

Research Article

Firas Mohammed Aswad, Ihsan Salman, and Salama A. Mostafa*

An optimization of color halftone visual cryptography scheme based on Bat algorithm

<https://doi.org/10.1515/jisys-2021-0042>

received March 16, 2021; accepted May 06, 2021

Abstract: Visual cryptography is a cryptographic technique that allows visual information to be encrypted so that the human optical system can perform the decryption without any cryptographic computation. The halftone visual cryptography scheme (HVCS) is a type of visual cryptography (VC) that encodes the secret image into halftone images to produce secure and meaningful shares. However, the HVC scheme has many unsolved problems, such as pixel expansion, low contrast, cross-interference problem, and difficulty in managing share images. This article aims to enhance the visual quality and avoid the problems of cross-interference and pixel expansion of the share images. It introduces a novel optimization of color halftone visual cryptography (OCHVC) scheme by using two proposed techniques: hash codebook and construction techniques. The new techniques distribute the information pixels of a secret image into a halftone cover image randomly based on a bat optimization algorithm. The results show that these techniques have enhanced security levels and make the proposed OCHVC scheme more robust against different attacks. The OCHVC scheme achieves mean squared error (MSE) of 95.0%, peak signal-to-noise ratio (PSNR) of 28.3%, normalized cross correlation (NCC) of 99.4%, and universal quality index (UQI) of 99.3% on average for the six shares. Subsequently, the experiment results based on image quality metrics show improvement in size, visual quality, and security for retrieved secret images and meaningful share images of the OCHVC scheme. Comparing the proposed OCHVC with some related works shows that the OCHVC scheme is more effective and secure.

Keywords: visual cryptography, halftone visual cryptography scheme, error diffusion, bat optimization algorithm

1 Introduction

The rapid growth of the Internet and the transmission channels enable access to visual information (image, video, etc.) much easier for an unauthorized individual [1,2]. The visual cryptography scheme (VCS) is a perfect method to encrypt visual information without complicated calculations on the receiver's side to protect this information's confidentiality [3,4]. Visual cryptography (VC), also called visual secret sharing, is an encryption method that encrypts pictures, text, and so on and uses the human visual system (HVS) to decrypt without any complicated computation is the principal strength of this method [5,6]. It has other

* **Corresponding author: Salama A. Mostafa**, Department of Software Engineering, Center of Intelligent and Autonomous Systems, Faculty of Computer Science and Information Technology, Universiti Tun Hussein Onn Malaysia, 86400, Johor, Malaysia, e-mail: salama@uthm.edu.my

Firas Mohammed Aswad: Computer Department, College of Basic Education, University of Diyala, 32001, Diyala, Iraq, e-mail: drfirasaswad@gmail.com

Ihsan Salman: Computer Department, College of Basic Education, University of Diyala, 32001, Diyala, Iraq, e-mail: ihsan1975.83@gmail.com

essential qualities such as reversibility and perfect security, and it is very suitable for specific applications such as medical image protection, military, forensics, and art images [7,8].

The VCS is a type of secret image sharing [9–11]. When Naor and Shamir explained the concept of “How to share a secret” by dividing D data into n pieces in such a way that simple reconstruction from any k pieces can recover the secret, but not any $(k - 1)$ pieces. Based on this principle, the concept of VCS presented by Naor and Shamir [2] emerges to encrypt digital images. Naor and Shamir’s scheme depends on the codebook technique to encode one secret image (SI) and generate random shares variant in the expansion of pixels. Codebook technique is a pattern or a mask that decides various secret pixels’ possibilities, as illustrated in Figure 1 [5].

Secret pixel P	Share1	Share2	Share1 \oplus Share2
□	■□	■□	■□
	□■	□■	□■
■	■□	□■	■■
	□■	■□	■■

Figure 1: (2,2)-VCS with (2 subpixels) scheme codebook [2].

Although this scheme has important features, it suffers from significant problems: (1) it is very difficult to manage and design the codebook, (2) it generates meaningless share that does not carry any visual information, (3) there is a loss of contrast and pixel expansion that results in increasing size and low quality of recovery image, and (4) it suffers from cross-interference problem [3]. It is, therefore, essential to enlarge the area of VC through a proposed scheme to create halftone shares that have meaningful information to increase visual quality and security. This scheme is called halftone visual cryptography (HVC) to obtain a better quality of the shares that carry visual information [4]. The main idea of the HVC scheme is the realization of VC via digital halftone technique depending on the blue noise concept to generate k shares more pleasant to the human eyes and more flexible shares management [12].

The HVC methods still endure unsolved problems like the visual quality of shares, large pixel expansion, difficulty design codebook, and cross-interference in the reconstruction of secret image and construction of share images [5]. This study proposes a novel HVC scheme for a color image using the proposed hash codebook technique and proposes a construction technique that offers the use of flags with a halftone cell size of $[4 \times 4]$ to avoid the problems of cross-interference and pixel expansion of the share images. It also proposes a new technique to distribute the secret information pixels (SIPs) into a halftone cover image in a randomly form-based bat optimization algorithm to make the OCHVC scheme more secure. This model can be implemented in different research domains including healthcare systems [13,14], medical optimization systems [15,16], and information security systems [17].

This article is subsequently organized as follows: Section 2 briefly reviews the related works. Section 3 explains theoretical backgrounds. Section 4 describes the details of the proposed OCHVC scheme. Section 5 presents the results and compares them with those obtained by other previous methods. Section 6 presents conclusions.

2 Related work

Several well-established studies on the optimization of color halftone visual cryptography are available in the literature. In this section, the most related work has been presented and discussed. In the previous work of Zhou *et al.* [4], a novel method called the HVC scheme based on dithering to provide better visual quality has been introduced. This scheme implements the principles of VCS via the halftone process to encode the secret image into n halftone shares carrying crucial visual information. Furthermore, using a pair of complementary shares prevents the shares' visual information shown in the decoded image. This scheme needs expansive computation to insert a SIP into preexisting encoded halftone share by applying the void and clustering halftone.

Hodeish and Humbe [5] proposed the optimal halftone visual cryptography scheme using the Jarvis E-D filter. This scheme avoids the explicit demand for codebooks and generates semi-random shares images by encoding only secret black pixels while leaving the white secret pixels intact. This technique results in less pixel expansion to improve the visual quality of recovering secret images faster, but this scheme is used only for the binary secret image. The recovered secret image's size is double the size of the original secret image.

The work of Wang *et al.* [6] developed HVC by using the error diffusion (E-D) halftone technique. In this scheme, they proposed three methods for generating shares based on HVCs. The first method uses halftone cover share and its complement. By using a pair of complementary shares, it solves the cross-interference problem on the reconstructed image. However, while the secret information pixel's location is determined by using the critical complementary pair's image feature, the place of the SIPs on other shares is randomly distributed, resulting in the low visual quality. The second method proposes using auxiliary black pixel (ABP) to solve cross-interference, but the consequence of using ABP is that the share looks darker. The third method uses parallel E-D to construct shares and reduce the ABP number, but there is a possibility of cross-interference.

Devi [7] proposed a new technique to overcome weaknesses in Wang's methods by employing a global optimization approach across all halftone shares images based on the concept void and clustering algorithm. The goal of using the global optimization approach is to rearrange the n shares' pixels to include good visual quality of the n shares. Without loss of generality, assume share 1 and share 2 are key complementary pairs among the n halftone shares. Then, the visual quality optimization can be performed on the 3rd, 4th, ..., n th shares successively.

Hameed and Ibrahim [8] proposed a method called color halftone visual cryptography. They use the dynamic codebook and error diffusion technique to retrieve color secret images of the same size and optimal contrast and overcome the cross-interference problems. Perfect security gives the dealer absolute control to check each share's authentication and flexibility in the management of share images.

The study by Liu and Wang [9] proposed the new color HVC scheme to encode a secret halftone image into natural color halftone shares. In contrast, these shares halftone by vector error diffusion. This algorithm can generate color halftone share, which carries significant visual information by modifying vector error diffusion to spread the quantization error submitted by encoding secret pixels into the color area. This area is least sensitive to human vision, which guarantees good visual quality for halftone shares. But this algorithm depends on generating auxiliary black pixels ABP, which lowers the visual quality and enlarges the secret image.

Yan *et al.* [10] introduced an HVC method to improve the visual quality and avoid the distortion of shares. This scheme generates shares with homogeneous distribution and a minimum number of ABPs. Yan scheme is based on the (k,n) principles – VCS to encode binary secret images into halftone share images. SIPs are fixed in parallel and separated maximally before halftone processing. The proposed method obtains excellent visual quality, but the shares' cross-interference problems are still unresolved.

