INDIAN JOURNAL OF SCIENCE AND TECHNOLOGY

RESEARCH ARTICLE

Half-Tone Visual Cryptography Scheme For RGB Color Images

D R Somwanshi[1]*, Vikas T Humbe[2]

1 Assistant Professor, Department of Computer Science, College of Computer Science and Information Technology (COCSIT), Latur, Maharashtra, India
2 Associate Professor, School of Technology, Swami Ramanand Teerth Marathwada University Nanded, Sub-Center, Latur, Maharashtra, India

OPEN ACCESS

Received: 16-10-2022
Accepted: 08-01-2023
Published: 07-02-2023

Citation: Somwanshi DR, Humbe VT (2023) Half-Tone Visual Cryptography Scheme For RGB Color Images. Indian Journal of Science and Technology 16(5): 357-366. https://doi.org/10.17485/IJST/v16i5.2038

* **Corresponding author**.

somwanshi1234@gmail.com

Funding: None

Competing Interests: None

Published By Indian Society for Education and Environment (iSee)

ISSN
Print: 0974-6846
Electronic: 0974-5645

Abstract

Objectives: Currently used visual-cryptography methods which use binary and gray-level images have some shortcomings such as large pixel expansion, poor visual quality of the reconstructed image, etc. Further modifications in visual-cryptography methods are required to provide error-free and better results. It has been observed that the use of color images is more convenient and accurate in approach. **Method:** This research study presents a new and optimal scheme for the visual-cryptography which is centered on RGB color images. Jarvis halftoning is applied on each decomposed color channel that is used in share generation. A special code matrix is defined for the generation of color shares and the optimal reconstruction of the original image. The method is tested with color images of different sizes, no specific dataset is required. Pixel Expansion, The Aspect Ratio, and Contrast of the method is compared with the existing method, and found more enhanced result. **Findings:** The scheme projected eliminates the problems of large pixel expansion and poor visual quality in the reconstructed images. The performance of the method is tested with the different statistical measures and values obtained as Mean Square Error (MSE):0, Peak- Signal-to-Noise-Ratio (PSNR): ∞, Universal Index Quality (UIQ):1, etc. This means that the original image is completely recovered with good contrast. **Novelty**: Color images of varied sizes and channels can be processed by applying the Jarvis half-toning technique through the codebook calculated to abolish the problems of pixel expansion and to improve the superiority of the renovated image.

Keywords: Color HalfTone Images; Error Diffusion; Optimal Contrast; Secret and Secure Sharing Scheme; Expansion of Pixels

1 Introduction

The idea and design of the secret-sharing method of visual cryptography is represented below in Figure 1. The secret image information that needs to be secured is distributed into two components called here to share 1 and share 2 and the superimposition of these two shares produces the secret image information. The important property of this technique is that a human-visual system can operate staking of shares or decryption

of shares if shares are printed on the transparencies and which does not require any computation.

Naor M. and Shamir A (1994). generalized a basic scheme for secret sharing into (k of n) or k from n scheme of visual-cryptography[1]. In this type of scheme, the secret original image has been distributed into different n shares, then those will be given to n different participants. A minimum k of those n participants have to provide their share for revealing the required secret image. The image reconstructed from this method is having poor contrast and pixel-expansion is increased by double which means the image size is into two (Image-Size X 2).

To intensify the results and to increase and improve the security of this scheme G. Ateniese et.al. (1996) further modified the (k, n) model of secrete sharing to the general-access model[2].

