and Chen propose ACM(additive color mixing)in a probabilistic way whose pixel expansion is fixed on 3 regardless of the number of colors in the reconstructed images and the values of k and n .Thus it is also named as color-number independent and (k,n) independent scheme. Its drawback is if one wants to improve the color contrast of the

reconstructed image, then one have to modify the original image.

In this algorithm, to simulate a secret color, appearance probability of R,G,B are used. Different color appearance probabilities (p_R^i, p_G^j, p_B^k) simulate the color luminance levels(R_i, G_j, B_k). An Nc- colored (k,n) CVCS can be represented as three primary colored sets C_R^i, C_G^j and C_B^k . The value of Nc is $(L_R \times L_G \times L_B)$ where L_R, L_G, L_B are the number of levels for R,G,B color planes. Note: If we have different intervals of color planes, we suggest the large L_G because green light is more sensitive to human eyes.

Method:

1. A secret pixel is divided into three colored subpixels (R, G, B) where R-colored subpixel has the appearance probability p_R^i and null color with probability $(1 - p_R^i)$. In the same way G-color and B-color have the appearance probabilities p_G^j and p_B^k , respectively.

2. Then calculate the number of colors on the three primary colors of the original image in L_R, L_G, L_B .

3. After that construct the primary color sets C_R^i, C_G^j and C_B^k as -

$$C_R^i = C_W \cup \dots \cup C_W \cup C_B \cup \dots \cup C_B$$

such that :

$$i = (255xr)/(L_R - 1)$$

$$C_W \cup \dots \cup C_W = L_R - 1 - r$$

$$C_B \cup \dots \cup C_B = r$$

$$r \in [0, L_R - 1]$$

$$1 \rightarrow R$$

$$0 \rightarrow N$$

C_W and C_B are the basis matrices of black and white schemes.

Similarly C_G^j and C_B^k are constructed.

4. Finally scan each pixel of the original image and apply the corresponding matrices obtained in step-3 by randomly choosing a column of each of the three basis matrices.

Assign the pixel to black color if the bit is one else assign it X color ($X \in \{R, G, B\}$).

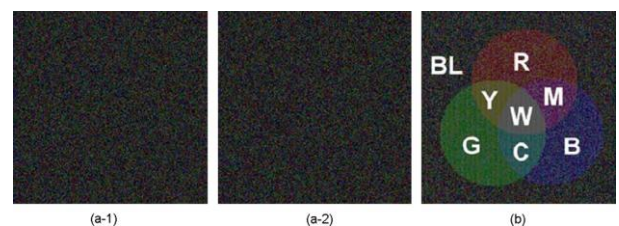


Fig 7: 8-colored (2, 2) CVCS using Fig. 2(a) as the secret image:

(a) two shadow images: S1 and S2 (b) the reconstructed image by stacking two shadows S1+S2

4.3 CVCS Scheme proposed by Wu-Wong-Li

The first scheme which supports all the five desirable properties:

1. Color number independent
- 2.No pixel expansion
- 3.No preprocessing
- 4.(k,n) independent
- 5.tunable

This scheme uses a probabilistic technique for achieving no pixel expansion. Also it allows user to choose the number of colors that the reconstructed image will have. This 'tunable' feature helps in controlling the quality of reconstructed image.

This scheme supports original images of any number of color levels with the assumption that the color of the original image is represented by the 24-bit color primitives. Each R,G,B has 256 levels(i.e. 8-bits) i.e. for each pixel the color quality is represented by 3-bytes of values.

Suppose for black and-white images ,the pixel expansion rate is m , so we use an $n \times m$ Boolean Matrix S where n rows denotes " n shares" and m columns denotes the "colors" (1 \rightarrow black; 0 \rightarrow white).

$$\begin{pmatrix} S_{0,0} & S_{0,1} & \dots & S_{0,m-1} \\ \vdots & \vdots & & \vdots \\ S_{n-1,0} & S_{n-1,1} & \dots & S_{n-1,m-1} \end{pmatrix}$$

Where $S_{ij} \in \{0,1\}$.