Thomas and Gharge [12] developed a new algorithm of error diffusion and compared this algorithm with existing error diffusion types based on image quality metrics. This new algorithm modifies the HVCs, VCs for gray images, and VCs for color images by decomposing secret images into R, G, and B components and using the (2,2)-VCS to encode each color band individually after applying the proposed error diffusion filter.

This process generates three meaningless shares by stacking all shares of the secret color image recovered in the same size, but the quality of restoring the color secret image is still unsatisfactory.

3 Research methods and materials

This section reviews the main methods that are used in the proposed OCHVC scheme.

3.1 Principle of HVCs (2,2)

The central concept of HVC can be illustrated through the simplest two-out-of-two HVC threshold scheme [3,4]. In this method, the gray level image GI is halftoned by an error diffusion filter to obtain halftone image I . The halftone image I is assigned to participant 1, and the complementary image I' is obtained by reversing the halftone image I ; all black/white pixels in I are reversed into white/black pixels in I' , and then, it is assigned to participant 2. Secret pixel P should be encoded into a $Q_1 \times Q_2$ halftone cell in each of the two shares, and to do this, only two pixels should be modified as the SIPs in each halftone cell. These two secret information pixels should also be in the same position in the two shares, such as pixels A and B in Figure 2. If P is white, a matrix M is randomly selected from the collection of matrices C_0 of conventional VC. If P is black, it is randomly selected from C_1 . The secret information pixels in the i th share are replaced by the two subpixels in the i th row of the selected matrix as shown in Figure 2.

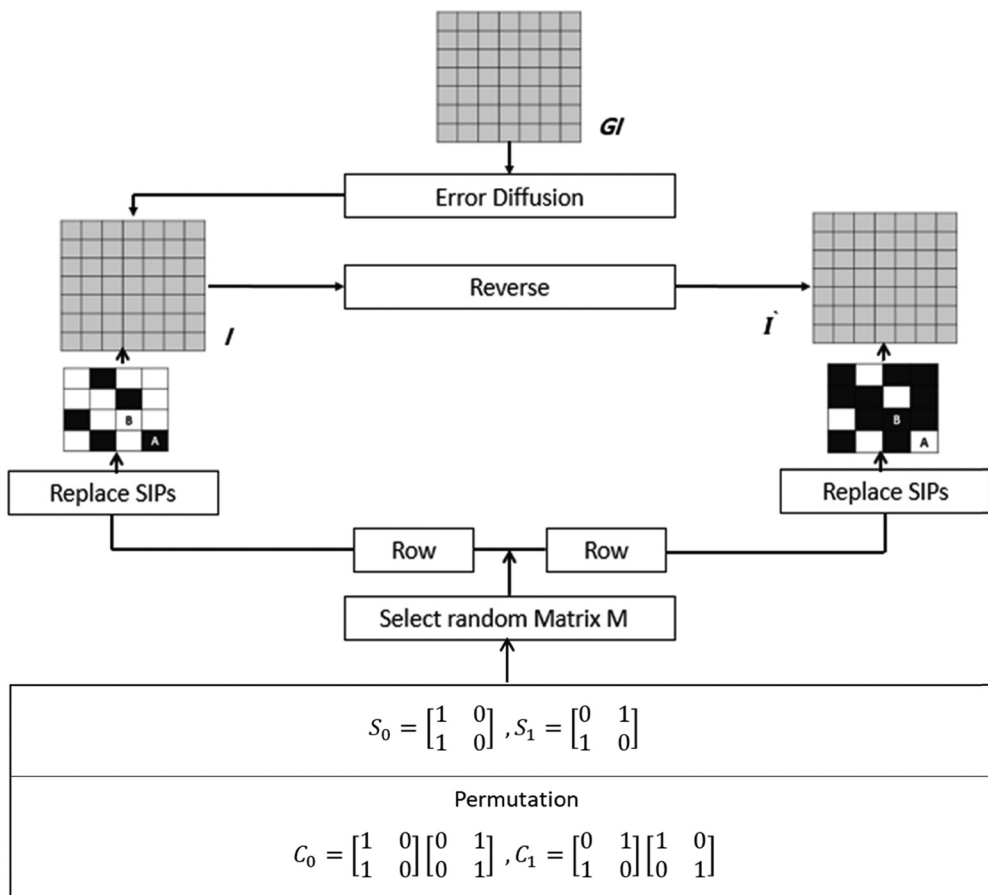


Figure 2: Block diagram for (2-out-of-2) HVC scheme with halftone cell size $q = 4$ [4].

Since C_0 and C_1 are the collections of conventional VC, these modified pixels carry the encoded secret. The other pixels in the halftone cell, which have not been modified, are referred to as ordinary pixels. It can also be found that if P is white, one out of $Q1Q2$ pixels in the reconstructed halftone cell, which is obtained by superimposing the two encoded halftone cells, is white, while all other pixels are black and if P is black, all pixels in the reconstructed halftone cell are black. Thus, the contrast condition is satisfied. The secret pixel can be visually decoded with contrast $(1/Q1Q2)$.

3.2 Error diffusion

Error diffusion (E-D) is a halftone process used to convert an image from a gray-level form to a binary form. It is seen as a standard workhorse among the existing halftone methods. This is due to its simplicity and efficiency in halftone a grayscale image. Moreover, it has the ability to provide halftone shares with quite good quality. The mechanism of error diffusion is to diffuse the error at each pixel of an image. The quantization error is filtered and fed to the input to diffuse the error at each pixel. The error filter diffuses the quantization error on one pixel away from the neighboring gray pixels. In nature, the error diffusion noise is of high frequency or “blue noise,” and, for human vision, it can provide pleasing halftone images [18]. Floyd and Steinberg [19] proposed Floyd–Steinberg E-D halftone algorithm. Floyd–Steinberg E-D circulates the current process pixel’s quantization error to four neighbor pixels by employing the error diffusion matrix shown in Figure 3 (where X is the current process pixel) [20–22].

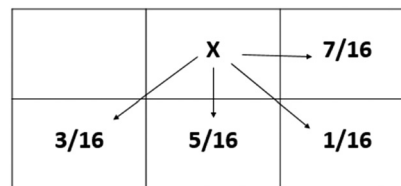


Figure 3: Floyd–Steinberg error diffusion matrix.

3.3 Bat optimization algorithm

Bat algorithm (BA) is a meta-heuristic algorithm introduced by Kotteeswaran and Sivakumar [23] in 2013, which is inspired by micro bats’ echolocation abilities for finding their prey. Microbats have a special type of sonar called echolocation to avoid obstacles and detect the prey even in low-intensity light. Bats emit a loud sound pulse, intercept its echo, and analyze it [24]. The sound vibration can be correlated with their hunting strategy depending on the prey. It means that if a bat goes near its prey, its pulse rate increases and sound decreases, while, on the other hand, if it goes away, its pulse rate decreases and sound increases. The pulse rate usually lasts for 8–10 ms, and its frequency lies in the range of 20 kHz (low pitch) to 150 kHz (high pitch). The echolocation phenomena can be characterized by the framework of certain idealized rules [23]:

- (1) Echolocation is an important parameter of bats, and it helps them to sense distance, identify their prey/food, and any potential obstacles.
- (2) Bats fly randomly at position x_i with velocity v_i having a fixed frequency f_{\min} by altering the loudness A_0 and wavelength λ in order to search preys. They can automatically adjust the wavelength or frequency of emitted pulses and pulse emission rate $r \in (0, 1)$ depending on the search range of targets.
- (3) Although loudness can be varied in many ways, we assume that loudness varies from large A_0 to the minimum standard value A_{\min} .

These three rules have been idealized to define BA, which is given in the following sections.

3.3.1 Initialization

Search space is basically a region in which prey/food is found. So, a bat moves randomly around the search space to find a prey since it has no idea about the target. The fitness of the bat determines the quality of the food. Initial population for n number of bats is generated randomly by the following equation (1):

$$x_{i,j} = x_{\min,j} + \text{rand}^*(x_{\min,j} - x_{\max,j}), \quad (1)$$

where $i = 1, 2, \dots, n$; $j = 1, 2, \dots, d$; $x_{\min,j}$ is the lower boundary for the dimension j ; and $x_{\max,j}$ is the upper boundary for the dimension j .

