

A Study on Secret Image Hiding in Diverse Color Spaces

G. Germine Mary¹, M. Mary Shanthi Rani²

Associate Professor, Department of Computer Science, Fatima College, Madurai, India¹

Assistant Professor, Dept of Computer Science and Applications, Gandhigram Rural Institute – Deemed University,
Dindigul, India²

Abstract: Visual Cryptography is a special encryption technique to hide information in images in such a way that human visual system can decrypt the secret without any complex computation. In this study Visual Cryptography shares are created in different Color spaces, to hide the given secret. This article aims at finding the best color space to hide an image which gives qualitatively good result in terms of human visual perception and quantitatively good performances measured using standard metrics like Discrete Entropy, Contrast Improvement Index, and Peak Signal-to-Noise Ratio.

Keywords: Visual Cryptography, Secret Sharing, Color Space, YCbCr Color Space, HSV Color space, RGB color space, CMY Color space.

I. INTRODUCTION

A secret is something which is kept from the knowledge of many except the privileged. Secret sharing defines a method by which a secret can be distributed between groups of participants, whereby each participant is allocated a piece of the secret. This piece of the secret is known as a share. The secret can only be reconstructed when a sufficient number of shares are combined together. While these shares are separate, no information about the secret can be accessed. That is, the shares are completely useless when they are separated.

Visual cryptography (VC) is a new type of cryptographic scheme that focuses on solving this problem of secret sharing. Visual cryptography uses the idea of hiding secrets within images. These images are encoded into multiple shares and later decoded without any computation. This decoding is as simple as superimposing transparencies, which allows the secret to be recovered [1].

Visual cryptography is a desirable scheme as it embodies both the idea of perfect secrecy and a very simple mechanism for decrypting the secret. The interesting feature about visual cryptography is that it is perfectly secure.

Image sharing defines a scheme which is identical to that of general secret sharing. In (k, n) image sharing, the image that carries the secret is split up into n pieces (known as shares) and the decryption is totally unsuccessful unless at least k pieces are collected and superimposed [2].

In this paper, a study on the application of VC in various color spaces is done. A color space is a specific organization of colors. In combination with physical device profiling, it allows for reproducible representations of color, in both analog and digital representations. The objective of this paper is to find out the best color space to

send the secret message in the form of images. This paper is organized as follows. Section 2 reviews the organization of colors in various color space. Section 3 presents visual cryptography schemes in various color spaces. Section 4 discusses some experimental results. Finally, the conclusion appears in Section 5.

II. BASIC PRINCIPLE OF COLOR SPACE

A digital image is a numeric representation of a two-dimensional image. Depending on whether the image resolution is fixed, it may be of vector or raster type. By itself, the term "digital image" usually refers to a raster image or bit mapped images [3].

A color space is a specific organization of colors. In combination with physical device profiling, it allows for reproducible representations of color, in both analog and digital representations. A color space may be arbitrary, with particular colors assigned to a set of physical color swatches and corresponding assigned names or numbers. A color model is an abstract mathematical model describing the way colors can be represented as tuples of numbers; however, a color model with no associated mapping function to an absolute color space is a more or less arbitrary color system with no connection to any globally understood system of color interpretation. Adding a specific mapping function between a color model and a reference color space establishes within the reference color space a definite "footprint", known as a gamut, and for a given color model this defines a color space [4].

A. RGB Color Space

The additive and subtractive models (Fig. 1) are commonly used to describe the constitutions of colors [5].

RGB uses additive color mixing because it describes what kind of light needs to be emitted to produce a given color. RGBA is RGB with an additional channel, alpha, to indicate transparency. In the additive system, the primaries are Red, Green, and Blue (RGB), with desired colors being obtained by mixing different RGB components. By controlling the intensity of red (green or blue) component, we can modulate the amount of red (green or blue) in the compound light. The more the mixed colored lights, the more is the brightness of the light. When mixing all red, green and blue components with equal intensity, white color will result. The computer monitor is a good example of the additive model.