A (k,n) black-and-white VCS consists of two $n \times m$ Boolean Matrices B^0 and B^1 , corresponding to the white and black pixel in the original image, respectively. Let C^b be the matrices obtained by permuting the columns of B^b where $b = 0, 1$. Since the sharing of the secret image is done pixel by pixel, so for each pixel if the color is white(resp. black), one $n \times m$ Boolean Matrix in C^0 (resp. C^1) is picked randomly and used for creating the n shares.

Example: Base Boolean Matrices for (3,4) black and white VCS is :

$$\begin{pmatrix} 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}$$

Now lets see how (k,n) black and white VCS is converted to CVCS with no pixel expansion.

Method: This scheme follows following four steps:

1.Histogram Generation: First generate three primary color(i.e. R,G,B) component images and then generate three histograms of R,G,B color primitives, representing the intensity distribution. In each component image we have 256 levels of intensity of that primary color.(In histogram, horizontal axis represents intensity ranging from 0 to 255 and vertical axis represents number of pixels of each intensity value.)



Fig 8: The Original Lena Image



Fig 9: The RGB Component Images of Lena

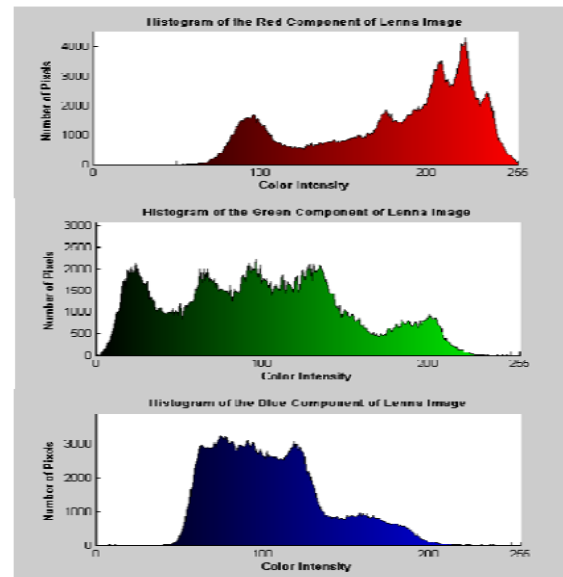


Fig 10: Histograms of the RGB Component Images

2. Color quality determination: As each color component has 256 levels of intensity, so here the choice is given to user to choose the number of intensity levels for the reconstructed secret image. This helps in maximizing the quality of the reconstructed image. Let N be the number of levels, such that $N = N_R \times N_G \times N_B$.

3.Grouping: In this we create groups on the histograms for each color primitive by specifying the color intensity

boundary between every pair of adjacent groups as $(0,k0),(k0,k1) \dots (kNx-2,255)$. The principle of division is to make each group of the same size.

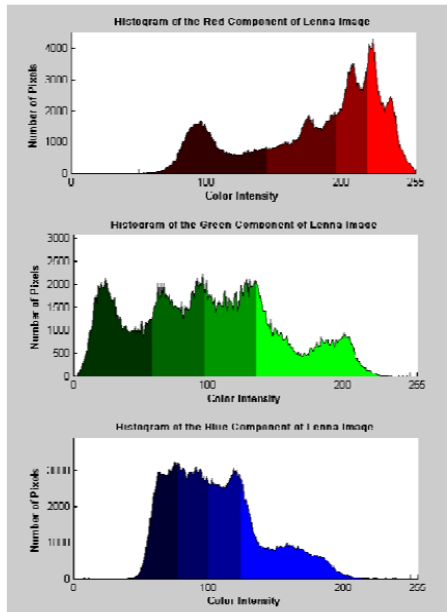


Fig 11: Histograms Illustrating the $4 \times 4 \times 4$ Color Levels

4.Share Creation: The method is applied to each of the primitive color independently. For the base boolean matrices $B^b = [B^b_0, B^b_1, \dots, B^b_{m-1}]$ ($b \in \{0,1\}$), B^b_i denotes column i of B^b .