3.3.2 Frequency, velocity, and position of BA

The frequency in this algorithm determines the pace and step size to produce new solutions and update the velocity and position accordingly. The pulse frequency value ranges between f_{\min} and f_{\max} values. The equations are as follows:

$$f_i = f_{\min} + (f_{\max} - f_{\min})\beta, \quad (2)$$

$$v_i^t = v_i^{t-1} + (v_i^{t-1} - x^*)f_i. \quad (3)$$

Finally,

$$v_i^t = x_i^{t-1} + v_i^t, \quad (4)$$

where $\beta \in (0, 1)$ is a random number, f_i is frequency value generated for the solution i , v_i represents the updated value of velocity for the solution, and x^* is the global best solutions in the population. Now, when the current best solution is updated, the solution is locally generated around the best solution using a random walk.

$$x_{\text{new}} = x_{\text{old}} + \epsilon A^t, \quad (5)$$

where ϵ is in the range of $(-1,1)$ and A^t is the average loudness at a time t .

3.3.3 Loudness and pulse rate

The loudness and pulse emission rate value change with an increase in iterations. As the bat nears toward its prey, the value of loudness A decreases, and pulse emission rate r increases. The following equations update loudness and pulse rate:

$$A_i^{t+1} = \alpha A_i^t, \quad r_i^{t+1} = r_i^0 [1 - \exp(-\gamma t)], \quad (6)$$

$$A_i^t \rightarrow 0, \quad r_i^t \rightarrow r_i^0, \quad \text{as } t \rightarrow \infty \quad \forall 0 < \alpha, \gamma < 1. \quad (7)$$

The value of α and γ is 0.9. The initial A_i^0 can be typically $[1,2]$, and the value of pulse rate can be $[0,1]$. The values of pulse emission rate and loudness are only updated if the solution is improved.

3.4 Image quality metrics

Metrics of HVC play an essential role in measuring the efficiency of algorithms and help to develop techniques used to obtain high security and maintain the quality of retrieved and share images, and these metrics are as follows:

3.4.1 Mean squared error

This measure is widely used as a measure of image quality index. It is applied between the input image and the restored image. It is preferable to have a low value of the mean squared error, which indicates a high-quality image. Mean squared error (MSE) can be calculated using equation (8) [12]:

$$\text{MSE} = \frac{1}{m \times n} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i,j) - k(i,j)]^2. \quad (8)$$

3.4.2 Peak signal to noise ratio

Peak signal-to-noise ratio (PSNR) is the ratio metrics between maximum single power to the mess up noise power that generates distortion of the image. The value of PSNR is calculated from equation (9) [12,20].

$$\text{PSNR} = 10 \log_{10}(\text{MAX}^2/\text{MSE}). \quad (9)$$

3.4.3 Normalized cross correlation

Normalized cross correlation (NCC) is a metric of similarity of two wavelengths as a function of the lost time affected by one of the wavelengths. The large value of CNN means good quality of images. Equation (10) calculates the value of NCC [12].

$$\text{NCC} = \frac{\sum_{m=1}^M \sum_{n=1}^N x(m, n) \cdot y(m, n)}{\sum_{m=1}^M \sum_{n=1}^N (x(m, n))^2}. \quad (10)$$

3.4.4 Universal quality index

Universal quality index (UQI) is relied upon when estimating the deformation of two images. This quality index treats any distortion as a combination of three different factors: loss of correlation, luminance distortion, and contrast distortion [5]. Let us assume that x represents an input image, and y represents an output distorted image. The loss of correlation is valued by the correlation coefficient, which measures the linear correlation degree between x and y . The luminance and contrast are estimated by mean and standard deviation, respectively. Mathematically, the UQI is expressed by equation (11) [5].

$$\text{UQI} = \frac{4\sigma_{xy}\bar{x}\bar{y}}{(\sigma^2x + \sigma^2y)[\bar{x}^2 + \bar{y}^2]}. \quad (11)$$

The UQI has a dynamic range of $[-1,1]$. The optimal value is achieved if and only if $x = y$ [5].

3.5 Gaussian attacks in visual cryptography scheme

Natural images often include noise, which is not part of a perfect image. Gaussian noise is a process that adds a single noise to an image to deliberately corrupt the image to decrease the visual quality of the image. Figure 4 shows the Gaussian probability density function (PDF), which is also called a normal PDF.

Generally, the PDF is utilized to create random numbers. This noise is believed to model nearly many random real-life events. The Gaussian PDF for random variable z is calculated using equation (12) [25].

$$P(z) = \sqrt{\frac{1}{2\pi\sigma^2}} e^{-\frac{(z-\mu)^2}{2\sigma^2}} \quad (12)$$

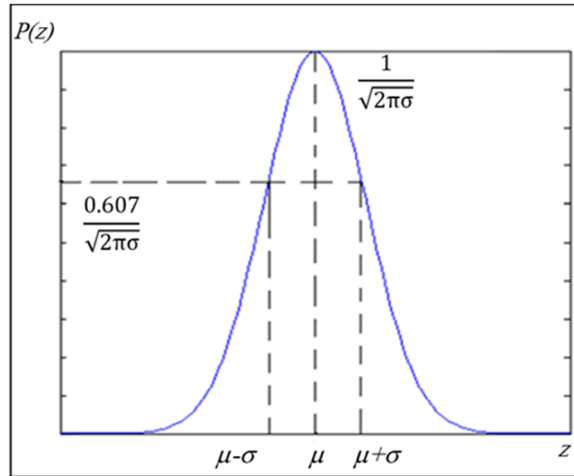


Figure 4: PDF for Gaussian noise [22].

4 The proposed system

A dealer selects a color secret image and six-color cover images as input and, via the proposed OCHVC, generates six significant shares, and under XOR operation, the secret image is decrypted. Figure 5 illustrates the general block diagram of the proposed OCHVC scheme.

As shown in Figure 5, the proposed method consists of two main stages, which are construction and reconstruction stages. The construction stage generates six meaningful, secure shares and distributes them to six participants over public communication channels. The reconstruction stage recovers halftone color secret image using XOR-Boolean operation as explained in the following sections.

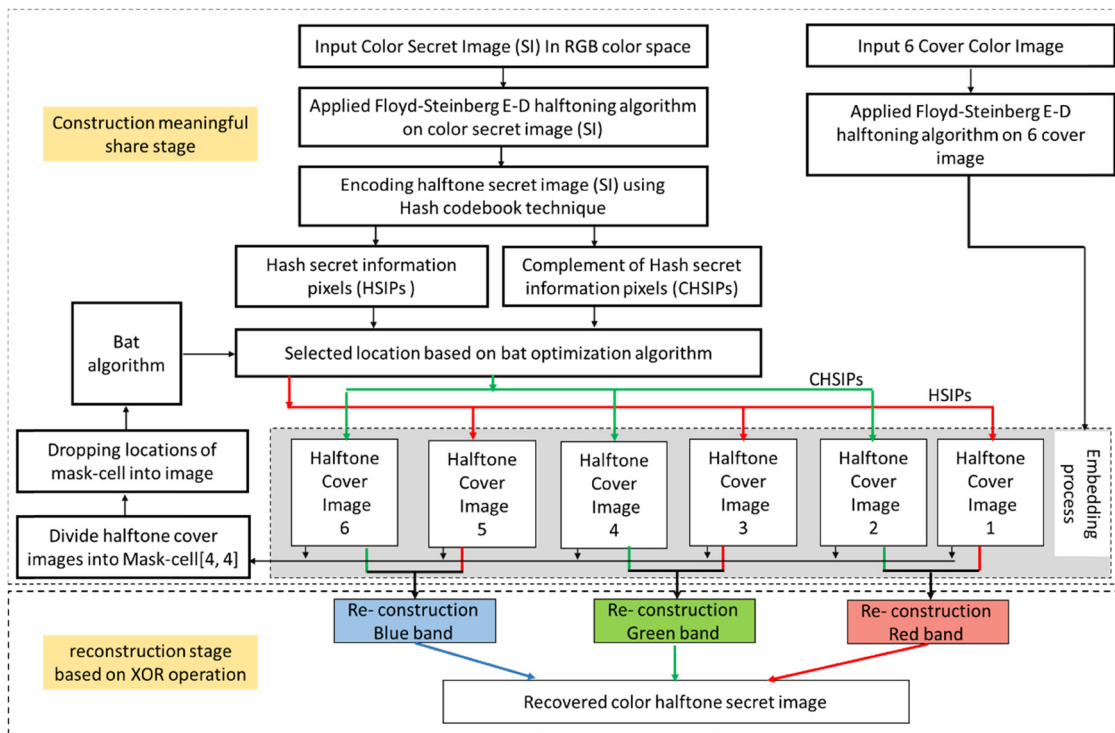


Figure 5: General block diagram of the OCHVC.