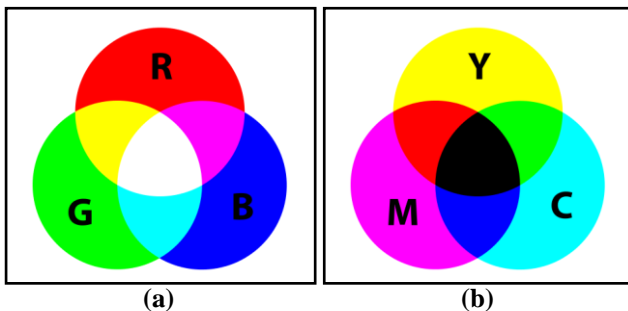


Fig. 1 (a) Additive color mixing (b) Subtractive color mixing

B. CMYK Color Space

CMYK uses subtractive color mixing used in the printing process because it describes what kind of inks needs to be applied so the light reflected from the substrate and through the inks produces a given color. In the subtractive model, (Fig. 1(b)) color is represented by applying the combinations of colored lights redirected from the surface of an object. For example, an apple under the natural light absorbs green and blue part of the natural light and redirects the red light to human eyes, so it becomes a red apple. By mixing Cyan (C) with Magenta (M) and Yellow (Y) pigments, we can produce a wide range of colors. The more the pigment we add, the lower is the intensity of the light, and thus the darker is the light[6]. This is why it is called the subtractive model. C, M, and Y are the three primitive colors of pigment, which cannot be composed of from other colors. The color printer is a typical application of the subtractive model [5]

C. HSV Color Space

HSV (Hue, Saturation, and Value) – defines a type of color space. It is similar to the modern RGB and CMYK models. The HSV color space has three components: hue, saturation, and value. ‘Value’ is sometimes substituted with ‘brightness’ and then it is known as HSB. The HSV model was created by Alvy Ray Smith in 1978. HSV is also known as the hex-cone color model.

In HSV, hue represents color. In this model, hue is an angle from 0 degrees to 360 degrees.

Saturation indicates the range of gray in the color space. It ranges from 0 to 100%. Sometimes the value is calculated from 0 to 1.

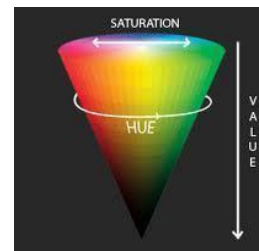


Fig. 2 HSV Color Model

When the value is ‘0,’ the color is gray and when the value is ‘1,’ the color is a primary color. A faded color is due to a lower saturation level, which means the color is grayer [6].

Value is the brightness of the color and varies with color saturation. It ranges from 0 to 100%. When the value is ‘0’ the color space will be totally black. With the increase in the value, the color space brightness up and shows various colors.

D. YCbCr Color Space

YCbCr used widely in video and image compression schemes such as MPEG and JPEG. YCbCr color spaces are defined by a mathematical coordinate transformation from an associated RGB color space. If the underlying RGB color space is absolute, the YCbCr color space is an absolute color space as well; conversely, if the RGB space is ill-defined, so is YCbCr [4].

The YCbCr color space was developed as part of ITU-R BT.601 during the development of a worldwide digital component video standard. YCbCr is a scaled and offset version of the YUV color space. Y is defined to have a nominal 8-bit range of 16– 235; Cb and Cr are defined to have a Nominal range of 16–240.

