

Expressive Color Visual Secret Sharing with Color to Gray & Back and Cosine Transform

Ratnesh N. Chaturvedi*, Sudeep D. Thepade⁺, Swati Ahirrao⁺, Sonali Kothari⁺

**PhD. Research Scholar, Symbiosis Institute of Technology, Symbiosis International University, Pune, India, and
Asst Professor, MPSTME, SVKM's NMIMS, Mumbai, India*

*⁺Professor, Dept. of Computer Engineering, Pimpri Chinchwad College of Engineering, Savitribai Phule Pune
University, Pune, India*

*⁺Asso. Professor, Dept. of Computer Engineering, Symbiosis Institute of Technology, Symbiosis International
University, Pune, India*

*⁺Asst. Professor, Dept. of Computer Engineering, Symbiosis Institute of Technology, Symbiosis International
University, Pune, India*

Received 3rd of March, 2021; accepted 21st of March 2023

Abstract

Color Visual Secret Sharing (VSS) is a basic form of VSS. It is so because nowadays, most people like to share visual data as a color image. There are color VSS schemes capable of dealing with halftone color images or color images with selected colors and natural color images, which regenerate lower quality of the reclaimed secret images. The proposed method deals with a color image in the RGB domain and generates gray shares for color images using color to gray and back through compression. These shares are encrypted into an innocent-looking gray cover image using a Discrete Cosine Transform (DCT) to make meaningful shares. Gray shares are extracted from a relatively innocuous grey cover image and then used to recreate a high-quality color image. Thus, using lower bandwidth for transmission and less storage, the quality of the reclaimed color secret is best obtained using the replication method for resizing compared to linear interpolation in terms of MSE, PSNR and SSIM.

Key Words: Color Visual Cryptography, Color Visual Secret Sharing, Color Image Encryption.

1 Introduction

Data security is a must in present-day data storage and communication environments. Data becomes vulnerable when stored on the device, cloud, or transmitted over the communication channel intruder's attempt to violate and ill-use the data's confidentiality. Cryptography plays an essential role in ensuring the confidentiality of the data stored and transmitted. In cryptography, a readable form of

Correspondence to: ratneshnc@gmail.com

Recommended for acceptance by Angel D. Sappa

<https://doi.org/10.5565/rev/elcvia.1405>

ELCVIA ISSN: 1577-5097

Published by Computer Vision Center / Universitat Autònoma de Barcelona, Barcelona, Spain

data is encrypted to a non-readable form and is stored or transmitted. When cryptography fails, steganography successfully conceals information by embedding it in an untraceable cover object.

There are a plethora of encryption protocols available to ensure confidential data transfer. One of the best-known methods which provide information security is cryptography. Visual Cryptography (VC) is a beautiful encryption method that utilizes human visual intelligence to decrypt secured images. Naor and Shamir proposed VC in 1995 [1], where a secret image divides into multiple parts called shares or transparencies. Each of these 'n' partners receives one of these transparencies. When any 'k' transparencies are stacked where ($k < n$), the original secret becomes visible to the human vision system, and ($k-1$) shares do not disclose any detail of the actual secret. The initial VC methods were limited to binary images only. Verheul and Tilborg first proposed color VC in 1997 [2].

Many other systems, including steganographic systems, biometric security systems, electronic remote voting systems, watermarking systems, and user authentication systems, are proposed to use VC methods.

The key contribution of the method proposed here is:

- Transmitting color secret as gray share.
- Reconstruction of color secret from gray shares
- Reconstruction of color secret from gray shares identical to the original secret with the least difference.
- Lesser data is transmitted over a communication channel and stored while dealing with a gray share for color secrets than existing methods where color shares are generated for a color secret.
- Color secrets are stored and transmitted as meaningful gray shares using Cosine Transform.

This paper overviews the visual cryptographic schemes and compares new color VC techniques. There are five major divisions to this study. Followed by an introduction; Various VC schemes are discussed in Related work, including some of the initial Color VC schemes. Systematically developing the paper's novel approach is the goal of the proposal. The experimental setup describes the tool, data set, and metrics used to gauge performance. The Discussion section analyses the proposed system's performance and comparisons to other colour VSS schemes already in use. Finally, the paper concludes with a conclusion.

2 Related Work

Verheul and Tilborg [2] have created a color VSS with the arch concept where each color pixel distributes into b subpixels of $0, 1, 2, 3, 4, \dots, c-1$ colors. Each subpixel is associated so that when these subpixels are superimposed on each other and held under the light source, if all subpixels are with color ' i ', then color ' i ' is seen else, black color.

Yang and Lai [3] proposed a new color VSS scheme that can be easily implemented due to its new sub-pixel structure and has better block length than color VSS in [2]. A new definition of color subpixel was based on VSS in [1], [4]–[8] for black and white VSS schemes and extended to color VSS schemes. In this scheme [3], the block length ' $b = c \times m$ ', where ' c ' is the number of colors and ' m ' is share size, is used in the binary secret VSS scheme.