4.1 Construction of meaningful share images stage

To generate secure meaningful share images, the following steps must be followed in that order:

- *Preprocessing the SI and cover images:* This step is performed only by the dealer. The proposed method cannot directly handle the secret, and cover color images must first be passed through a preprocessing phase as a preliminary stage to the encoding phase. The preprocessing of the secret image consists of three substeps: (i) apply Floyd–Steinberg E–D algorithm to convert secret image to secret halftone image, (ii) decompose color components of halftone SI into R, G, and B color bands, respectively, and finally, (iii) for each color band of halftone SI apply the histogram technique. The six-color cover images apply only for Floyd–Steinberg E–D halftone in the traditional HVC scheme to generate a halftone cover image and its complement. However, the color cover image case cannot apply the same technique because it has a range of colors between 0 and 255. Therefore, the proposed scheme is arranged as pairs in the order of six halftone cover images such as pair 1 = {halftone cover 1, halftone cover 2}, pair 2 = {halftone cover 3, halftone cover 4}, and pair 3 = {halftone cover 5, halftone cover 6}.
- *Encoding Halftone Secret image based on hash codebook technique:* Encoding HSI is based on the proposed color (k,n) –CVCS [5]. This step generates k random shares with size four times bigger than the original halftone secret image, where $k = 1, \dots, 6$ of random shares, each k consists of $[n \times n]$ of SIPs, which carries the confidential information. To generate hash codebook technique with a fixed length of binary code (Length_Bin), for each secret pixel in halftone secret image (SP_i), it must follow several steps as follows:

Input R, G, and B halftone secret image, respectively

Create binary code

For $i = 1$ to Length_Bin

Bin = convert (i) to binary and check the balance of (Bin) is equal;

Next i;

Read (SP_i) For each color band, assign (Bin) to (SP_i), and create Mask1[4,4] and Mask2[4,4];

Distribute (Bin) into Mask1[3,4], let Row [4] in Mask1 for flags & given to flags default value (0 or 1);

Distribute (complement (Bin)) into Mask2[3,4], let Row [4] in Mask2 for flags and given to flags default value (0 or 1);

Distribute Mask1[4,4] to random share 1 and Mask2[4,4] to random share 2

The hash function concept inspires the hash codebook idea to ensure that each pixel in halftone SI has a unique binary code. Each pixel in SI is taken in order from left to right as an input into the hash codebook. The given data to it are the number of SIP, binary code (HSIP), and complement binary code (CHSIPs), where HSIP creates share 1 and CHSIPs create share 2; so for each color bands for halftone SI, two random shares are created. The hash binary code consists of 12 mean bits. There are 2^{12} different possibilities to create the codes. Still, this code must satisfy the initial condition, which is the number of 1's must be equal to the number of 0's to keep the unique attribution for the binary code as illustrated in Figure 6.

To generate a random share image, divide it into a mask cell with size = $[4 \times 4]$, in which the first three rows in the mask distribute the 12 bits of the hash binary code in order (sequentially) to fill the rows 1–3 of the Mask 1 and Mask 2 matrix, but row 4 is allocated for flags and given default value x , where $x = (0 \text{ or } 1)$ as shown in Figure 7.

- *Construct meaningful shares based on proposed embedded technique:* Figure 8 illustrates the steps to embed SIPs = {HSIP, CHSIP} into halftone cover that must be followed as described follows:
 - Take each halftone cover image $[h,w]$ and divide it into halftone cell called $q[4,4]$ and divide random share $[h,w]$ to mask cell $[4,4]$, where mask cell $[4 \times 4]$ consists of 12 bit referred to as SIPs.
 - Save locations of $q[4,4]$ in 1d cover matrix (CM) and locations of mask cell $[4,4]$ in 1d random matrix called RM.

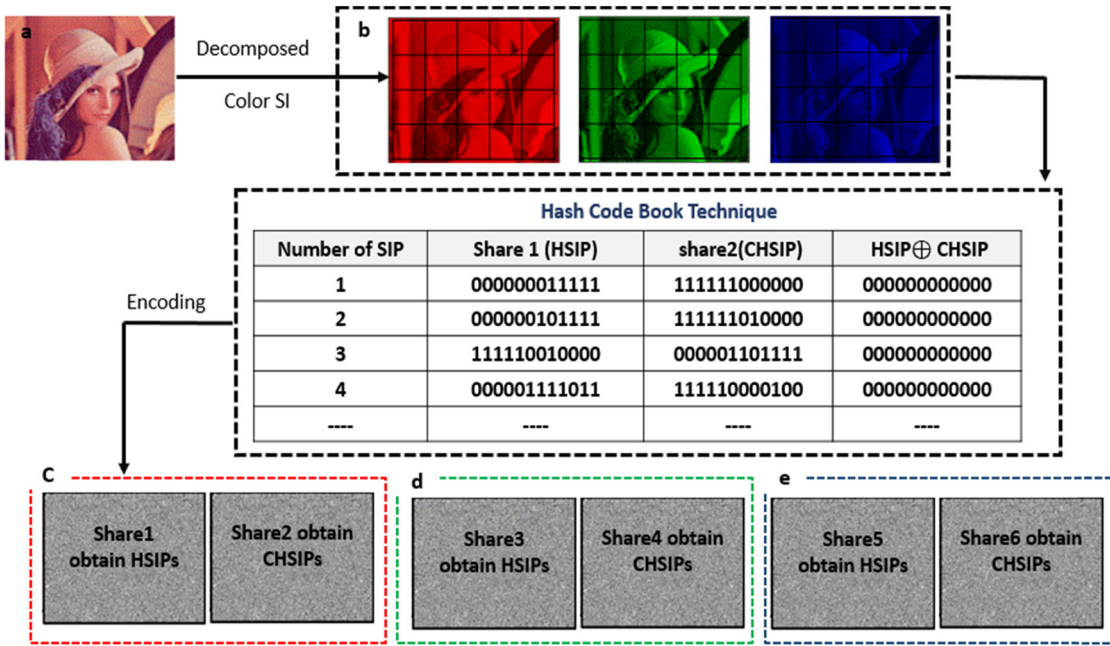


Figure 6: Generation of random shares hash codebook technique: (a) halftone SI, (b) R, G, B halftone SI, (c) shares 1 and 2 for red halftone secret image SI, (d) shares 3 and 4 for green halftone secret image SI, and (e) shares 5 and 6 for blue halftone secret image SI.

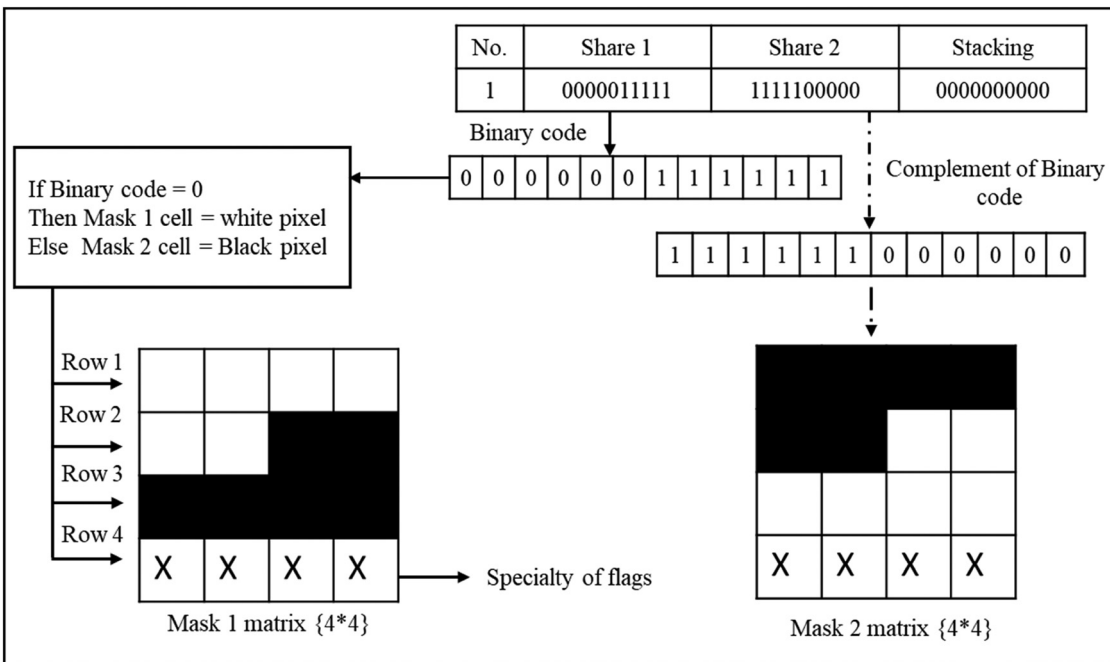


Figure 7: Create Mask 1 [4,4] and Mask 2 [4,4] matrix in Hash codebook where x represents default value for flags.