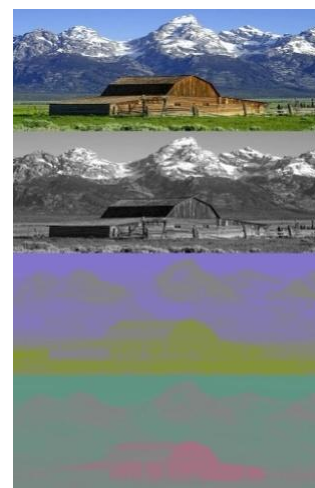


Fig. 3 A color image and its Y, C_B and C_R components

III.CREATION OF VC SHARES IN DIFFERENT COLOR SPACE

Cryptography is a technique to scramble the secret message so that unauthorized users can’t get a meaningful message. In conventional VC Systems, shares are formed as random patterns of the pixel. These shares look like meaningless noise. Noise-like shares do not stimulate the

attention of hackers since it is complex to handle meaningless shares and all shares look alike [2]. In a (2, 2) - threshold color visual secret sharing scheme, let the SI ($X_{(m,n)}$) be of size $m \times n$. We use pixel value of '0' and '1' to represent black and color pixels (RGB) respectively. Naor and Shamir (1994) constructed the pixels of VC shares based on two basis matrices C_0 and C_1 as shown below.

$$C_0 = \{ \text{all the matrices obtained by permuting the columns of } \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{bmatrix} \} \quad (1)$$

$$C_1 = \{ \text{all the matrices obtained by permuting the columns of } \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix} \} \quad (2)$$

where C_0 is used to represent shares of the black pixel and C_1 is used to represent shares of the color pixel [1,7].

A. VC creation using RGB Color space

Every pixel in the image $X_{(m,n)}$ is split into 3 color channels (RGB). Two shares are created for every color channel depending on the intensity of pixel values of each color channel. Each pixel in every color channel is extended into a two 2×2 block to which a color is assigned according to the model presented in Fig. 4, and each block is composed of two black pixels and two color pixels. Fig. 4, depicts the 2×2 blocks created for Red channel. The blocks are combined to form Share1 and Share2 for the red channel. In a similar way Share3 and Share4 for green channel and Share5 and Share6 for the blue channel are created [8]. At the end of the process, six shares are created. The six shares created will look like random dots and will not reveal any information since they have an equal number of black and color pixels. Finally, the shares of RGB, to be exact, the Shares 1, 3 and 5 are merged to form VC share1 and similarly Share2, Share4 and Share6 are merged to form VC share2 as in Fig. 5(b) and 5(c) respectively.

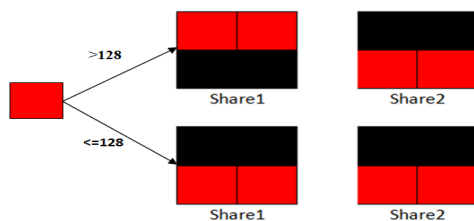


Fig. 4 Share creations for red channel



Fig. 5 (a) Color SI (b) Encrypted VCs hare1 (c) Encrypted VC share2 (d) Decrypted secret

In Fig. 5, the SI (a) is decomposed into two visual cryptography transparencies (b) and (c). When stacking the two transparencies, the reconstructed image (d) is obtained.

Algorithm

Step 1: Read Secret Image that is to be transmitted securely across network

Step 2: Extract RGB components from each pixel in SI

Step 3: Check the pixel value of the red (green/blue) component which ranges from 0 – 255

Step 4: According to the value of pixels, each pixel is replaced with a 2×2 block and create share1 and share2 as shown in Fig. 4

Step 5: Repeat step 3 and step 4 for green and blue colors to create share3, share4, and share5, share6 respectively

Step 6: Shares 1, 3 and 5 are merged to form VC share1 and similarly Share2, Share4 and Share6 are merged to form VC share2

B. VC creation using CMY Color space

In VC, we use sharing images as the decryption tool; that is, the final outputs are transparencies. The subtractive model is more suitable for printing colors on transparencies. RGB and CMY possess the following relationships: $C = 255 - R$, $M = 255 - G$, $Y = 255 - B$; Thus, in the (C, M, Y) representation, (0; 0; 0) represents full white and (255; 255; 255) represents full black[4, 9].

