symmetry

Article

A Novel Color Visual Cryptography Approach Based on Harris Hawks Optimization Algorithm

Dyala Ibrahim [1], Rami Sihwail [1,*], Khairul Akram Zainol Arrifin [2,*], Ala Abuthawabeh [3] and Manar Mizher [1]

[1] Department of Cyber Security, College of Computer Science and Informatics, Amman Arab University, Amman 11953, Jordan; d.ibrahim@aau.edu.jo (D.I.); mmizher@aau.edu.jo (M.M.)
[2] Department of Cyber Security, Faculty of Information Science & Technology, Universiti Kebangsaan Malaysia, Bangi 43600, Selangor, Malaysia
[3] Department of Software Engineering, College of Computer Science and Informatics, Amman Arab University, Amman 11953, Jordan; a.abuthawabeh@aau.edu.jo
* Correspondence: r.sihwail@aau.edu.jo (R.S.); k.akram@ukm.edu.my (K.A.Z.A.)

Abstract: Hundreds of millions of people worldwide use computing devices and services, including smartphones, laptops, and messaging apps. Visual cryptography (VC) is one of the most secure encryption methods for image encryption in many applications, such as voting security, online transaction security, and privacy protection. An essential step in VC is encrypting secret images into multiple digital shares to hide them with the intention of successfully reverting them to their original form. Hence, a single share cannot reveal information about the secret image. Issues including pixel enlargement, high processing costs, and low decryption quality influence the current state of VC. We address these issues by introducing a novel technique based on (2, 2) secret sharing and the algorithm of Harris hawks optimization (HHO) for color photos. For the encryption process, the appropriate color levels are determined using the HHO algorithm. Consequently, images are decrypted with improved quality and a small impact on the overall processing complexity. The suggested scheme is also non-expandable due to the equal size of the initial secret image and the shared images. This results in lower memory requirements and improved image quality. The approach is applied to a set of well-known benchmark images. Moreover, a set of standard metrics is used to assess the robustness of the proposed scheme, including its capability in defending against cryptanalytic attacks, a correlation, a histogram, and the quality of encryption. According to the findings, the proposed solution provides better reconstructed image quality, time-efficient encryption, and nearly optimal statistical properties compared to previous approaches.

Keywords: visual cryptography; Harris hawk optimization; HHO; optimization; image encryption; cyber security

check for updates

Citation: Ibrahim, D.; Sihwail, R.; Arrifin, K.A.Z.; Abuthawabeh, A.; Mizher, M. A Novel Color Visual Cryptography Approach Based on Harris Hawks Optimization Algorithm. *Symmetry* **2023**, *15*, 1305. https://doi.org/10.3390/sym15071305

Academic Editor: Christos Volos

Received: 21 April 2023
Revised: 23 May 2023
Accepted: 12 June 2023
Published: 24 June 2023

1. Introduction

With the widespread implementation of technological solutions, the dissemination of visual information has expanded rapidly. For a long time, the mechanism of securely sending data over a network has been the focus of computer scientists. Due to the prevalence of cybercrime today, keeping a secret while navigating the web is incredibly challenging. To protect against cybercrime and ensure safe data transmission, data scientists and researchers are working hard to implement multiple methods and techniques. Photos have been used to pass on secrets from one person to another for years [1]. However, recently, the focus has been on making this process as safe as possible. Data privacy is protected in modern transmission channels primarily through steganography [2] and visual cryptography [3,4]. Visual cryptography (VC) is one of the most widely used image-based encryption techniques because it is effortless, efficient, and secure [5]. VC was first used to solve the secret sharing problem of binary images by Noar and Shamir in 1995 [6]. To encrypt a particular image, VC first encrypts it into a series of random pieces (shares). In order to reassemble the original picture, these shares must be superimposed (overlapping). The original image involves dividing a secret black-and-white image into several parts using two matrices, one for each color used [7].