Chang et al. [9] developed a VSS scheme to transmit a secret color image. Two color images are randomly selected to conceal the secret image, making them appear to be of normal size. Secret

embedded cover images are known as concealment images. Lookup of the Color Index Table (CIT) embeds the secret into two concealment images. Both the concealment images are stacked to reconstruct the original secret, and the inverse of Lookup CIT is applied.

Hou [10] proposed a VSS which converted color (Red, Green, and Blue) images into CMY (Cyan, Magenta, and Yellow) color images, and then it is halftoned. Each pixel extends to a block of '2x2'. The color allotted is per the table shown in Fig. 1 for Method 1. In the stacked image, unwanted colors are overcome by a half-black and half-white mask so that only desired colors appear. Method 2 expands each halftone CMY image's pixel to a 2x2 block with cyan, magenta, yellow and transparent pixels. The stacked image can generate various colors using these four colors with different permutations, as shown in Fig. 2.

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. 1. Color VSS scheme 1 [10]

Revealed color (C,M,Y)	Share 1	Share 2	Stacked image	Method	Resultant result	Revealed color quantity (C,M,Y)
(0, 0, 0)				Share 1 and Share 2 with the same permutation		(1/4, 1/4, 1/4)
(1, 0, 0)				Swap the position of cyan and transparent		(1/2, 1/4, 1/4)
(0, 1, 0)				Swap the position of magenta and transparent		(1/4, 1/2, 1/4)
(0, 0, 1)				Swap the position of yellow and transparent		(1/4, 1/4, 1/2)
(1, 1, 0)				Swap the position of cyan and magenta		(1/2, 1/2, 1/4)
(0, 1, 1)				Swap the position of yellow and magenta		(1/4, 1/2, 1/2)
(1, 0, 1)				Swap the position of cyan and yellow		(1/2, 1/4, 1/2)
(1, 1, 1)				Swap two positions in pair		(1/2, 1/2, 1/2)

Fig. 2. Color VSS scheme 2 [10]

Lukac and Plataniotis [11] proposed a color VSS by extending conventional VSS in [1], [12] for binary and halftoned images to color VSS using the concept of bit-level-based VSS.

R.Youmaran et al. [13] improved Chang's method [9], which generated a better-quality concealment image. To eliminate the value "0" in pixels, we add "1" to every pixel value, and the most value a pixel may be is 255. When new shares are issued, each '0' is converted to a value of one. Recreating the original secret requires both concealing images and random bit strings.

Shyu [14] proposed a color VSS scheme that followed Yang and Lai's [3] color VSS scheme with additional considerations. Shyu proposes a more striking color VSS method where the pixel expansion is of the order ' $\log_2(c \times m)$ ', where 'm' is the pixel expansion matrix of a conventional binary VSS method.

Heidarinejad et al. [15] proposed an RGB color image VSS that correctly reconstructs the original RGB color secret with reduced size of shares compared to the secret size by using optimal Maximum Distance Separable (MDS) code.

Tsai et al. [16] proposed color VSS which combines a neural network (NN) with Feed-Forward Network (FFN) to generate share. The color cover image conceals these shares. The reconstruction of the original secret requires low computation to materialize it.

F. Lui et al. [17] proposed a color VSS scheme with smaller pixel expansion and the capability to represent all colors. This method has also considered the color darkening phenomenon and does not rely on halftoning for smaller pixel expansion. The reconstruction process does not need computation and can generate extended VSS for the general access structure.

Wu et al. [18] devised a color VSS method for expressive-share using halftoning, cover the coding table (CCT), and secret coding table (SCT). Four techniques applied to this scheme are:

- Color Halftoning: A halftone combines two randomly selected colour cover images and one colour secret.
- Pixel Abstraction: Pixels for an even or odd number of rows are taken from the created color halftone cover and hidden picture, respectively, to decrease the file size of the halftone images.
- Encoding Cover Image: CCT converts the secret halftone image into a cover halftone image, and SCT creates two meaningful shares, share-1 and share-2.
- Decoding Secret: Both the meaningful shares are stacked together to reconstruct the secret.

Yu et al. [19] proposed a modified multi-secret sharing method, significantly improving contrast.

C. C. Chang [20] proposed a scheme on Shape from focus (SFF) which depends on the concept of focused image surface (FIS). This method uses conventional SFF, which fits the surface around the initial approximation.

Qiao et al. [21] proposed halftoned CMY color VSS scheme where share creation takes place using conventional VSS and reconstructing the CMY halftoned secret stack with the appropriate number of shares.

Malik and Sardana in [22] proposed a color VSS scheme with SDS (Sieve, Division, Shuffle) algorithm. Sieve – Split the secret image into its primary color component., Division – Randomly divide the split image as shares. Shuffle – shuffle each share within itself. These shares are randomized and then distributed.

Wang et al. [23] have given an extended multi-secret sharing method that encrypts the variable size of secrets to the exact size of shares.

Kumar and Srivastava [24] proposed a technique that is a combination of VSS and key safeguarding techniques. Combining a random image with a secret image and then deforming both before reconstructing the secret image with the reformation approach yields a key image.