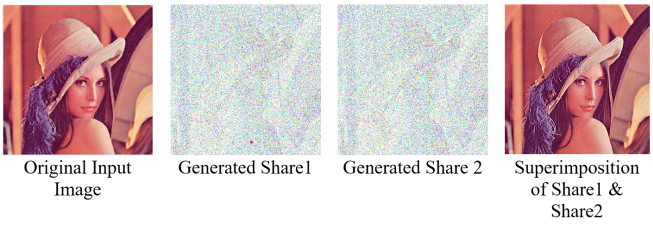

Fig 1. The Idea and Design of the Visual Cryptography

According to them, the n shares are created and split up into two parts or subsets as per the need and importance. Among the two parts, the first part is referred to as the qualified subset and the second part is called the forbidden subset. Any k number of shares from a qualified subset can produce the required secret image information, but any k number or even more than k shares from the forbidden subset cannot produce the original image information that is hidden inside the shares. Again to maintain the good contrast and improve security, Zhi Zhou, et.al. (2006) proposed a novel method called half-tone visual cryptography[3]. The specialty of this secret-sharing process of visual cryptography is that the pixels of the binary image are divided into an array of sub-pixels, which are called half-tone cells, in all the n-shares. Mahmoud E. Hodeish et.al (2018) recommended an improved half-tone scheme of visual cryptography that works by adding the error diffusion mechanism. They work on binary and grayscale images and improve the expansion of pixels by defining the elements of the code matrices, but they only work on binary halftone images[4].

Chang-Chou Lin et.al. (2003) suggested one more scheme which is especially for the gray images[5]. The scheme introduced by them uses the technique called dithering for the conversion of a grayscale image into the required image type and the approximate binary image. Then they applied existing techniques of VC that are available for binary images for producing the different shares.

Again to decrease the problem of pixel expansion the scheme Vikas Humbe and I (2021)[6] presented a new scheme for processing color images. In that scheme, we proposed the techniques for the color image depiction in which the method separates the color channels: Red(R), Green (G), and Blue (B). Each color channel is then used for the creation of two shares using a verification image. LSB Based Image Steganography is also used for creating meaningful shares but the problem with this scheme was only two shares are possible.

To enhance the existing scheme for color image processing Anli Sherine et. al. (2022)[7] proposed a technique that uses CMY (cyan-magenta-yellow) color space. They have used color channel decomposition and error diffusion methods for share generations. The four shares they have created as cyan, magenta, then yellow, and mask. The mask is used as random, to randomly generate the pixels half white and half black in a block. Here every share is needed for reconstructing the required image. After that, they used the OCR (optical character recognition) to recognize the secret image message. Again creating more than four shares using this proposed technique is difficult and OCR needs to use which means the original theme of VC is not maintained.

Arvind Choudhary et. al. (2022)[8] proposed a new scheme that uses Competitive-Swarm-Improved Invasive-Weed-Optimization (CSIIWO) algorithms to provide security to generated shares, initially they used grayscale images for creating and superimposition of shares. Encryption and decryption keys are produced using the proposed CSIIWO) algorithms to keep the confidentiality of information among multiple users involved in the application. Their method achieved good performance of the different statistical measures such as the extreme Peak-Signal-to-Noise-Ratio (PSNR) is approximately 40.749 dB, minimum-conditional-privacy-loss is 0.508, and the maximum entropy is 7.987, etc. The method they have proposed protects the numerous data sharing and has some advantages as compared with preceding methods. Again there is scope for using color image processing and improving the standards of statistical measures that are used in their study.

Efe Çiftci and Emre Sümer (2022)[9] suggested one more novel method that is based on steganography and suitable for hiding plaintext information in a halftone image. The method proposed by them is recycled to distribute the secret information into multiple output halftone images that provide better security. The result obtained by their method proves that is the most secure and that is used to hide large consignment information. Again this is not the visual cryptographic method, it is only the steganography method.

While producing and reconstructing a secrete image from the different shares, problems such as the expansion of the pixels, improper alignment of the shares, requirements of extensive code matrices, flipping issues in shares, and distortion of shares, etc. are arises [4, 5, 6, and 7]. Pixel expansion refers to the increasing number of pixels in the shares, due to the size of share increases and alignment problems may occur. Due to the improper alignment of the shares, the combined secret image looks different. If the image generated is not restructured in the proper direction flipping issue may arise. With this, several of the past secret-sharing methods presented are established on binary (black-and-white) images and very few of them are established on gray and color-secrete images. This research study handles color-secrete image processing with color component decomposition and the half-toning technique. The method proposed also eliminated all the problems discussed above, especially problems of expansion of the pixels that is reduced to 100% and the method produces the optimum contrast of the reassembled image. All these are achieved by designing the code matrices for generating the shares. The authenticity of this method proposed is compared using different statistical measures and by performing a comparison with the previously known methods.