Computing devices and services, such as smartphones, laptops, and messaging programs, are used by hundreds of millions of people worldwide. To protect the information on these devices, the encryption feature is enabled. Further, these services and devices can provide encrypted communications for their customers. Encryption is used to combat the dangers posed by diverse actors, including unsophisticated and sophisticated criminals, foreign intelligence agencies, and authoritarian governments. Individuals, businesses, and governments all rely on encryption to do this. Encryption is a crucial technology, but it cannot address the problem of ensuring adequate security for data and systems by itself. On the other hand, criminals also rely on encryption to escape investigation and prosecution. Encryption makes law enforcement and intelligence investigations harder. When communications are encrypted "end-to-end", no one can understand the intercepted messages. If a smartphone is locked, encrypted, and taken by law enforcement, the information cannot be read [8–10].

Encryption techniques are classified as symmetric, asymmetric, and visual cryptography [11]. The symmetric technique requires a single key (private key) for encryption and decryption. Asymmetric encryption relies on two keys: a public key is used for encryption and a private key is used for decryption. Visual cryptography (VC) has many applications in privacy protection, online transaction security, and voting security. VC is used to solve the secret-sharing problem. When the secret image is decomposed into shares, each of these shares cannot reveal any clues about the secret image. Conversely, stacking these shares up allows the decrypted image (secret image) to be revealed. However, applying a hybrid scheme, in which VC and symmetric techniques are hybridized, may strengthen security in most cases [11–15]. Our scheme has the following advantages over existing schemes: it includes color-shared images, no computation is required for decoding, and there is no interference from the shared image with the recovered secret image.

A (k, n) VC approach obscures the secret image into n components requiring at least k shares for decrypting and recovering the image to the original. There are no elaborate mathematical calculations needed for this. Metrics such as contrast and pixel expansion (how many decomposed sub-pixels are extracted from each source image pixel) are used to assess the efficacy of VC methods. A VC scheme aims to maximize the contrast of the decrypted image while avoiding large shares by minimizing the expansion of pixels. When each pixel in the secret image is encrypted to many sub-pixels, affecting the size of the shares, the size might be doubled or tripled; accordingly, the contrast of the decrypted images and the quality of the encrypted image will be low [7]. Bank applications [16,17], electronic voting systems [18], and authentication systems [19] are just a few of the many places you can put VC to use. Studies of steganography and VC to leverage the security level of data transmission have also been conducted [20,21]. There is a strong relation between the decryption procedure in VC and the decrypted image quality. There are two methods for decryption: logical OR and XOR. Each black pixel, 1, can be reconstructed using OR by computing 1 V 0 or 1 V 1, where V represents the OR operation. However, to decipher white pixels representing a value of 0, the equation 0 V 0 must be applied. As a result, the recovered images using OR-based VC schemes always contain a small amount of distortion, and the maximum value of the relative contrast is always less than 1. Thus, this indicates that there are still flaws in the recovery method. Alternatively, the decryption method can also be applied using XOR, as described in [22]. As Fu et al. demonstrated, the direct XORing of shares allows for flawless image recovery when using OR-based schemes based on much smaller share sizes [23].

To allocate the best subset of features, a variety of search methods can be used, such as a greedy search, random search, and meta-heuristic search. A greedy search is used to evaluate all the dataset's feature combinations. However, it takes a long time to complete. By contrast, the best subset of features can be explored randomly in random search methods.

However, there is a chance it might get trapped in a local solution [24]. Meta-heuristic methods, on the other hand, mimic natural biological or physical phenomena as well as animal behaviors in exploring the search space. Due to their success, meta-heuristic search techniques have been successfully used in a variety of fields, including machine learning [12,13,25–30].

HHO is one of the recent meta-heuristics developed by Heidari et al. [31]. It is considered a powerful, fast, and effective optimization algorithm. The algorithm imitates Harris Hawk birds in their hunting and chasing behavior. In HHO, a rabbit represents prey, which is the ideal solution to the problem found by the algorithm. According to [31], HHO outperformed other well-known meta-heuristic algorithms, including PSO, GA, GOA, ALO, WOA, and BOA, in 29 benchmark datasets used to test the algorithm that mirror real-world engineering tasks.