K Rajput [25] proposed a color image scheme using an Extended Visual Secret Sharing (EVSS) scheme for a recovered image with better contrast. Shares are generated by bit-level encoding for R, G,

and B components using EVSS. The combination of the shares of each component R, G, and B does reconstruction.

Karolin and Meyyapan [26] proposed a scheme that transforms the 256 color code image into 16 color code images using the Floyd Steinberg method. Share creation for 16 color code images using XOR-based VSS and reconstruction by stacking the shares.

Shiny et al. [27] proposed a tagged color VSS. Conventional VSS scheme generates shares. They are tagged with tag patterns using probabilistic VSS to get tagged shares and a color secret reconstruction by superimposing the shares.

Pahuja and Kasana [28] proposed a VSS using Floyd and Steinberg's error diffusion for color VSS which deals with color halftone images.

Sathishkumar and Sudha [29] devised a Two In One Image Secret Sharing scheme (TiOISSS) using Adaptive Halftoning for meaningful color shares with perfect regeneration of color secrets.

Using bit-level decomposition, Chaturvedi et al. [30] proposed an RBG Color VSS scheme for meaningless shares. Employing the information of pixel expansion employed during the encoding of meaningless shares to denoise and resize the reconstructed noiseless share to its original size. The original secret reconstruction with "zero" mean squared error (MSE), "infinite" peak signal-to-noise ratio (PSNR), and "1" structural similarity index measure (SSIM) in the Proposed system.

Various color VSS schemes deal with CMY, RGB, and Color Halftone Images for which the distributed shares are color shares. The proposed VSS scheme has a different approach to secret color images. Distribution of color secrets as meaningful gray shares and reconstruction of color secrets using gray shares of acceptable visual quality during reconstruction. Distributing color secrets as gray shares minimizes the data stored and transmitted over the network. The proposed system converts a 24-bit color image to 16-bit gray, generates meaningless gray shares using bit-level encoding, and normalizes [31] the shares with pixel values ranging from 0-255 to 0-1 to reduce the embedding error. These shares are then embedded into a 16-bit gray cover image in the transform domain using Discrete Cosine Transform by exploiting 37.5% of high-frequency data in the cover image resulting in meaningful gray shares. During the reconstruction phase, shares are extracted from the meaningful shares in the transform domain and de-normalized by expanding the pixel range of 0-1 to 0-255. These shares are superimposed to reconstruct a 16-bit gray secret image. This 16-bit gray secret converts to a 24-bit color secret image using inverse Color to Gray & Back.

2.1 Color to Gray and Back

Fig. 3 shows the conversion of Color-to-Gray and Back. 24-bit RGB decomposes to R, G, and B components. Consider the five most significant bits (MSB) per color component, resulting in 15-bit to construct a 16-bit gray image, and the 16th bit is assumed to be "zero". While reconstructing the 24bit color image back, the first 5-bits of the gray image go to the first 5 MSB bits of the R-component, the next 5-bits of the gray image go to 5 MSB bits of the G-component, and the last 5-bits of the gray image go to 5 MSB bits of B-component. Furthermore, pad the last three bits of R, G, and B components with "zeros". Furthermore, reconstruct the 24-bit color image. Using Color to Gray and black, the variation between the original pixel in the secret image and the reconstructed pixel would be a minimum, 'zero' if the last 3 LSBs (Least Significant Bit) are "zero" in the original image and the maximum it would be "7" if the last 3 LSB's are "1" in the original image.

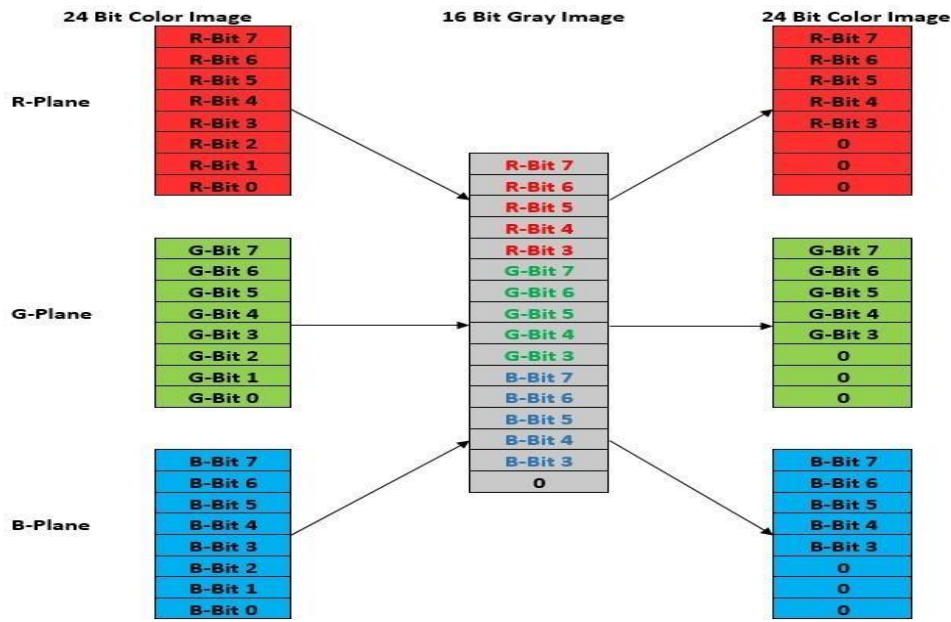


Fig. 3. Color to Gray and Back

2.2 Gray Share Creation

The meaningful share creation process shown in Fig. 4 is:

- Convert 24-bit color image to 16-bit gray image using Color to Gray and Back to reduce the amount of secrets stored and transmitted over a communication channel.
- Generate shares of a 16-bit image using bit-level encoding.
- Shares are normalized and embedded into an innocent-looking gray cover image using Discrete Cosine Transform by exploiting 62.5 % of the High-Frequency region so that the secret shares a look-alike cover image, which is entirely meaningful.
- These innocent-looking meaningful shares are then stored and transmitted over a communication channel to raise the least qualm to the attacker.

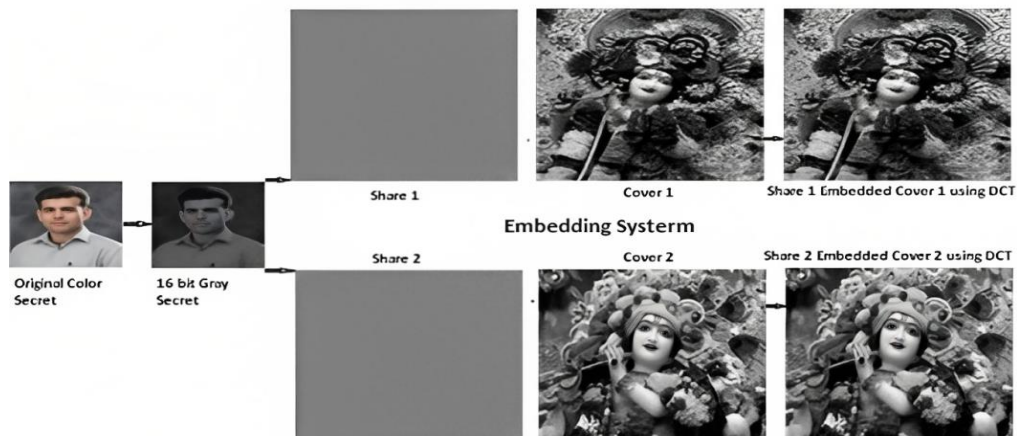


Fig. 4. Gray Shares creation for Color Secret Image in Proposed Color VSS Method

2.3 Color Secret Reconstruction

Reconstruction of a secret color image shown in Fig. 5 is:

- Secret Shares are extracted from the innocent-looking meaningful shares using Discrete Cosine Transform and de-normalized.
- Overlay these shares are using OR logic to retrieve the original gray secret with noise introduced in it.
- Using the knowledge of pixel expansion retrieved secret is de-noised and resized to its original size as in [30] using Method 1 (Linear Interpolation) and Method 2 (Replication).
- Finally, convert 16-bit gray secrets to a 24-bit color secret.

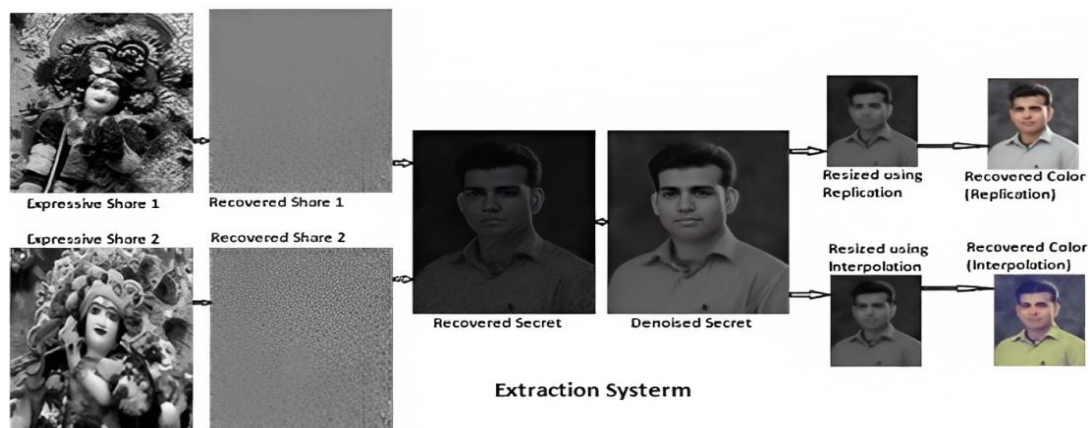


Fig. 5 Color Secret image reconstruction from Gray Shares in Proposed Color Visual Secret Sharing Method

3 Experimental Environment

MATLAB as a tool carried out the entire experimentation. The experiment employs Wang's 1000 pictures database, which splits over 10 categories with 100 images per category. In Fig. 6, we see an example of a database of hidden images with 5 examples per category. Figure 7 depicts the cover photos utilized in the creation of relevant shares.