- (iii) To make the selected locations of q cell in a random manner. It drops all locations that are saved in CM randomly into an image called location image (LI) and runs the BA on LI for the selected location of halftone cell q as shown in Figure 8.

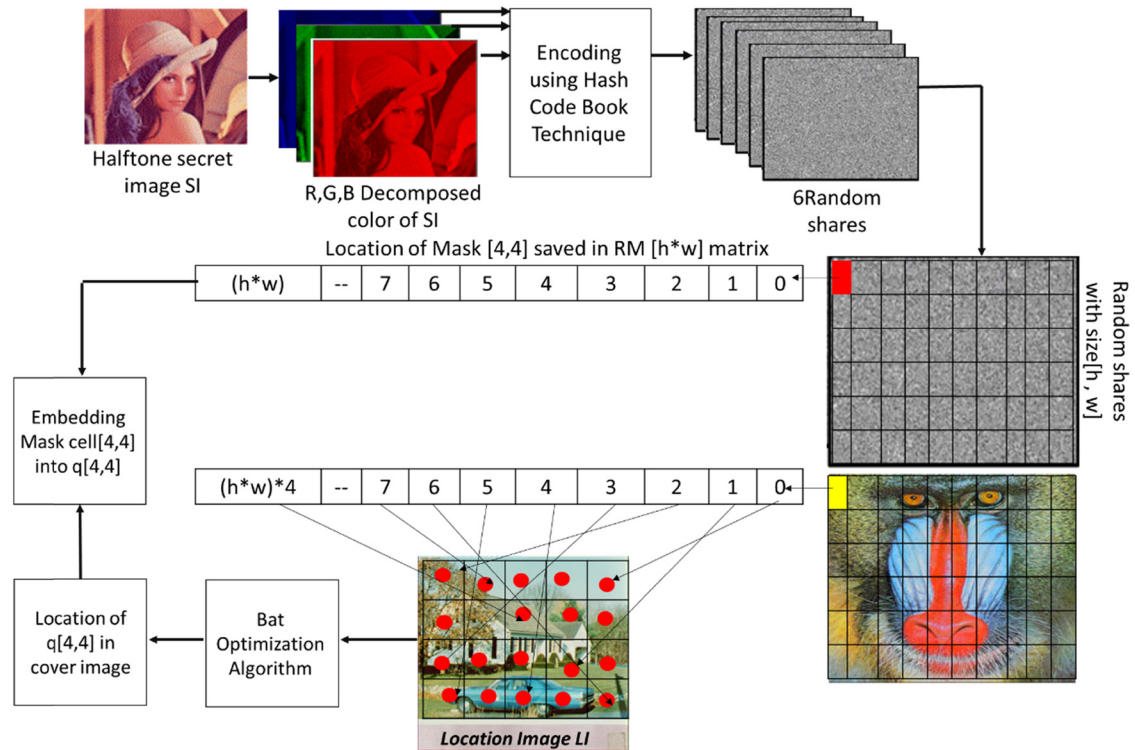


Figure 8: Distributing SIP into cover image based on the BA.

- (iv) Then, the SIP is embedded into halftone cell $q[4 \times 4]$. The location of this SIP in q cell is made sequential to produce $\hat{q}[4 \times 4]$ meaningful cell that carries visual information taken into consideration. The last row for all cells is allocated for flags. These flags are set when assigned values to variables z . The first two flags in \hat{q} cell must be equal to $([4,1] = [4,2])$.
- (v) The halftone cell size is $[4 \times 4]$. Only three rows are used for encoding and use semi-random code, which means the changes applied only on fewer bits in the halftone cell. In this way, the proposed embedded technique can overcome the cross-interference problem.

4.2 Reconstruction color halftone secret image stage

The decryption of the color halftone secret image is made only by the HVS. If the dealer wants to retrieve the original HSI, this is achieved by stacking all k meaningful shares in order; the proposed method cannot decode the SI when the number of shares is less than k . The flags play an important role in recovering the secret image, a process that starts by determining the first \hat{q} cell in the final share and then directly checking the value of the flags. If flag 1 = flag 2, then the value of the locations that hold z is automatically seen in the \hat{q} cell with the value of z , which is interpreted as 1. By default, any value that is not equal to z is interpreted as 0. In this way, it is able to retrieve the existing binary code in a dynamic codebook.

5 Implementation and results




The proposed method for color HVC and performance evaluation techniques for attacks are designed using Visual Studio Ultimate C# programming language version 2013. The workstation that holds our program is a

TOSHIBA Laptop with Windows 10 64-bit Operating System (OS), 6.00 GB RAM, and 2.10 GHz Intel Core i7-3686U CPU. However, the standard of Lena, baboon, pepper, fruits, house, tree, and vegetable images are taken from USC-SIPI image database to test the proposed system. These images had selected for several reasons such as follows:

- It is available online and free.
- It has been processed from the aspects of textured, smooth, size, with straight edges, sharp, blur.

Table 1 shows the test images that are used in the implementation of the proposed methods.

Table 1: Test images

Image name	Image	Size	Image name	Image	Size
Lena		128 × 128	House		128 × 128
Baboon		128 × 128	Tree		128 × 128
Pepper		128 × 128	Vegetables		128 × 128
Fruits		128 × 128			

The dealer selects Lena as a secret image and (baboon, pepper, fruits, house, tree, and vegetables) as cover images. Figure 9 shows the interface of the loaded secret and cover images by the dealer.



Figure 9: The interface of loaded secret and cover images by the dealer.

The preprocessing stage includes converting secret and cover images into halftone images using the Floyd–Steinberg error diffusion algorithm and decompose the color space of the secret images with

appealing histograms. The encoded halftone secret image SI outputs are two random shares for each color band R, G, and B, respectively. Then divide each random share and halftone covers sequentially into cells with the size of [4,4]. First, to embed the SIP into halftone covers in a secure manner, choose the halftone cover cell's location randomly based on BA with its set of initial parameters.

The control parameters of the BA algorithm are loudness (A) = 0.7, population size (NP) = 30, pulse rate = 0.3, frequency minimum (Q_{\min}) = -15, frequency maximum (Q_{\max}) = 15, lower bound (lower) = 0, the maximum number of iterations = 100, and an upper bound (upper) = 2. When dropping all locations of halftone cell q into location image (LI), then the BA operating on it selects the halftone cell q randomly [4,4] to be hash secret information code HSIPs. Figure 10 shows the BA's fitness, and Figure 11 shows the halftone cell's location, where Figures 10 and 11 show that the behaviors of the BA are nonlinear. So, this makes the proposed OCHVC more secure.

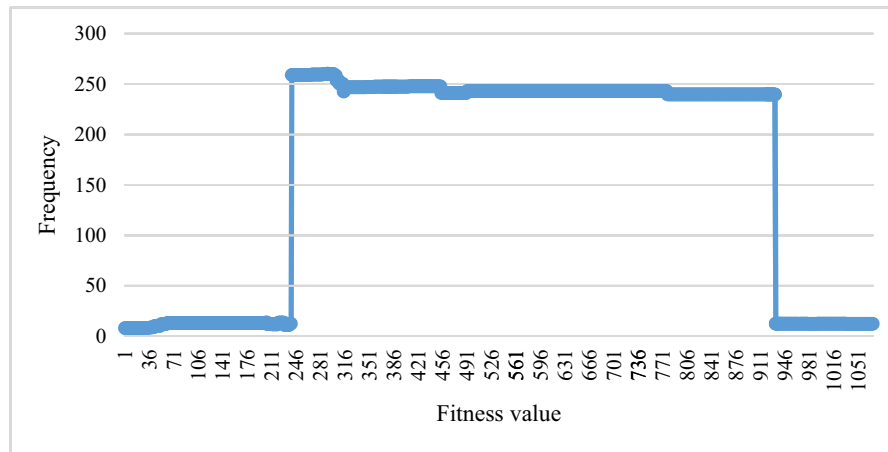


Figure 10: The fitness values of the BA.