This paper presents an improved (2, 2) threshold scheme for color images by exploiting Harris hawks optimization (HHO). The first contribution deploys HHO to find three optimal solutions for each color channel: R, G, and B. These solutions will maximize the quality of the recovered image. Then, we propose an improved color VC scheme based on the HHO algorithm. Due to using the probabilistic method, the proposed scheme is not burdened by pixel expansion. We evaluate the proposed scheme by many metrics, such as the number of pixels change rate (*NPCR*), unified average changed intensity (*UACI*), correlation, entropy, and peak signal-to-noise ratio (*PSNR*), then compare the results with those of existing schemes [32]. The proposed scheme has a lower computational complexity due to the need for the pre-processing of the original images as well as higher encryption and security compared to other schemes. Additionally, there is no need to expand pixels under the proposed scheme, which is more efficient in terms of space and memory. Having these qualities allows the new approach to be applied in various situations. For example, it can be used for authentication methods such as multifactor authentication.

The paper has six sections, including a review of related work (Section 2) and a brief introduction to color VC and HHO (Section 3). The fourth section discusses the proposed procedure, followed by a detailed analysis (Section 5). Finally, the conclusion is presented in Section 6.

2. Related Works

Grayscale and binary images were the only ones used in early-stage VC schemes [7]. Later, in 2003, Hou applied the principle to multi-layered color images with transparency [32]. Other works following previous approaches have been proposed for encryption and decryption procedures that would improve security by making image reconstruction more effective. Through decreased pixel expansion and cross-interference incidences, Wu and Yang (2020) presented two new approaches for a probabilistic color visual cryptography scheme with a threshold of (k, n), which uses colors to solve the expanding pixels issue. In experiments, both proposed approaches demonstrated the ability to meet security and contrast criteria requirements. Further, the proposed approaches were shown to be practical and advantageous through a theoretical analysis and experiments [33].

Furthermore, Aswad et al. (2021) attempted to enhance the visual quality of shared images. The authors developed an optimized color halftone visual cryptography scheme (OCHVC) by combining two proposed approaches: a hash codebook and a construction technique. Considering the new methods, the pixels' information from the secret image was randomly distributed into a halftone cover image using a bat optimization algorithm. Thus, the proposed OCHVC scheme was more secure when using these methods. The results revealed that the OCHVC scheme achieved an *MSE* of 95.00%, a *PSNR* of 28.30% at the peak signal-to-noise ratio, an *NPCR* of 99.40%, and a *UACI* of 97.30% on average across all six stocks. The outcomes of the experiments reflecting the image quality metrics demonstrated that the OCHVC scheme can enhance visual quality and recover images securely. This is in addition to its ability to share meaningful images [34].

Based on visual cryptography exploiting public key encryption, an authentic secret-sharing approach was presented by Karolin and Meyyappan in 2021. This approach involved applying the RSA algorithm to multiple copies of secret images to encrypt and decrypt them. The encryption process used a multiplication technique to generate keys that were then used to encrypt data using public keys and decrypt them using private keys. The *MSE* (the mean square error) and *PSNR* (the peak signal-to-noise ratio) were used to evaluate the quality of the hidden images. The *PSNR* value of the decrypted image was found to be 156.32 through experimentation, with an *MSE* value of 0.5031. To determine the level of protection afforded by a hidden picture, the researchers compared the values of the *UACI* (the unified averaged changing intensity) and *NPCR* (the number of pixel change rate). According to the experiment's findings, the image's *NPCR* value was 69.44, and its *UACI* value was 13.88. As a result, the suggested approach was more effective and offered higher security and quality when exchanging private images [35].

Moreover, other researchers have also suggested an improved VC approach that works with binary and color images and uses enhanced half-tone technology. The proposed algorithm has three phases: detection, encryption, and decryption. (2, 2) visual cryptography, the half-tone technique, encryption, and the idea of fake shares all contribute to increasing security. The genuine user is thus given access to the original restored image. However, a person who enters the wrong password is given a combination of any fake share with any real share. The proposed method can efficiently process colored and black-and-white images [36].