2 Methodology

2.1 Preliminary concepts

2.1.1 Color channel decomposition techniques

This paper uses an RGB color channel, a secret RGB image that needs to be encoded or encrypted and is decomposed or divided into R(Red), G(Green), and B(Blue) component images. For each component's image, there will be four shares created and finally, shares are concatenated to form RGB shares.

2.1.2 HVC scheme and Error Diffusion

This proposed method converts each component's image into a half-tone image, Half-tone is generally an image, generally created with a series of dots instead of a continuous tone. These dots can be of varying sizes, shapes, and colors. Smaller dots from an image are taken for representing a lighter area of the image and larger dots are taken for representing a dense area of the image. Such a scheme is called Half-tone Visual Cryptography (i.e. in short HVC)[3]. Each color component image represented here can be a separate gray component image. Error diffusion technique is the procedure of converting an image in gray level (color components image) to binary image form in a manner that the picture in binary image form looks similar to the gray image with a somewhat better quality image. This is the simplicity and effectiveness of the binary image. The procedure of error diffusion diffuses or minimizes the error in the binary image. For error diffusion at each pixel's level, the error called quantization-error is filtered and then feedback to the input is given. The error filter process diffuses quantization-error, one pixel away from each neighboring gray level pixel. In nature, the error diffusion noise is of high frequency or blue noise, and for human vision; it can provide pleasing half-tone images[4–6].

Figure 2 represents how Jarvis's error diffusion matrix of distributed error fraction of 12 pixels works. If the address of the pixel that is being processed is (1, 4) then the error distributed to the neighboring pixel is represented in figure 2 as 8/42, 4/42, 2, 42, etc.

2.1.3 Code Matrix

For the simulation of a method proposed, we develop the code block for each half-tone color component of the RGB secrete image. So codes for black pixels and the codes for white pixels in each halftone image used for the preparation of four different shares are represented in Figure 3.

2.2 Proposed Algorithm

Original RGB color secretes image i.e. is taken as input, is first decomposed/converted into R(Red), G(Green), and B(Blue) components image, then each component's image is then converted into halftone image using Jarvis halftone algorithm. For each halftone image, four shares are generated using code blocks presented in Figure 3 and using Algorithms 1 developed, and that is presented in Table 1. Code matrices are constructed from the code matrix of Mahmoud E. Hodeish and et. al[4]. In this research work proposed, four shares are created and all are needed for the regeneration of the required image that is

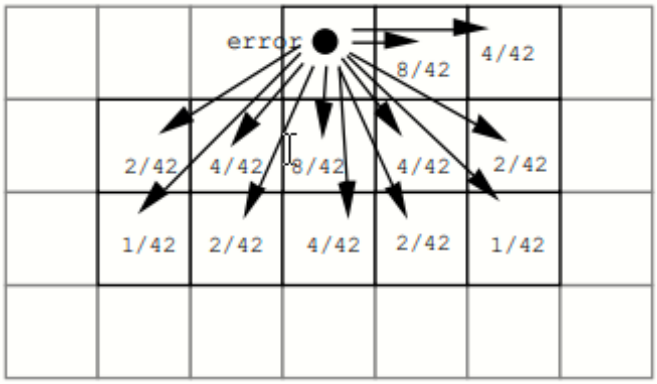

Fig 2. Jarvis error Diffusion Matrix

distributed in shares, and also focused on the generation of only four shares. So the code block and algorithms are designed only for four shares, but any even number of shares, as per the requirement can be generated by designing the code block. Generated halftone shares are again concatenated to one another to form four RGB shares, then these four RGB shares are circulated among four participants.

For superimposition and reconstruction of the original information image again four RGB shares need to convert into R, G, and B components images then into a binary image. Finally, XOR operations need to perform on the shares, to combine all four shares, to construct an original image. Decoding or superimposition is the process of stacking the share on one another to regenerate the original required secret image from shares. Though, the Visual System of Human beings can be used to understand and get the original required secret image. For regenerating or obtaining the original image Algorithms II is developed and that is illustrated in Table 2.