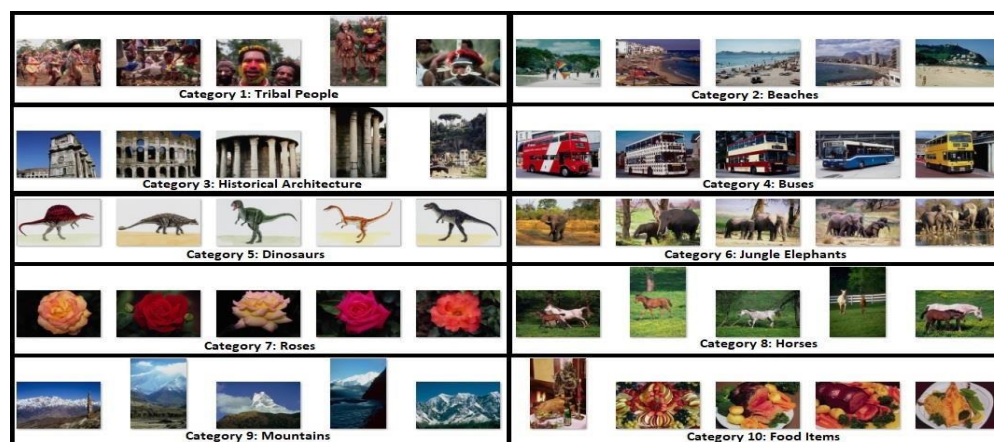


Fig. 6. Sample images from the Wang image dataset [32]



Cover Image 1



Cover Image 2

Fig. 7 Secret Embedding Cover Images

4 Quality Assessment

Commonly used metrics for evaluating image quality include mean squared error (MSE) and peak-to-average noise ratio (PSNR) due to their ease of calculation, transparency of physical meaning, and amenability to mathematical implementation in optimization. The structured similarity indexing method (SSIM) provides a normalized mean value of structural similarity between the two images, which evaluates visual quality.

Mean Squared Error (MSE), Peak Signal Noise Ratio (PSNR), and Structural Similarity Index (SSIM) assess the quality of the restored color secret concerning the original color secret.

MSE is a metric of quality that is always non-negative. A value closer to '0' indicates an improved quality of the restored secret and vice versa. Equation (1) represents MSE

$$MSE = \frac{1}{MN} \sum_{y=1}^M \sum_{x=1}^N [I(x, y) - I'(x, y)]^2 \quad (1)$$

Where: $I(x,y)$ = original secret, $I'(x,y)$ = restored secret, M and N are the dimensions of the secret image

PSNR is a measure of peak noise. This 'signal' is the original secret image, and the 'noise' is the error in the reconstructed secret image. Equation (2) represented PSNR.

$$PSNR = 20 \times \log\left(\frac{MAX_I}{\sqrt{MSE}}\right) \quad (2)$$

Where: MAX_I is the maximum possible pixel value of the image =255

SSIM calculates the subjective dissimilarity of two images. It's a subjective metric for quantifying the decline in perceived image quality due to post-processing. In this test, the pair of images represents a rebuilt secret, and it is compared to the original secret to see whether there are any structural similarities. SSIM takes the least value of '0', indicating no visual similarity between the original and restored secret images. The maximum value of '1' indicates that the two images are visually identical. Equation (3) represents SSIM.

$$SSIM(x, y) = \frac{(2\mu_x\mu_y+c_1)(2\sigma_{xy}+c_2)}{(\mu_x^2+\mu_y^2+c_1)(\sigma_x^2+\sigma_y^2+c_2)} \quad (3)$$

where: μ_x = average of x_i μ_y = average of y_i

σ_x^2 = variance of x , σ_y^2 = variance of y , σ_{xy} = covariance of x and y
 $c_1 = (k_1L)^2$, $c_2 = (k_2L)^2$ variables to stabilize the division with weak denominator
 L = dynamic range of the pixel values ($2^{\text{bits per pixel}} - 1$) $k_1 = 0.01$ and $k_2 = 0.03$ by default

5 Results and Discussion

The experiment employs Wang's image database [32] of a color image of 1000 images, 100 images of each category. Fig 8. Shows Examples of color secrets converted to gray secrets and transformed into meaningful share and the regeneration of the original color secret from the reconstructed gray secret.



















Original Color Secret (24 Bit)	Converted Original Gray Secret (16 Bit)	Expressive Share1 (512 x 512)	Expressive Share 2 (512 x 512)	Reconstructed Gray Secret (Replication)	Regenerated Color Secret (Replication)
 (384 x 256)					 (384 x 256)
 (256 x 384)					 (256 x 384)
 (256 x 384)					 (256 x 384)

Fig. 8. Examples of Secrets from Wang Dataset getting conveyed in expressive shares using the proposed VSS technique and reconstructed from these shares.