The binary dragonfly algorithm was presented by Ibrahim in 2022 using (2, 2) secret sharing for color images. With the dragonfly algorithm, achieving optimal color levels during encryption leads to higher-quality reconstructed images upon decryption at a negligible computational cost. In the proposed approach, each shared image's size and the original image's size are the same, which is also non-expandable. As a result, the image quality is improved while the memory usage is reduced. The quality of the encryption, entropy, histogram, and correlation was evaluated to determine how well the proposed approach stood up to cryptanalytic attacks. The results demonstrated that the new visual secret-sharing approach improved upon prior developments in encryption speed, reconstructed image quality, and statistical characteristics [23].

3. Background

The proposed approach is based on two existing algorithms: visual cryptography and Harris hawks optimization. As a context for the proposed visual cryptography, the following subsections give an overview of these two seminal techniques.

3.1. Visual Cryptography of Color Images

Visual encryption (VC) was developed by Naor and Shamir [6]. VC uses human vision to decrypt secret data instead of sophisticated mathematical calculations or decryption hardware, which makes it different from traditional cryptographic techniques. VC involves encrypting a single image into two noisy images, referred to as shares. In order to recover the hidden image during the decryption process, the shares are superimposed [4]. Nair and Shamir developed this fundamental idea as the (k, n) secret sharing technique, where n is the total number of shares and k is the minimal number of shares necessary to recover the secret. Since each of these pixels is independently managed, each will be represented by n different versions (in corresponding shares). A group of m grayscale subpixels is contained within each of these n shares. The created structure can be represented as a matrix with the notation $S = [Si,j]$, where Si,j equals 1 if and only if the jth sub-pixel in the ith transparency is black, and the sub-pixel is white when Si,j equals zero. When the layers of transparency (i_1, i_2, i_3, ... i_n) in S are layered (stacked) one on top of the other, the OR operation performed on the rows of i_1, i_2, i_3, ... i_n in S produces black pixels. A user's visual system can differentiate between black and white pixels based on a predetermined threshold. This threshold has a relative contrast that is greater than 0 and $d \in [1, m]$. If the hamming weight of the ORed m-vector H (V) $\geq d$, the resulting pixel is considered to be black. If H (V) is less than $d - am$, then the pixel is considered to have a white value. Shares are composed of matrices, which are randomly selected based on the positions of each pixel in the original image. For instance, matrices starting with C_1 are included in the shares if the first pixel in the source image is black. The selection will switch to matrices starting with C_0 if the second pixel is white.

Examining fewer than k components or shared images by a cryptanalyst using high-performance computers cannot reveal the initial color, despite the fact that the approach is conceptually straightforward.

As mentioned in Section 2, color visual cryptography was invented by Hou [32]. There are three methods suggested for visual cryptography of grayscale and color images, all of which are based on prior research in black-and-white visual cryptography, halftone technology, and color decomposition. These approaches maintain the advantages of black-and-white visual cryptography, which relies on the human visual system to decrypt secret images without the need for computation. However, they also have backward compatibility with earlier findings in black-and-white visual cryptography, such as the t out of n threshold scheme. Moreover, they are simple to apply to both grayscale and color images. Therefore, they have all the benefits of black-and-white visual cryptography without any disadvantages.

Our proposed VC approach incorporates techniques taken from combining Nair and Shamir's shared generation process with the color decomposition approach in the HHO algorithm. By selecting color levels optimally, high-quality reconstruction images can be achieved without pixel expansion. Details regarding HHO are discussed in the following subsection.

3.2. Harris Hawks Optimization

The HHO algorithm was inspired by the surprise pounce and seven killing tactics of the Harris's hawk in nature [26,37]. This behavior involves hawks working together to hunt their prey. In this cunning tactic, several hawks work together to attack their prey from a variety of directions at the same time. Throughout their lives, Harris hawks have shown various chase patterns. These patterns are determined by the prey's agility and behaviors as they try to escape. The HHO has a few mechanisms for exploration and exploitation, contributing to its significant advantages, including its ease of use. In addition, it has a reduced number of control parameters and a high rate of convergence [31,38].