Black Block	Pixel	Code	White Block	Pixel	Code
$\begin{bmatrix}0&1&1&1\\1&0&1&1\\1&1&0&1\\1&1&1&0\end{bmatrix}\begin{bmatrix}1&0&1&1\\1&1&0&1\\1&1&1&0\\0&1&1&1\end{bmatrix}\begin{bmatrix}1&1&0&1\\1&1&1&0\\0&1&1&1\\1&0&1&1\end{bmatrix}\begin{bmatrix}1&1&1&0\\0&1&1&1\\1&0&1&1\\1&1&0&1\end{bmatrix}$			$\begin{bmatrix}0&0&0&0\\1&1&1&1\\1&1&1&1\\1&1&1&1\end{bmatrix}\begin{bmatrix}1&1&1&1\\0&0&0&0\\1&1&1&1\\1&1&1&1\end{bmatrix}\begin{bmatrix}1&1&1&1\\1&1&1&1\\0&0&0&0\\1&1&1&1\end{bmatrix}\begin{bmatrix}1&1&1&1\\1&1&1&1\\1&1&1&1\\0&0&0&0\end{bmatrix}$		
BC1,BC2,BC3,BC4			WC1,WC2,WC3,WC4		

Fig 3. Code Matrix

3 Results and Discussion

Several experiments are conducted to test the result obtained using the method proposed, which uses different images of different sizes and the output of the experiments conducted on Lena's image with a size of 512x512 is presented. The results obtained with Algorithm I and II illustrated in Tables 1 and 2 are represented in Figure 4. Lena's color image, represented in Figure 4, (a) is first decomposed into R, G, and B component images represented in Figure 4 (b), (c), and (d) using step 1 of

Table 1. 2.2.1 Algorithm I: Algorithm for creation of share from secrete image

Input: Original RGB Secrete Color Image $OI = (OI_{ij})$ of size H X W where i=0 to H-1 and j=0 to W-1

Output: Four noise-like RGB share images $SA = (SA_{ij})$, $SB = (SB_{ij})$, $SC = (SC_{ij})$ and $SD = (SD_{ij})$ where i=0 to H-1 and j=0 to W-1

Begin

1: Separate original RGB secrete image OI_{ij} into R(Red), G(Green), and B(Blue) components image as $RI = (RI_{ij})$, $GI = (GI_{ij})$ and $BI = (BI_{ij})$.

2: Convert each component image RI, GI and BI into a half-tone image using Jarvis Half-toning algorithms as RI_{ij}^{hft}, GI_{ij}^{hft}, BI_{ij}^{hft}

3: As per table 1 define the code matrix for black-pixel & white-pixel of a half-tone image RI_{ij}^{hft}, GI_{ij}^{hft}, BI_{ij}^{hft}

4: Define four share images for RI_{ij}^{hft} as $R1_{ij}$ $R2_{ij}$, $R3_{ij}$ *and* $R4_{ij}$

5: For i=0 to H-1

For j=0 to W-1

If $\left(RI_{ij}^{hft} = 0\right)$ then

1. Randomly select one code block from black code (BC1 to BC4 from table 1) block

2. Randomly select one row from selected code block and assign to row vector V= {V0, V1, V2, V3}

End

If $\left(RI_{ij}^{hft} = 1\right)$ then

1. Randomly select one code block from white code (WC1 to WC4 from table1) block

2. Randomly select one row from selected code block and assign to row vector V={V0, V1, V2, V3}

End

Assign each pixel from the row vector V to different shares $R1_{ij}R2_{ij}, R3_{ij}$ and $R4_{ij}$ sequentially as below for Red components share construction.

$R1_{ij} = V0, R2_{ij} = V1, R3_{ij} = V2, R4_{ij} = V3$

End

6: Define four different share images for GI_{ij}^{hft} as $G1_{ij}$ $G2_{ij}$, $G3_{ij}$ *and* $G4_{ij}$ and repeat step 5 for Green components share construction

7: Define four different share images for BI_{ij}^{hft} as $B1_{ij}$ $B2_{ij}$, $B3_{ij}$ *and* $B4_{ij}$ and repeat step 5 for Blue components share construction

8: Concatenate four Red, Green and Blue components share to produce four noise-like final RGB shares as

$SA_{ij} = Concatenate\ (255 * R1_{ij}, 255 * G1_{i,j}, 255 * B1_{i,j})$, $SB_{ij} = Concatenate\ (255 * R2_{ij}, 255 * G2_{i,j}, 255 * B2_{i,j})$,