The experimentation shows the MSE, PSNR and SSIM between the original secret and the reconstructed secret, which resizes using linear interpolation and replication methods for each secret category, as in Table 1. It shows that the method using the replication method gives minimum MSE. PSNR is inversely proportional to MSE. Bigger values of MSE in Table 1, using linear interpolation, correspond to smaller values of PSNR. For smaller values of MSE in Table for Replication, bigger values of PSNR are calculated for each category of a secret image. Table 1 shows that the PSNR using replication is more than the linear interpolation method. SSIM evaluate the perception variation between the original and reconstructed secrets resized using linear interpolation and replication.

Table1 shows that the SSIM for all the category secrets is low for reconstructed secrets using linear interpolation compared to the replication method. So, from Table 1, it is easily noticeable that the structural similarity between the recovered secret resized using replication is more with the original secret when compared with the recovered secret resized using linear interpolation.

Table 1. MSE, PSNR, and SSIM between the original secret and reconstructed secret resized using linear interpolation & replication in the proposed color VSS method.

Image Category	MSE		PSNR		SSIM	
	Linear Interpolation	Replication	Linear Interpolation	Replication	Linear Interpolation	Replication
1: Tribal People	10214.28	17.31	8.1147	35.7498	0.0129	0.8994
2: Beaches	7624.78	17.39	9.3945	35.7293	0.0111	0.8001
3: Historical Architecture.	9758.36	17.39	8.3353	35.7349	0.0151	0.7978
4: Buses	11294.72	16.96	7.6509	35.8396	0.0088	0.8621
5: Dinosaurs	9529.35	17.58	8.5148	35.7938	0.131	0.6027
6: Jungle Elephants	8751.25	17.39	8.7445	35.7287	0.0076	0.8746
7: Roses	11618.17	17.46	7.7353	35.7211	0.0077	0.6153
8: Horses	9507.44	17.21	8.4256	35.7738	0.005	0.9453
9: Mountains	9041.93	17.29	8.7471	35.7553	0.0107	0.7861
10: Food Items	10984.49	17.18	7.7984	35.789	0.0114	0.8648
<i>Average Values</i>	<i>9832.48</i>	<i>17.31</i>	<i>8.3461</i>	<i>35.7615</i>	<i>0.0221</i>	<i>0.8048</i>

Table 2 summarizes the analysis of various color VSS concerning the type of shares in terms of Meaningful or Meaningless shares, the number of bit-planes in color shares, the size of the reconstructed secret, and the color secret transmitted as color or gray shares. The table shows that for sharing color secrets, some existing systems share 'Meaningful shares' and some share 'Meaningless shares', which are 24-bit shares with reconstructed secret quality as High, Medium and Low, but in the proposed system using replication. Meaningful shares are 16-bit shares with a high-quality reconstructed secret. Also, it is evident that the existing systems share the color secret only as color shares and can reconstruct the shares of the same size or greater than the original secret. However, in the proposed system, all the color secrets are transmitted as gray shares capable of reconstructing same-size shares.

Table 2. Analysis of various color visual secret-sharing schemes

	Type of Share Meaningful/ Meaningless	Number of bit-plane in shares of color image	Quality of Reconstructed Secret	Size of Reconstructed Secret w.r.t Original Secret	Color Secret Transmitted as Color shares or Gray Shares
Proposed Method (Replication)	Meaningful	16	High	Same	Gray
Proposed Method (Interpolation)	Meaningful	16	Low	Same	Gray
Young-Chang Hou [10]	Meaningless	24	Medium	Greater	Color
Lukac and Plataniotis [11]	Meaningless	24	High	Same	Color
R.Youmaran et al. [13]	Meaningful	24	High	Same	Color
Shyong Jian Shyu[14]	Meaningless	24	Medium	Greater	Color
<i>M.Heidarinejad et al.</i> [15]	Meaningless	24	High	Same	Color
Tsai et al. [16]	Meaningful	24	High	Same	Color
Wu et al. [18]	Meaningful	24	Low	Greater	Color
Chang et al. [20]	Meaningless	24	High	Same	Color
Qiao et al. [21]	Meaningless	24	Low	Greater	Color
Malik et al. [22]	Meaningless	24	Very Low	Greater	Color
Aarti and Pushpendra [25]	Meaningful	24	High	Greater	Color
M.Karolin1 and T.Meyyapan [26]	Meaningless	24	Medium	Greater	Color
R.Shiny et al. [27]	Meaningless	24	Very Low	Same	Color
Shivani and Singara [28]	Meaningless	24	Medium	Greater	Color
R.Sathishkumar and GF Sudha [29]	Meaningless	24	Medium	Greater	Color
Ratnesh et al.[30]	Meaningless	24	High	Same	Color