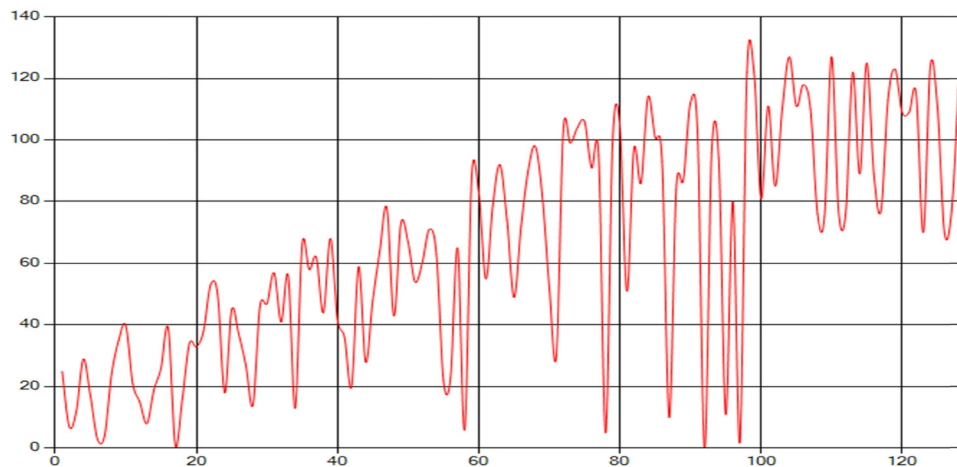


Figure 11: The location of halftone cell $q[4,4]$ based on BA.

Figure 12 simulates the interface of construction of six significant shares images and distributes one meaningful share to one subscriber over public communication channels and then reconstruction of color halftone secret image by the dealer.

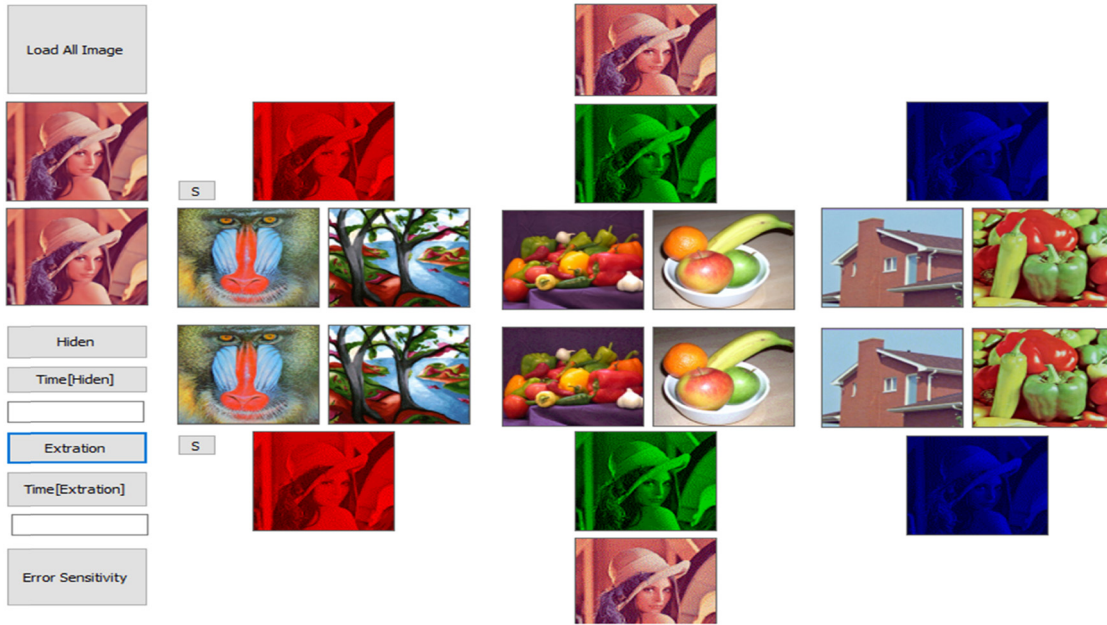


Figure 12: Interface of construction of six meaningful shares image and reconstruction of halftone color secret image SI.

5.1 Results of image quality metrics

The proposed OCHVC scheme includes two outputs. The first output results from the reconstruction of the halftone secret image step. The second output results from the six meaningful share images, representing the construction of significant shares image step. Test results for each of them are shown in this section based on image quality metrics: MSE, PSNR, NCC, and UQI. The image quality metrics applied between the halftone secret image and its corresponding reconstruction images are presented in Table 2 and that between the halftone cover images and their related final share images are presented in Table 3. Both Tables 2 and 3 illustrate that the proposed system could generate meaningful shares with higher visual quality without cross-interface problems. The proposed OCHVC scheme can reconstruct halftone color secret images with the same size and the contrast. The best results of the proposed OCHVC scheme that

Table 2: Results of image quality metrics in construction six meaningful share images using proposed OCHVC

Image quality metrics	Share 1	Share 2	Share 3	Share 4	Share 4	Share 5	Share 6
MSE	111.7447	114.5831	98.3926	95.1748	100.6062	98.5320	111.7447
PSNR	27.6485	27.5396	28.2012	28.3456	28.1046	28.1950	27.6485
NCC	0.9896	0.9939	0.9943	0.9907	0.9893	0.9933	0.9896
UQI	0.9712	0.9731	0.8287	0.8325	0.9908	0.9933	0.9712

Table 3: Results of image quality metrics in the reconstruction of color halftone secret image using proposed OCHVC scheme

Image quality metrics	Halftone secret image	Red band (SI)	Green band (SI)	Blue band (SI)	Ideal value of metric
MSE	0.0000	0.0000	0.0000	0.0000	0.0000
PSNR	∞	∞	∞	∞	∞
NCC	1.0000	1.0000	1.0000	1.0000	1.0000
UQI	1.0000	1.0000	1.0000	1.0000	1.0000

are achieved in generating significant shares image are MSE = 95.1748, PSNR = 28.3456, NCC = 0.9943, and UQI = 0.9933. The results of the proposed OCHVC that succeed in recovering halftone color secret image prove that the proposed methods are perfect in dealing with recovering halftone color secret image as shown in Table 2.

5.2 Security analysis of the OCHVC

This section proves that the proposed OCHVC scheme is more secure by using BA and presents the embedding techniques to distribute hash secret information pixels HSIPs in cover images in a random manner. The share images are distributed via the public communication channel and exposed to an attack to achieve this objective. The reason is to study the possibility of the attacker obtaining information about the halftone secret image using the proposed OCHVC scheme. It provides the distributor's ability to reject the recovered image if a major change occurs based on the objective evaluation metrics' results. The determined objective evaluation metrics use many error metrics. To calculate the objective evaluation metrics, true positive (TP), false positive (FP), true negative (TN), and false negative (FN) should first be calculated concerning input and output images [5,28]. This work uses Gaussian attacks on the share images in communication channels using equation (12), and to evaluate the performance of the proposed OCHVC scheme, the following set of objective evaluation metrics are used: recall/sensitivity, precision, specificity, and accuracy metrics, as shown in equations (13–16) [13–15].

$$\text{Recall} = \frac{TP}{TP + FN}. \quad (13)$$

$$\text{Precision} = \frac{TP}{TP + FP}. \quad (14)$$

$$\text{Specificity} = \frac{TN}{TN + FP}. \quad (15)$$

Finally,

$$\text{Accuracy} = \frac{TP + TN}{TP + FP + FN + TN}. \quad (16)$$

Figure 13(a) and (b) shows the simulation interfaces of one share image exposed to Gaussian attacks, in which Figure 13(a) represents the interface of the training process. The dealer performs this process, which compares the original halftone cover image before embedding SIP and its corresponding share image after embedding SIP to compute the number of positive pixels (+), which means the pixels do not change. Still, negative pixels (–) indicate that the pixels change. Figure 13(b) represents the testing process interface, on which the dealer also performs this process. This process compares share images before sending to a subscriber and their corresponding shares in communication channels after exposure to Gaussian attacks. With initial parameters mean (μ) = 0 and standard deviation (std) = 20, this comparison is made by applying the objective evaluation metrics, and the results of these metrics are presented in Table 4.

Table 4 presents the ratio values recall, precision, specificity, and accuracy. It is divided into two sides. The first one represents the dealer side, and the second is the attacker side. The best results from the dealer side when the accuracy ratio becomes lower than the mean. Conversely, the best results from the attacker side when the accuracy ratio becomes higher than the mean. The dealer side value reflects the robustness of the proposed solution for sensing changes in the images coming from the channel. The results show that the proposed OCHVC scheme achieves high performance, but it cannot distinguish some of the changes in the shared image.