$SC_{ij} = Concatenate\ (255 * R3_{ij}, 255 * G3_{i,j}, 255 * B3_{i,j})$, $SD_{ij} = Concatenate\ (255 * R4_{ij}, 255 * G4_{i,j}, 255 * B4_{i,j})$

End

Table 2. 2.2.2 Algorithm II: Algorithm for Secrete Recovery

Input: Four noise-like RGB share images $SA = (SA_{ij})$, $SB = (SB_{ij})$, $SC = (SC_{ij})$ and $SD = (SD_{ij})$ where i= 0 to H-1 and j=0 to W-1

Output: Original RGB Secrete Color Image $OI = (OI_{ij})$ of size H X W where i=0 to H-1 and j=0 to W-1

Begin

1: Separate four noise-like RGB share images SA_{ij} , SB_{ij} , SC_{ij} , *and* SD_{ij} into R, G, and B components images and convert these into a binary image as below: $(R1 = (R1_{ij})/255$,$G1 = (G1_{ij})/255$ and $B1 = (B1_{ij})/255)$, ($R2 = (R2_{ij})/255, G2 = (G2_{ij})/255$ and $B2 = (B2_{ij})/255)$), $(R3 = (R3_{ij})/255, G3 = (G3_{ij})/255$ and $B3 = (B3_{ij})/255)$ and $(R4 = (R4_{ij})/255, G4 = (G4_{ij})/255$ and $B4 = (B4_{ij})/255)$ respectively.

2: Combine all R(Red), then G(Green), and finally B(Blue) components binary share images using XOR operation as below:

$R = (R1 \oplus R2 \oplus R3 \oplus R4)$,

$G = (G1 \oplus G2 \oplus G3 \oplus G4)$,

$B = (B1 \oplus B2 \oplus B3 \oplus B4)$

3: Concatenate binary Red(R), G(Green), and B(Blue) as color R, G, and B component image to produce original RGB secrete image as:

$OI = Concatenate\ (R * 255,\ G * 255,\ B * 255)$

End

algorithm 1, then each R, G, and B component image are converted into halftone image using Jarvis error diffusion half-toning technique discussed in 2.1.2. Then in the next step code matrices for black-pixel and the code matrices for the white pixel are used as represented in Figure 4 and that is consequent to the code matrix used by Mahmoud E. Hodeish et al.[4]. The code matrix designed and used in step 5 of the Algorithms is represented easily and provides better visual excellence of the generated share images as represented in Figure 4 (e), (f), and (g). Finally, with the other steps presented in Algorithms I and II four color shares and the final secret image are regenerated by applying the simple XOR Boolean operation on share images.

Figure 4 shows that the final reassembled image and used original image are the same clarity and size, meaning that the expansion of pixels issue is resolved 100%. The code block designed here creates all shares of equal size and which are exactly equivalent to the size of the original secret image and the size of the reassembled image. Flipping issues and also share distortion problems are not arising.

3.1 Performance Evaluation

The performance evaluation and analysis of the presented method is performed using different statistical methods and different standard secret image. For measuring the noiselessness or imperceptibility between the reconstructed secret image and the original required secret image, different scientific metrics for objective evaluation were used. All the images manipulated in the experiments are converted and processed in binary format, because of that, the objective evaluation[10,11] matrices are then used for the identification of the communal relationship between the position of the pixel and the value of the pixel and it is suitable for binary images.

3.1.1 Metrics for Objective Evaluation

For the Objective Evaluation of different images, either the input or output and various metrics of error or objective evaluation are used. For the calculation error metrics, True-Positive (TP), False-Positive (FP), True-Negative (TN), and False-Negative (FN) pixels need to be calculated first with the respect to original input and generated output images.