6 Conclusion

This paper has proposed a unique way of color visual secret sharing with a better-quality reconstructed secret that looks almost identical to the original secret without any noise. The proposed method converts the color secret to gray secret using a lossy method with a minimum loss, where the

minimum loss in each pixel value is '0' and the maximum loss in each pixel value is '7'. Shares are generated of this gray secret and embedded into innocent-looking cover images using DCT. The visual quality of the regenerated color secret is almost identical to the original secret. This conversion of a color secret to a gray secret helps minimize the storage, and less data transmits over the network. To evaluate the performance of the proposed systems, MSE, PSNR, and SSIM between the original secret and reconstructed secret resized using linear interpolation and replication are calculated. Compared with a reconstructed secret using a replication method, the original secret gives minimum MSE, maximum PSNR, and SSIM closer to '1' compared to the reconstructed secret resized using linear interpolation. And the process of Color to Gray and Back also gives an extra capability of hiding the color information of color secret, which needs an extra step of inverse color to gray and back to reveal the color. Existing systems share 'Meaningful shares' and 'Meaningless shares,' which are 24-bit shares with reconstructed secret quality of High, Medium, and Low, respectively.

In contrast, the proposed replication system shares Meaningful shares, 16-bit shares with a high-quality reconstructed secret. Furthermore, present systems only exchange the color secret as color shares and may rebuild shares of the same or higher size than the original secret. However, all color secrets send as gray shares capable of reconstructing same-size shares in the proposed system.

References

- [1] M. Naor and A. Shamir, "Visual cryptography", De Santis, A. (eds) *Advances in Cryptology — EUROCRYPT'94. Lecture Notes in Computer Science*, vol 950. Springer, Berlin, Heidelberg, 1994. <https://doi.org/10.1007/BFb0053419>
- [2] E. R. Verheul and H. C. A. Van Tilborg, "Constructions and Properties of k out of n Visual Secret Sharing Schemes," *Des. Codes, Cryptogr.*, 1997, doi: 10.1023/A:1008280705142. <https://doi.org/10.1023/A:1008280705142>
- [3] C. N. Yang and C. S. Lai, "New Colored Visual Secret Sharing Schemes," *Des. Codes, Cryptogr.*, 2000, doi: 10.1023/A:1008382327051. <https://doi.org/10.1023/A:1008382327051>
- [4] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, "Constructions and bounds for visual cryptography," 1996. https://doi.org/10.1007/3-540-61440-0_147
- [5] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, "Visual Cryptography for General Access Structures," *Inf. Comput.*, 1996. <https://doi.org/10.1006/inco.1996.0076>
- [6] S. Droste, "New results on visual cryptography," in *CRYPTO'96*, 1996, vol. 1109, pp. 401-415, Springer-Verlag LNCS. https://doi.org/10.1007/3-540-68697-5_30
- [7] K. Kobara and H. Imai, "Limiting the visible space visual secret sharing schemes and their application to human identification," 1996. <https://doi.org/10.1007/BFb0034846>
- [8] M. Naor and A. Shamir, "Visual cryptography II: Improving the contrast via the cover base," 1997. https://doi.org/10.1007/3-540-62494-5_18
- [9] C. Chang, C. Tsai, and T. Chen, "A new scheme for sharing secret color images in computer network," *Parallel Distrib.*, pp. 21–27, 2000. <https://doi.org/10.1109/ICPADS.2000.857679>
- [10] Y.-C. Hou, "Visual cryptography for color images," *Pattern Recognit.*, vol. 36, no. 7, pp. 1619–1629, 2003. [https://doi.org/10.1016/S0031-3203\(02\)00258-3](https://doi.org/10.1016/S0031-3203(02)00258-3)
- [11] R. Lukac and K. N. Plataniotis, "Bit-level based secret sharing for image encryption," *Pattern Recognit.*, 2005. <https://doi.org/10.1016/j.patcog.2004.11.010>