The given RGB image is first converted into CMY image and the algorithm presented in section 3A is used to create the shares as shown in Fig. 6.

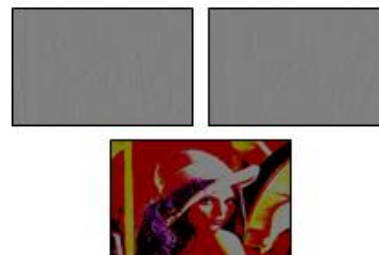


Fig. 6 Encrypted VCs share1 and VC share2 of CMY color space and Decrypted secret

C. VC creation using HSV Color space

Hue represents the color type. It can be described in terms of an angle on the above circle. Although a circle contains 360 degrees of rotation, the hue value is normalized to a range from 0 to 255, with 0 being red. Saturation represents the vibrancy of the color. Its value ranges from 0 to 255. The lower the saturation value, the grayer color is present, causing it to appear faded. The value represents the brightness of the color. It ranges from 0 to 255, with 0 being completely dark and 255 being fully bright. White has an HSV value of 0-255, 0-255, 255. Black has an HSV value of 0-255, 0-255, 0. The dominant description for black and white is the term, value. The hue and saturation level do not make a difference when the value is at max or min intensity level [6].

To create VC shares in HSV color space the same algorithm is used after converting the given secret RGB

image to HSV image using the Matlab function `rgb2hsv` (image) and the shares are created as given in Fig. 7.

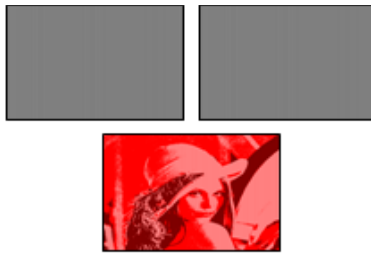


Fig.7 Encrypted VC share1 and VC share2 of HSV color space and Decrypted secret

D. VC creation using YCbCr Color space

The basic equations to convert between 8-bit digital RGB data with a 16–235 nominal range and YCbCr are:

$$Y = 0.299R + 0.587G + 0.114B \quad (3)$$

$$Cb = -0.172R - 0.339G + 0.511B + 128 \quad (4)$$

$$Cr = 0.511R - 0.428G - 0.083B + 128 \quad (5)$$

$$R = Y + 1.371(Cr - 128) \quad (6)$$

$$G = Y - 0.698(Cr - 128) - 0.336(Cb - 128) \quad (7)$$

$$B = Y + 1.732(Cb - 128) \quad (8)$$

To create VC shares in YCbCr color space the same algorithm is used after converting the given secret RGB image to YCbCr image using the Matlab function `rgb2ycbcr` (image) and the shares are created as given in Fig. 8.



Fig. 8 Encrypted VCs hare1 and VC share2 of YCbCr color space and Decrypted secret

IV. RESULTS AND DISCUSSIONS

The proposed VC method in different Color Space has been tested using Matlab on customary color and gray images of size 512 X 512, such as Baboon, Lenna, Peppers, Barbara, and Cameraman. The functioning of all these methods is assessed qualitatively in terms of human visual perception and quantitatively using standard metrics like Peak Signal-to-Noise Ratio (PSNR), Discrete Entropy, and Contrast Improvement Index (CII) to authenticate the quality of the image. The human visual perception of the image shows that the VC shares created using CMY mode looks better and closure to the original image.

A. PSNR

The term Peak Signal-to-Noise Ratio (PSNR) is the ratio between the maximum possible value of a signal and the

power of distorting noise that affects the quality of its representation. Because many signals have a very wide dynamic range, the PSNR is usually expressed in terms of the logarithmic decibel scale. Using the same set of tests images, PSNR is compared scientifically to identify whether a particular algorithm produces better results [10].