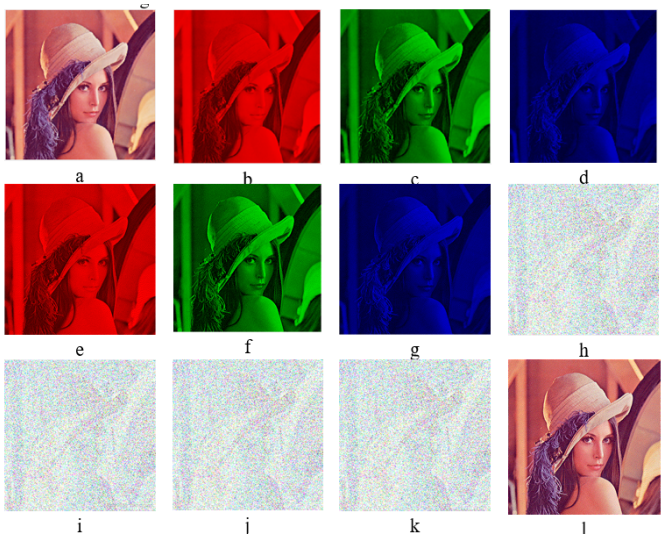

Fig 4. Result Obtained with Alogirthm I and II: Caption a-Original RGB Image b,c, and d are RGB Color components e f, and g are the half-tone image of color components image h, i, j, and k are the four shares generated and the l is reconstructed image.

1. Recall/Sensitivity

$$\text{Recall} = \frac{TP}{TP+FN} \tag{1}$$

2. Precision

$$\text{Precision} = \frac{TP}{TP+FP} \tag{2}$$

3. Specificity

$$\text{Specificity} = \frac{TN}{TN+FP} \tag{3}$$

4. Accuracy

$$\text{Accuracy} = \frac{TP+TN}{TP+FP+FN+TN} \tag{4}$$

5. F-Measure

$$FM = \frac{2X \text{ Recall X Precision}}{\text{Recall X Precision}} \tag{5}$$

$$\text{Where } R_{FN} = \frac{FN}{FN+TP}, R_{FP}\frac{FP}{FP+TN}$$

6. Negative Rate Matrix (NRM)

$$NRM = \frac{R_{FN}+R_{FP}}{2} \tag{6}$$

7. Balanced Classification Rate (*BCR*)/ Area Under the Curve (*AUC*)

$$BCR = 0.5X \text{ (Specificity } + \text{ Recall)} \tag{7}$$

8. Balanced Error Rate (BER)

$$BER = 100X(1-BCR) \tag{8}$$

Table 3. Objective Evaluation Metrics between encoded halftones R, G, and B components of the secrete image and their corresponding decoded image

	Halftone Red Component encoded share and equivalent decoded share	**Halftone Green Component encoded share and equivalent decoded share**	**Halftone Blue Component encoded share and equivalent decoded share**	**Ideal values**
Recall	1.00	1.00	1.00	1
Precision	1.00	1.00	1.00	1
Specificity	1.00	1.00	1.00	1
Accuracy	1.00	1.00	1.00	1
F-Measure	2.00	2.00	2.00	1
NRM	-0.00	-0.00	-0.00	0
BCR	1.00	1.00	1.00	1
BER (%)	0.00	-0.00	0.00	0

Here, TP, FP, TN, and FN are first calculated for each Red(R), Green(G), and Blue(B), component halftone image formed from the original required secrete image and reconstructed halftone image formed from Red(R), Green(G), Blue(B), component image.

Evaluation metrics between each R, G, and B component halftone image and reconstructed component image are displayed in Table 3. The result represented in the table shows that the values obtained are exactly equal to ideal values which mean the regenerated image is noiseless and there should be imperceptibility between the secret information image and the superimposed image.

3.2 Pixel expansion

The number of pixels that are used for representing the single secret information pixel p in the secret image is called pixel expansion. So p should be as lesser as possible in the shared image, in this proposed work value of p=1 means that the expansion of pixel is zero, so the problem is 100% reduced in the study, because the size of the shared image and regenerated image size is exactly equal which is displayed in Figure 4 (a) original image, share images are b, c, d and e, and the superimposed image is f.

3.3 Contrast and statistical analysis

As represented in Figure 4 (a), and (f) the reconstructed secret image is achieved without pixel distortion. To measure the superiority of the reconstructed image and to demonstrate that the regenerated original image represented equal superiority as the secret input image, different statistical metrics of image restoration are used as below.