- [12] C. C. Lin and W. H. Tsai, "Visual cryptography for gray-level images by dithering techniques," *Pattern Recognit. Lett.*, 2003. [https://doi.org/10.1016/S0167-8655\(02\)00259-3](https://doi.org/10.1016/S0167-8655(02)00259-3)
- [13] B. Symposium, "AN IMPROVED VISUAL CRYPTOGRAPHY SCHEME FOR SECRET HIDING R . Youmaran, A . Adler, A . Miri School of Information Technology and Engineering (SITE), University of Ottawa, Ontario, Canada," pp. 340–343, 2006.
- [14] S. J. Shyu, "Efficient visual secret sharing scheme for color images," *Pattern Recognition*, 2006. <https://doi.org/10.1016/j.patcog.2005.06.010>
- [15] M. Heidarinejad, A. A. Yazdi, K. N. Plataniotis, and O. Ms, "ALGEBRAIC VISUAL CRYPTOGRAPHY SCHEME FOR COLOR IMAGES" The Edward S . Rogers Sr . Department of ECE, University of Toronto, 10 King's College Road, Department of CE, Sharif University of Technology, P . O . Box 11155-9517, Tehran, Iran," pp. 1761–1764, 2008.
- [16] D. S. Tsai, G. Horng, T. H. Chen, and Y. Te Huang, "A novel secret image sharing scheme for true-color images with size constraint," *Inf. Sci. (NY)*, vol. 179, no. 19, pp. 3247–3254, 2009. <https://doi.org/10.1016/j.ins.2009.05.020>
- [17] X. J. L. F. Liu¹, C.K. Wu, "When AES Blinks," *IET Inf. Secur.*, vol. 2, no. 2, pp. 28–32, 2008. <https://doi.org/10.1049/iet-ifs:20070078>
- [18] H. C. Wu, H. C. Wang, and R. W. Yu, "Color visual cryptography scheme using meaningful shares," *Proc. - 8th Int. Conf. Intell. Syst. Des. Appl. ISDA 2008*, vol. 3, pp. 173–178, 2008. <https://doi.org/10.1109/ISDA.2008.130>
- [19] B. Yu, G. Shen, and Z. X. Fu, "A lossless multi-secret sharing visual cryptography scheme," *Dianzi Yu Xinxu Xuebao/Journal Electron. Inf. Technol.*, vol. 34, no. 12, pp. 2885–2890, 2012. <https://doi.org/10.3724/SP.J.1146.2012.00300>
- [20] C. C. Chang, C. C. Lin, T. H. N. Le, and H. B. Le, "Self-verifying visual secret sharing using error diffusion and interpolation techniques," *IEEE Trans. Inf. Forensics Secur.*, vol. 4, no. 4, pp. 790–801, 2009. <https://doi.org/10.1109/TIFS.2009.2034203>
- [21] W. Qiao, H. Yin, and H. Liang, "A kind of visual cryptography scheme for color images based on halftone technique," *2009 Int. Conf. Meas. Technol. Mechatronics Autom. ICMTMA 2009*, vol. 1, pp. 393–395, 2009. <https://doi.org/10.1109/ICMTMA.2009.294>
- [22] S. Malik and A. Sardana, "A Keyless Approach to Image Encryption," *2012 Int. Conf. Commun. Syst. Netw. Technol.*, vol. 4, no. 5, pp. 879–883, 2012. <https://doi.org/10.1109/CSNT.2012.189>
- [23] H. Wang, M. He, X. Li. An Extended Multi-secret Images Sharing Scheme Based on Boolean Operation. *1st International Conference on Information and Communication Technology (ICT-EurAsia)*, Mar 2013, Yogyakarta, Indonesia. pp.513-518. https://doi.org/10.1007/978-3-642-36818-9_59
- [24] H. Kumar and A. Srivastava, "A secret sharing scheme for secure transmission of color images," *Proc. 2014 Int. Conf. Issues Challenges Intell. Comput. Tech. ICICT 2014*, pp. 857–860, 2014, <https://doi.org/10.1109/ICICT.2014.6781393>
- [25] P. K Rajput, "An EVCS for Color Images with Real Size Image Recovery and Ideal Contrast Using Bit Plane Encoding," *Int. J. Comput. Netw. Inf. Secur.*, vol. 6, no. 2, pp. 54–60, 2014, <https://doi.org/10.5815/ijcnis.2014.02.08>

- [26] M. Karolin and T. Meyyapan, "RGB Based Secret Sharing Scheme in Color Visual Cryptography," *Int. J. Adv. Res. Comput. Commun. Eng.*, vol. 4, no. 7, pp. 151–155, 2015. <https://doi.org/10.17148/IJARCCCE.2015.4734>.
- [27] R. M. Shiny, P. Jayalakshmi, A. Rajakrishnammal, T. Sivaprabha, and R. Abirami, "An efficient tagged visual cryptography for color images," 2017, <https://doi.org/10.1109/ICCIC.2016.7919685>
- [28] S. Pahuja and S. S. Kasana, "Halftone visual cryptography for color images," *2017 Int. Conf. Comput. Commun. Electron. COMPTELIX 2017*, pp. 281–285, 2017. <https://doi.org/10.1109/COMPTELIX.2017.8003979>
- [29] R. Sathishkumar and G. F. Sudha, "Authenticated color extended visual cryptography with perfect reconstruction," *Proc. 2017 IEEE Int. Conf. Commun. Signal Process. ICCSP 2017*, vol. 2018-Janua, pp. 609–615, 2018, <https://doi.org/10.1109/ICCSP.2017.8286430>
- [30] R. N. Chaturvedi, S. D. Thepade, and S. N. Ahirrao, "Quality Enhancement of Visual Cryptography for Secret Sharing of Binary, Gray and Color Images," *Proc. - 2018 4th Int. Conf. Comput. Commun. Control Autom. ICCUBEA 2018*, pp. 1–6, 2018. <https://doi.org/10.1109/ICCUBEA.2018.8697870>
- [31] H. B. Kekre, S. D. Thepade, and R. N. Chaturvedi, "*Color to gray and back*" using DST-DCT, Haar-DCT, Walsh-DCT, Hartley-DCT, Slant-DCT, Kekre-DCT hybrid wavelet transforms, vol. 259. 2014. https://doi.org/10.1007/978-81-322-1768-8_54
- [32] Wang's image database: <http://wang.ist.psu.edu/~jwang/test1.tar> (Downloaded on May 2019)