The mathematical representation of the PSNR is as follows:

$$PSNR = 20 \log_{10} \left(\frac{MAX_f}{\sqrt{MSE}} \right)$$


























Original Image	VC RGB	VC CMY	VC HSV	VC YCbCr
				
	7.2862	7.0902	5.7642	5.7848
				
	6.8266	6.8905	5.5260	5.5419
				
	6.4613	8.0490	6.6006	6.6282
				
	6.4090	7.1667	5.6856	5.6988
				
	6.2922	7.5117	6.4594	6.4803

Fig. 9 Comparison of PSNR value of decrypted secret in different color space

where the MSE (Mean Squared Error) signifies the average of the squares of the "errors" between the original image and processed image. The error is the quantity by which the values of the actual image differ from the degraded image. It is calculated using the following formula

$$MSE = \frac{1}{mn} \sum_0^{m-1} \sum_0^{n-1} \|f(i,j) - g(i,j)\|^2 \quad (10)$$

where f represents the matrix data of original image, g represents the matrix data of processed image, m represents the numbers of rows of pixels of the images and i represents the index of that row, n represents the number of columns of pixels of the image and j represents the index of that column, MAX_f is the maximum signal value that exists in original image.

Fig. 9 shows the PSNR value of the decrypted VC images in different color spaces compared to the original standard image. In general the PSNR value is low because of pixel expansion of VC shares, where each pixel is replaced with 4 pixels. The VC created using CMY space gives better PSNR value compared to other modes.

B. Average Information Contents (AIC)

E = entropy (I) returns E, a scalar value representing the entropy of grayscale image, where a higher value of Entropy signifies richness of the information in the output image. Entropy is a statistical measure of randomness that can be used to characterize the texture of the input image [11]. The self-information represents the number of bits of information contained in it and the number of bits we should use to encode that message. Larger entropies represent larger average information.

Entropy is defined as:

$$AIC (Entropy) = -\sum_{k=0}^{l-1} P(k) \log P(k) \tag{11}$$

where P(k) is the probability density function of the kth gray level.

TABLE I COMPARISON OF ENTROPY VALUES

Image	RGB	CMYK	HSV	YCbCr
Lenna	0.8615	0.7684	0.9875	0.8141
Baboon	0.8510	0.7852	0.9911	0.8095
Pepers	0.8713	0.7482	0.9608	0.8190
Total	2.5838	2.3018	2.9394	2.4426

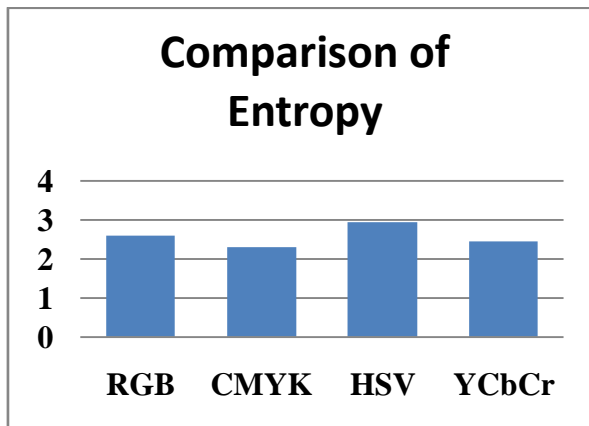


Fig. 10 Comparison of Entropy

A Higher value of the AIC indicates that more information is brought out from the images. A full grayscale image has high entropy, a threshold binary image has low entropy and a single-valued image has zero entropy [11].

Table I presents the entropy values of different VC images. The richness of details in the image is better in HSV and RGB color modes than other techniques and is shown in Fig. 10.

C. Contrast Improvement Index (CII)

The Contrast Improvement Index (CII) is used for evaluation of performance analysis of the proposed algorithm and is defined by

$$CII = C_p / C_o \tag{10}$$

where C_p and C_o are the contrasts for the proposed and original images respectively [12]. Using the tested images a comparative study has been made and the values are given in Table II. The brightness of the image is more if VC shares created using HSV and YCbCr color modes.