3.3.1 MSE-Mean Square Error

Mean-Square-Error in short MSE[12] can be mathematically computed using the formula

$$MSE = \frac{1}{MX\,N}\sum_{i=1}^{M}\sum_{j=1}^{N}(h_{ij} - h'_{ij})^2 \tag{9}$$

Where h_{ij} *and* h'_{ij} are pixels value of the original input image and regenerated image respectively.

3.3.2 Peak-Signal-to-Noise-Ratio(PSNR

Peak-Signal-to-Noise-Ratio(PSNR)[10] is also and mathematical or engineering formulation calculated using MSE by the following formula.

$$PSNR = 10 * loglog\,\frac{R^2}{MSE} \tag{10}$$

Statistically, when the value PSNR=1, it signposts that the method delivers the optimal visual quality.

3.3.3 Universal Index Quality (UIQ)

Universal Index Quality (UIQ)[10] can be calculated by the following equation

$$UIQ = \frac{4\sigma_{zy}\,\bar{x}\bar{y}}{\sigma_x^2 + \sigma_y^2\,[\,\bar{x}^2 + (\bar{y})^2\,]} \tag{11}$$

This is used to model image distortion which is the combination of the subsequent three factors these are

1. Loss-of-correlation,
2. Luminance distortion then
3. Contrast distortion

The UIQ value of two images varies from -1 to +1. The two images X and Y have a strong positive linear correlation if UIQ is close to +1. The value -1 (one) of UIQ designates an adverse association between two images, and the value 0(zero) designates that there is almost no association between these two images[11].

3.4 Maximum Difference (MD)

The maximum Difference(MD) measure is used here to calculate the error between the original input image, and the reconstructed image. MD is directly proportional to contrast giving an image dynamic range which can be calculated with the expression 12.

$$MD = max\,(x_{ij} - y_{ij}\big| \tag{12}$$

3.5 Average Difference (AD)

The average difference is a method of calculating the difference between two images; the original input image and the regenerated image. The average Difference(AD) between the original secrete input image with the superimposed image is then calculated below[11].

$$AD = \frac{1}{M\,X\,N}\sum_{i=1}^{M}\sum_{j=1}^{N}(X_{ij} - Y_{ij}) \tag{13}$$

Where the value of X and the value of Y denote the original input image and calculated recovered image. All the metrics values discussed above are represented in Table 4. Table 4 represents values of MSE, MD, AD is zero, the value PSNR is infinite ∞ and the UIQ value is equal to 1, representing and assuring that the original image is completely recovered without any damage or loss of any meaningful information from the reconstructed image.

Table 4. Value of Difference Statistical Metrics Obtained in the experiment

Statistical Metrics	Value Obtained in Experiments
MSE	0
PSNR	∞
UIQ	1
MD	0
AD	0

We compare our method with the previously known method the result achieved using different statistical measures are represented in Table 5.

Table 5. Results of comparison between the previously known scheme available and the proposed method using statistical measures

Scheme	Secret Image	Pixel Expansion	Decoding Method	Aspect Ratio	Reconstructed Image
Zhou et. al.,'s scheme [3]	Binary(m x n)	p=4	OR Operation	Changed	Better quality
Zhongmin Wang et. al.,'s [13]	Binary(m x n)	P=4	OR Operation	changed	Lossless
Mahmoud. Hodeish et. al.,'s [12]	Binary Halftone	P=1	XOR Operation	Changed	Lossless
Mahmoud. Hodeish et. al.,'s [4]	Binary Halftone	P=2	XOR Operation	Changed	Lossless
Chang-Chou Lin [5]	Grey Level	P=4	OR Operation	Changed	Lossy
F Liu et. al.,'s [14]	Color	P=4	OR operation	Changed	Lossy
Proposed Scheme	Color	p=1	XOR Operation	Unchanged	Lossless