As shown in Table 4, the proposed OCHVC scheme is very sensitive to changes. The results of the performance metrics are affected when the shares are exposed to Gaussian attacks.

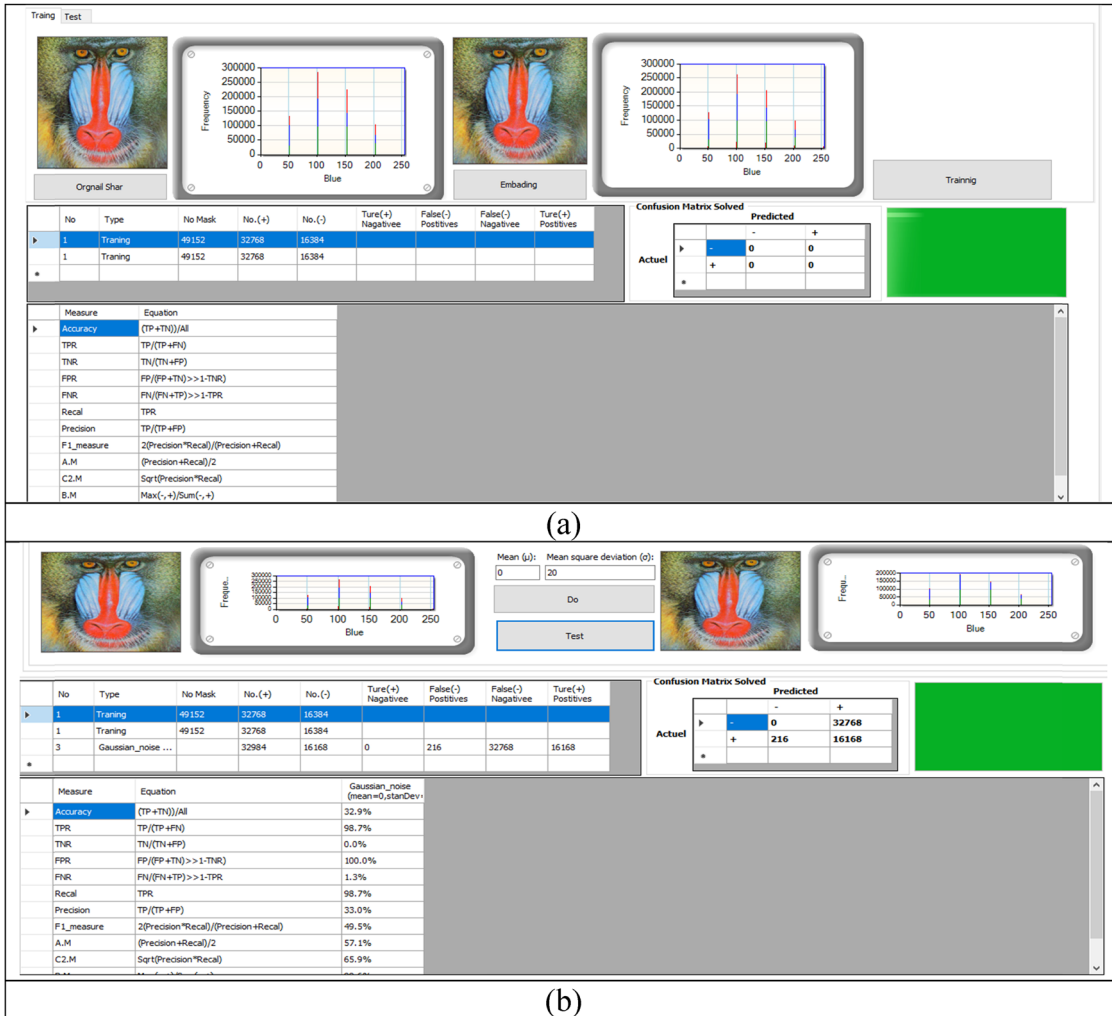


Figure 13: The interface of Gaussian attack initial parameters, mean (μ) = 0 and standard deviation (std) = 20: (a) interface of the training process and (b) interface of the testing process.

Table 4: Results of objective evaluation metrics

Evaluation metrics	Share 1 (%)	Share 2 (%)	Share 3 (%)	Share 4 (%)	Share 5 (%)	Share 6 (%)
Recall	98.7	98.8	98.6	98.6	98.7	98.7
Precision	33.0	33.1	33.0	33.0	30.0	30.0
Specificity	17.3	17.2	17.2	17.3	17.0	17.1
Accuracy	32.9	32.8	32.9	32.7	32.8	32.8

5.3 Comparing the OCHVC scheme with related work

Several studies have been concerned about VCs for images using different methods and techniques that have been adopted in the previous years. This section compares the proposed OCHVC scheme with some related methods based on a set of qualitative metrics of HVC, as presented in Table 5. Table 6 compares both the proposed OCHVC scheme and some related methods based on time complexity.

Table 5: Comparison between the proposed OCHVC scheme and related methods

HVC methods	Size of halftone cell	Type of secret image	Halftone technique	Algorithm locating SIP	Decoding operation	Type of code book	Shares contents
Zhou et al. [4]	2×2	Binary	Dithering	Void and clustering	OR operation	(2,2)-VCs code book	Random
Wang et al. [6]	2×2	Binary	Classical E-D	Random	OR operation	(2,2)-VCs code book	Random
Devi [7]	2×2	Binary	Classical E-D	Global optimization	OR operation	(2,2)-VCs code book	Random
Boyat and Joshi [22]	2×2	Binary	Adaptive E-D	Random	OR operation	(2,2)-VCs code book	Random
Yan et al. [10]	2×2	Binary	Classical E-D	Random	OR operation	(2,2)-VCs code book	Random
Thomas and Gharage [12]	2×2	Color	Adaptive E-D	Random	XOR operation	(2,2)-VCs code book	Random
Saturwar and Chaudhari [21]	2×2	Color	Adaptive E-D	Random	XOR operation	Hou color VCs code book	Random
Hodeish and Humbe [5]	2×2	Binary	Classical E-D	Random	XOR operation	(2,2)-VCs code book	Semi-random
Hameed and Ibrahim [8]	4×4	Color	Classical and modern E-D	Sequential and randomly using chaotic map	XOR operation	Dynamic code book	Semi-random
Proposed methods	4×4	Color	Classical and modern E-D	Randomly using a BA	XOR operation	Hash code book	Semi-random

Table 6: Comparison between the proposed OCHVC scheme and related methods based on time complexity

HVC methods	Time complexity	
	Construction cost	Retrieving cost
Zhou et al. [4]	$O(n^2)$	$O(n) \otimes$
Wang et al. [6]	$O(n^2)$	$O(n) \otimes$
Devi [7]	$O(n^2)$	$O(n) \otimes$
Boyat and Joshi [22]	$O(n^2)$	$O(n) \otimes$
Yan et al. [10]	$O(n^2)$	$O(n) \otimes$
Saturwar and Chaudhari [21]	$O(n^2)$	$O(n) \oplus$
Hodeish and Humbe [5]	$O(n^2)$	$O(n) \oplus$
Hameed and Ibrahim [8]	$O(n^2)$	$O(n) \oplus$
Proposed method	$O(n^2)$	$O(n) \oplus$

Table 5 presents the proposed schemes that have some features, such as supporting true color for secret and cover images [26,27]. Employing the XOR operation, dynamic codebook, the contents of shares generated are considered semi-random. Conversely, they are using sing Floyd–Steinberg error diffusion filters [28,29]. Finally, using two techniques for distributing SIP are considered sequential or random based on the BA. These features have made values of the image quality metrics shown in tables in previous sections toward the ideal values. For this reason, the proposed methods are more suitable for various applications like in refs. [28–30].

The proposed OCHVC scheme has the same time complexity as the previous related works in the construction of shares process, as illustrated in Table 6 and that it proves the strength of the proposed methods. In the recovery process, all related schemes' time complexity is $O(n)$ by using one OR or XOR operation. Still, the proposed model's complexity is $O(n)$ by using four XOR operations to recover the halftone secret image. The model is faster than the compared methods because the proposed model uses flags to recover halftone secret images.

The proposed OCHVC scheme of this work proves a novel HVCS for a color image. It includes a new technique to distribute the SIP into a halftone cover image in a random form based on a BA to make the OCHVC scheme more secure. Two limitations are identified in this model according to the research scope as follows:

- In the OCHVC scheme, the performance metrics results are affected when the shares are exposed to Gaussian attacks.
- The OCHVC scheme is tested only with a standard dataset. Therefore, testing it with images in different formatting such as RGB, JPEG, and BMP is recommended.
- The BA converges very quickly at the early stage, and then, the convergence rate slows down. This might affect the performance, especially when the number of evaluated points is not high.