TABLE III COMPARISON OF CII VALUES W.R.TO ORIGINAL IMAGE

Image	RGB	CMY	HSV	YCbCr
Lenna	0.7552	0.6281	1.5983	1.0643
Baboon	6.0723	5.2337	13.618	9.4516
Pepers	0.5554	0.4357	1.2639	0.7785

V. CONCLUSION

The main aim of this article is to find out the best color map to be used in conjunction with VC. VC offers a secure way to transfer images on the internet. The advantage of visual cryptography is that it exploits human eyes to decrypt secret images without any computation. Exploiting the possibility of representing images in different modes, VC shares are created for different color modes and compared. The qualitative measurement in terms of human visual perception and PSNR reveals that VC created using CMY color space gives better visibility than other color models. The quantitative measurements like discrete entropy and contrast improvement index shows better result for HSV color model. The traditional RGB color space gives good result both qualitatively and quantitatively. Based on the application, end user can choose the color mode. The proposed study may be extended to enhance the quality of the decrypted secret.

REFERENCES

- [1] M.Naor and A Shamir, —Visual Cryptography], Proceeding of Eurocrypt 94 Lecture Notes in Computer Science, LNCS963: Springer, 1994,
- [2] Ateniese, G., Blundo, C., De Santis, A. and Douglas R. Stinson. ‘Extended capabilities for visual cryptography’, Theoretical Computer Science, Vol. 250, pp. 143-161, 2001.
- [3] Clarke, C.K.P., 1986, Colour Encoding and Decoding Techniques for Line-Locked Sam-pled PAL and NTSC Television Signals, BBC Research Department Report BBC RD1986/2.
- [4] Sharma, G. Digital Color Imaging Handbook. Boca Raton, FL: CRC Press. ISBN 0-8493-0900-X, 2003.
- [5] Y. C. Hou, “Visual cryptography for color images”, Pattern Recognition.,vol. 36, pp. 1619–1629, 2003
- [6] Agoston, Max K.. Computer Graphics and Geometric Modeling: Implementation and Algorithms. London: Springer. pp. 300–306, 2005. ISBN 1-85233-818-0
- [7] InKoo Kang, Gonzalo R Arce, Heung Kyu Lee, “Color Extended Visual Cryptography using Error Diffusion” , IEEE Transactions On Image Processing, VOL. 20, NO. 1, pp.132-145, 2011
- [8] Mary Shanthi Rani, M., Germine Mary, G. and Rosemary Euphrasia, K., ‘Multilevel Multimedia Security by Integrating Visual Cryptography and Steganography Techniques’, in: Muthukrishnan SenthilKumar (Ed.), Computational Intelligence, Cyber Security and Computational Models – Proceedings of ICC3 , Advances in Intelligent Systems and Computing, Vol 412, Springer, Singapore, pp.403-412, 2016
- [9] Bernice Ellen Rogowitz, Thrasyvoulos N Pappas and Scott J Daly (2007). Human Vision and Electronic Imaging XII. SPIE. ISBN 0-8194-6605-0.
- [10] Pooja Kaushik and Yuvraj Sharma, ‘Comparison of Different Image Enhancement Techniques based upon PSNR & MSE’, International Journal of Applied Engineering Research, Vol.7 No.11, pp 1-5. 2012.
- [11] Gonzalez, R.C., Woods, R.E. and Eddins, S.L., ‘Digital Image Processing Using MATLAB’, Second edition, Gatesmark Publishing , 2009.
- [12] Zeng, F. and Liu, I., ‘Contrast enhancement of Mammographic Images using Guided Image Filtering’, in: Tieniu Tan, et al.,(Ed.), Advances in Image and Graphics Technologies, Proceedings of Chinese Conference IGTA 2013, pp.300 – 306, Springer, China, 2013.