Now, For each color primitive, $XC(R,G,B)$ this step is carried out pixel by pixel:

For each pixel:

- Suppose the color intensity of the pixel w.r.t. X falls in k th-group ($0 \leq k \leq Nx-1$). We compute P (probability value) as $P=k/Nx-1$
- With the probability value P , we proceed as:
 - (a) Look into B^0 and pick any column randomly (e.g. B^0_j)
 - (b) Let B^0_j be an n -bit vector. For the first bit, assign black color (zero color intensity) if bit is 1 otherwise assign red color (255 color intensity).

The process continues till we have assigned colors for all the n shares

- With the probability $1-P$, follow the same steps with B^1 .

Since the columns in B^0 (resp. B^1) are chosen randomly, so the chance of picking any column for group k will be $k/((Nx-1)m)$ (resp. $(1-k/(Nx-1))/m$).

Finally superimpose i th R -share with i th G -share and i th B -share to form the i th Share consists of R,G,B components

5. RESULTS AND DISCUSSION

Hou's Schemes are considered to be the first for CVCS. All the three methods have pixel expansion 4 and do not support general (k,n) threshold setting. Preprocessing is required of original image.

Table 1. Hou's Schemes Comparison

Parameters	No. of Shares	Color Intensity Range	Contrast
Hou's Method			
1	4	1/2 to 1	50% loss
2	2	1/4 to 1/2	25% loss
3	2		Most lesser loss

Yang's scheme has not only color-number-independent and (t, n) -independent properties but also the benefit of being a probabilistic VCS, i.e., no pixel expansion. From the preceding description (the small size, the ACM feature and the color-independent and (t, n) -independent properties), this means that our CVCS will certainly have more practical applications.

In Yang's scheme the color is mixed by using additive color mixing in a probabilistic way, and the appearance frequencies of R , G and B color subpixels simulate a secret color. Examples and experiments reveal that our CVCS based on the probabilistic ACM truly functions: retaining the benefit of probabilistic VCS, our CVCS has a fixed pixel expansion 3 which is less than ever.

Wu's scheme allows user to deal with colored image and determine the color number of reconstructed image according to the expected quality of it. Besides, our scheme does not need to do the dithering, which would degrade the quality of reconstructed image, but still has no pixel expansion.

Table 2. Comparison of all the four schemes

	Color	Expansion Rate	General k out of n	Color Levels	Tunable
NS	B/W	$m > 1$	General	2	No
HOU	Color	4	$k = n$	8	No
YANG-CHEN	Color	3	General	Multi	No
WU	Color	1	General	Multi	Yes

6. CONCLUSION

According to the comparative results, Wu's scheme is the first one that achieves all the desirable properties. It provides one of the best reconstructed images and share images in quality due to the "tunable" feature in the secret share creation step. Also Wu discussed how to determine the number of color levels. Hence the result shows that Wu's scheme is optimal.

7. FUTURE SCOPE

Work can be done on the

- Security of shares
- Extended CVCS where meaningful shares are generated
- Videos with various watermarking techniques.

8. REFERENCES

- [1] G. Ateniese, C. Blundo, A. D. Santis, and D. R. Stinson. Visual cryptography for general access structures. *Inf. Comput.*, 129(2):86–106, 1996.
- [2] Y. C. Hou. Visual cryptography for color images. *Pattern Recognition*, 36:1619–1629, 2003.
- [3] S. Cimato, R. Prisco, A. De Santis, Probabilistic visual cryptography schemes, *Computer J.* 49 (2006) 97--107.
- [4] C. N. Yang and T. S. Chen, “Colored visual cryptography scheme based on additive color mixing,” *Pattern Recognition*, vol. 41, no. 10, pp. 3114–3129, 2008.
- [5] Xiaoyu Wu¹, Duncan S. Wong², and Qing Li² “Threshold Visual Cryptography Scheme for Color Images with No Pixel Expansion ” 26-28,Dec. 2009, pp. 310-315
- [6] M. Naor and A. Shamir. Visual cryptography. In *Advances in Cryptology - EUROCRYPT '94*, pages 1–12, 1994. *Lecture Notes in Computer Science*
- [7] E. Verheul and H. van Tilborg. Construction and properties of k out of n visual secret sharing schemes. 1997.
- [8] R. Gonzalez and R. Woods, *Digital Image Processing Fourth Impression*