4 Conclusion

In the proposed research work, a novel scheme for the secret sharing of Half-tone visual cryptography is presented it mainly works on color images, and it overcomes the pixel expansion, less contrast, and poor superiority of the superimposed image problem by designing the required code book. RGB color-secrete images used are alienated into color channels and then converted into half-tone images using Jarvis's Halftone algorithms. For each color half-tone channel, four different shares are produced using a codebook designed for white-and-black pixels. All four shares of the three-color channel's halftone image are then concatenated to reproduce the four RGB shares. Those shares are then distributed among the four participants. Finally, all four shares are superimposed together to reproduce the original image. Selection of the code book and row vector from the selected codebook is performed randomly depending on the pixels present in each color channel. Shares are combined with XOR-Boolean operation for producing better quality output images. The performance of the method is tested with different statistical measures and their values are obtained- such as Mean-Square-Error(MSE): 0, Peak-Signal-to-Noise-Ratio(PSNR): ∞, Universal Index Quality (UIQ):1, etc. This means that the image is completely recovered and obtained a good contrast. We found good results concerning the quality and zero-pixel expansion.

References

1) Naor M, Shamir A. Visual cryptography. In: Santis D, A, editors. Advances in Cryptology — EUROCRYPT'94;vol. 950. Springer Berlin Heidelberg. 1995;p. 1–12. Available from: https://doi.org/10.1007/bfb0053419.
2) Ateniese G, Blundo C, De Santis A, Stinson DR. Visual Cryptography for General Access Structures. *Information and Computation*. 1996;129(2):86–106. Available from: https://doi.org/10.1006/inco.1996.0076.
3) Zhou Z, Arce GR, Crescenzo GD. Halftone visual cryptography. *IEEE Transactions on Image Processing*. 2006;15:2441–2453. Available from: https://doi.org/10.1109/TIP.2006.875249.
4) Hodeish ME, Humbe VT. An Optimized Halftone Visual Cryptography Scheme Using Error Diffusion. *Multimedia Tools and Applications*. 2018;77(19):24937–24953. Available from: https://doi.org/10.1007/s11042-018-5724-z.
5) Lin CC, Tsai WH. Visual cryptography for gray-level images by dithering techniques. *Pattern Recognition Letters*. 2003;24(1-3):349–358. Available from: https://doi.org/10.1016/S0167-8655(02)00259-3.

6) Somwanshi DR, Humbe VT. A Secure and Verifiable Color Visual Cryptography Scheme with LSB Based Image Steganography. *International Journal of Advanced Trends in Computer Science and Engineering*. 2021;10(4):2669–2677. Available from: https://doi.org/10.30534/ijatcse/2021/031042021.
7) Sherine A, Peter G, Stonier AA, Praghash K, Ganji V. CMY Color Spaced-Based Visual Cryptography Scheme for Secret Sharing of Data. *Wireless Communications and Mobile Computing*. 2022;2022:1–12. Available from: https://doi.org/10.1155/2022/6040902.
8) Singh A, Kumar CM. Competitive Swarm Improved Invasive Weed Optimization-Based Secret Sharing Scheme for Visual Cryptography. *Cybernetics and Systems*. 2022. Available from: https://doi.org/10.1080/01969722.2022.2080903.
9) Çiftci E, Sümer E. A novel steganography method for binary and color halftone images. *PeerJ Comput Sci*. 2022;8:1062. Available from: https://doi.org/10.7717/peerj-cs.1062.
10) Wang Z, Bovik AC, Sheikh HR, Simoncelli EP. Image Quality Assessment: From Error Visibility to Structural Similarity. *IEEE Transactions on Image Processing*. 2004;13(4):600–612. Available from: https://doi.org/10.1109/TIP.2003.819861.
11) Ece C, Mullana MMU. Image quality assessment techniques pn spatial domain. 2011. Available from: http://ijcst.com/vol23/1/sasivarnan.pdf.
12) Hodeish ME, Bukauskas L, Humbe VT. An Optimal (k,n)Visual Secret Sharing Scheme for Information Security. *Procedia Computer Science*. 2016;93:760–767. Available from: https://doi.org/10.1016/j.procs.2016.07.288.
13) Wang Z, Arce GR, Crescenzo GD. Halftone Visual Cryptography Via Error Diffusion. *IEEE Transactions on Information Forensics and Security*. 2009;4(3):383–396. Available from: https://doi.org/10.1109/TIFS.2009.2024721.
14) Liu F, Wu CK, Lin XJ. Colour visual cryptography schemes. *IET Information Security*. 2008;2(4):151–151. Available from: https://doi.org/10.1049/iet-ifs:20080066.