6 Conclusion

This article proposes the OCHVC scheme using the Hash codebook and Floyd–Steinberg error diffusion halftone algorithm. The proposed scheme eliminates HVC constraints such as random shares pattern, a static codebook requirement to overcome all problems of fixed codebook like pixel expansion, low contrast that deals with high resolution of color images, set in consideration that halftone cell size is $[4 \times 4]$. The central concept of VCS is followed. The security condition is satisfied in the construction. Besides, applying XOR operation enables the scheme to check each share's authentication so that the dealer can determine the amount of change in each block in the decoding stage. The proposed OCHVC scheme employs novel embedding techniques to distribute SIPs into halftone cover images based on bat optimization algorithm

without affecting the visual quality on final shares and making it more secure. Moreover, the proposed system is applicable in IoT, cloud computing, and transmission media channels. The experiment and results of image quality metrics prove that the proposed OCHVC scheme has the ability to construct meaningful shares without cross-interference, and there is no effect of the secret image on the cover images. The proposed method has a high level of security and gives the dealer the ability to manage shares effectively. For future work, it is recommended to employ machine learning and deep learning techniques to secure the data during transmission from attacks such as Gaussian attacks. Also, the proposed scheme is not tested with real data; therefore, testing the proposed scheme in a real environment such as healthcare or medical imaging systems represents another future work.

Acknowledgment: The authors would like to thank the Center of Intelligent and Autonomous Systems (CIAS), Faculty of Computer Science and Information Technology, Universiti Tun Hussein Onn Malaysia (UTHM) for supporting this work.

Funding information: Communication of this research is made possible through monetary assistance by Universiti Tun Hussein Onn Malaysia and the UTHM Publisher's Office via Publication Fund E15216.

Conflict of interest: The authors have no conflicts of interest to declare. The authors certify that the submission is original work and is not under review at any other publication. All authors have seen and agree with the contents of the manuscript and there is no financial interest to report.

References

- [1] Chen WK. Image sharing method for gray-level images. *J Syst Softw.* 2013;86(2):581–5.
- [2] Naor M, Shamir A. Visual cryptography. In *Workshop on the Theory and Application of Cryptographic Techniques*. Berlin, Heidelberg: Springer; 1994 May p. 1–12.
- [3] Wang Z, Arce GR. Halftone visual cryptography by iterative halftoning. 2010 IEEE International Conference on Acoustics, Speech and Signal Processing. Dallas, TX, USA: IEEE; 2010 Mar. p. 1822–5.
- [4] Zhou Z, Arce GR, Di Crescenzo G. Halftone visual cryptography. *IEEE Trans Image Process.* 2006;15(8):2441–53.
- [5] Hodeish ME, Humbe VT. An optimized halftone visual cryptography scheme using error diffusion. *Multimed Tools Appl.* 2018;77(19):24937–53.
- [6] Wang Z, Arce GR, Di Crescenzo G. Halftone visual cryptography via error diffusion. *IEEE Trans Inf Forensics Secur.* 2009;4(3):383–96.
- [7] Devi ES. Enhanced visual secret sharing scheme via halftoning technique. 2010 International Conference on Communication Control and Computing Technologies. Nagercoil, India: IEEE; 2010 Oct. p. 769–76.
- [8] Hameed RS, Ibrahim AWS. Color halftone visual cryptography scheme using dynamic codebook and error diffusion technique. *Iraqi J Inf Technol.* 2019;9(4):2018.
- [9] Liu Y, Wang Z. Halftone visual cryptography with color shares. 2012 IEEE International Conference on Granular Computing. Hangzhou, China: IEEE; 2012 Aug. p. 746–9.
- [10] Yan X, Wang S, Niu X, Yang CN. Halftone visual cryptography with minimum auxiliary black pixels and uniform image quality. *Digital Signal Process.* 2015;38:53–65.
- [11] Snyder J. Visual cryptography and secret image sharing. *J Electron Imaging.* 2012;21(1):019901.
- [12] Thomas SA, Gharge S. Halftone visual cryptography for grayscale images using error diffusion and direct binary search. 2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI). Tirunelveli, India: IEEE; 2018 May. p. 1091–6.
- [13] Abdulsahib AA, Mahmoud MA, Mohammed MA, Rasheed HH, Mostafa SA, Maashi MS. Comprehensive review of retinal blood vessel segmentation and classification techniques: intelligent solutions for green computing in medical images, current challenges, open issues, and knowledge gaps in fundus medical images. *Netw Model Anal Health Inform Bioinform.* 2021;10(1):1–32.
- [14] Abd Ghani MK, Mohamed MA, Mostafa SA, Mustapha A, Aman H, Jaber MM. The design of flexible telemedicine framework for healthcare big data. *Int J Eng Technol.* 2018;7(320):461–8.
- [15] Elhoseny M, Mohammed MA, Mostafa SA, Abdulkareem KH, Maashi MS, Garcia-Zapirain B, et al. A new multi-agent feature wrapper machine learning approach for heart disease diagnosis. *Comput Mater Contin.* 2021;67:51–71.

- [16] Husham S, Mustapha A, Mostafa SA, Al-Obaidi MK, Mohammed MA, Abdulmageed AI, et al. Comparative analysis between active contour and otsu thresholding segmentation algorithms in segmenting brain tumor magnetic resonance imaging. *J Inf Technol Manag.* 2020;12(Special Issue):48–61.
- [17] Khalaf BA, Mostafa SA, Mustapha A, Mohammed MA, Mahmoud MA, Al-Rimy BAS, et al. An adaptive protection of flooding attacks model for complex network environments. *Secur Commun Netw.* 2021;2021:1–17.
- [18] Hameed RS, Ibrahim AS. Halftone visual cryptography scheme for color image using dynamic codebook and chaotic maps. *J Eng Appl Sci.* 2019;13(24):8600–8.
- [19] Floyd RW, Steinberg L. An adaptive algorithm for spatial grey scale. *Proc Soc Inf Display.* 1976;17:75–7.
- [20] Patel SB, Desai Vinod L. Comparative study and analysis of halftone visual cryptography via error diffusion. *Int J Adv Res Comput Sci Softw Eng.* 2016;6(1):250–4.
- [21] Saturwar J, Chaudhari DN. Secure visual secret sharing scheme for color images using visual cryptography and digital watermarking. *Second International Conference on Electrical, Computer and Communication Technologies (ICECCT).* Vol. 4, Issue 3. India: IEEE; 2017. p. 1–4.
- [22] Boyat AK, Joshi BK. A review paper: noise models in digital image processing. *arXiv preprint arXiv:1505.03489.*
- [23] Kotteeswaran R, Sivakumar L. A novel Bat algorithm based re-tuning of PI controller of coal gasifier for optimum response. *Mining intelligence and knowledge exploration.* Cham: Springer; 2013. p. 506–17.
- [24] Jubair MA, Mostafa SA, Muniyandi RC, Mahdin H, Mustapha A, Hassan MH, et al. Bat optimized link state routing protocol for energy-aware mobile ad-hoc networks. *Symmetry.* 2019;11(11):1409.
- [25] Prabhishak S, Aayush A, Jyoti G. Image watermark attacks: classification & implementation. *Int J Electron Commun Technol.* 2013;4(2):95–100.
- [26] Fadel H, Hameed RS, Hasoon JN, Mostafa SA, Khalaf BA. A light-weight ESalsa20 Ciphering based on 1D logistic and chebyshev chaotic maps. *Solid State Technol.* 2020;63(1):1078–93.
- [27] Ibrahim DR, Abdullah R, Teh JS. An enhanced color visual cryptography scheme based on the binary dragonfly algorithm. *Int J Comput Appl.* 2020;1–10.
- [28] Alex NS, Jani AL. Enhanced image secret sharing via error diffusion in halftone visual cryptography. *IEEE 3rd International Conference on Electronics Computer Technology.* Kanyakumari, India: IEEE; 2011. p. 393–7.
- [29] Pahuja S, Kasana SS. Halftone visual cryptography for color images. *2017 International Conference on Computer, Communications and Electronics (Comptelix).* Jaipur, India: IEEE; 2017 July. p. 281–5.
- [30] Ismael HA, Abbas JM, Mostafa SA, Fadel AH. An enhanced fireworks algorithm to generate prime key for multiple users in fingerprinting domain. *Bull Electr Eng Inform.* 2021;10(1):337–43.