The following subsection discusses the mathematical model for HHO, which includes exploration and exploitation phases.

3.2.1. Exploration Phase

Although the Harris's hawk's strong eyesight enables it to recognize and track prey, there are times when prey is not visible. In this situation, the hawks wait on the top of trees surveying the area for potential prey. The hawks' positions are considered candidate solutions in the HHO algorithm, but the prey is always treated as the most optimal solution or situation at each iteration. Hawks use two hunting techniques that require them to perch in specific locations and constantly scan their surroundings to identify their prey.

Based on the relative positions of the other family members, the hawks decide where to roost when $p < 0.5$. Within the population area completely at random, the hawks pick a perching spot when $p \geq 0.5$, as shown in the following equation:

$$A(X+1)\begin{cases} (A_r) - a_1|A_a(x) - 2a_2A(x)| & , \ p \geq 0.5 \\ A_{rabbit}(x) - A_P(x)) - a_3(L_B + a_4(U_B - L_B)), & p < 0.5' \end{cases} \tag{1}$$

As shown in Equation (1), $A(x+1)$ represents the hawks' position in the next iteration, and $A_{rabbit}(x)$ represents the rabbit's position. $A(x)$ represents the current position of the hawks. p, a_1, a_2, a_3, and a_4 are random variables that are generated from a range of 0 to 1.

L_B and U_B refer to the lower and upper bands of the random variables. $A_P(x)$ represents the average hawk's position, as represented by Equation (2).

$$A_P(x) = \frac{1}{H} \sum\nolimits_{i=1}^{H} A_i(x), \tag{2}$$

where $A_i(x)$ represents the location of each hawk at *i*th iteration, and H denotes the number of hawks in the search space.

3.2.2. Transition from Exploration to Exploitation

This subsection explains the transition from the exploration phase to the exploitation phase. In HHO, the transition is based on the prey's energy level to escape, which can be mathematically defined as follows:

$$P = 2P_0\left(1 - \frac{x}{I}\right), \tag{3}$$

In an iteration, P stands for the prey's energy to escape. I denotes the overall number of iterations. P_0 represents the initial energy of the prey. The prey's energy level dramatically decreases during the escaping process. In every iteration, P_0 will change its value between (−1,1). According to this range, when the P_0 value decreases from 1 to 0, the prey is exhausted. However, when the value increases from 0 to 1, the prey is reinforced. When $|P| \geq 1$, the exploration phase begins. However, when $|P| < 1$, the exploitation phase is initiated.

3.2.3. Phase of Exploitation

This phase uses four parameter sets that help the hawks plan an attack against the prey: hard besiege, soft besiege, hard besiege with progressive rapid dives, and soft besiege with progressive rapid dives.

The prey flees from the hawks during the soft besiege phase by jumping randomly while exerting less energy. At this point, Harris hawks softly encircle the prey, instructing it to consume any remaining energy before performing an unexpected pounce attack. The equation of the soft besiege can be defined as follows:

$$Y(t+1) = \Delta Y(t) - Energy|JY_{rabbit}(t) - Y(t)|, \tag{4}$$

$$\Delta Y(t) = Y_{rabbit}(t) - Y(t), \tag{5}$$

where $Y_{rabbit}(t)$ is the rabbit's position vector, and $Y(t)$ is the rabbit's current location. The difference between the rabbit's position vector and its current location in iteration t is represented by $\Delta Y(t)$.

Hawks quickly encircle their prey and use surprise pounces during the hard besiege phase by updating their exact location. The prey is worn out and has little ability to flee at this point. Harris hawks also surround their prey before making a surprise pounce.

$$Y(t+1) = Y_{rabbit}(x) - Energy|\Delta Y(t)|, \tag{6}$$

Progressive rapid dives help to create a soft besiege for a surprise pounce. This is more intelligent than the earlier ones due to the escape energy of the prey. Equation (7) demonstrates that a successful hunting technique of hawks is based on locating themselves in accurate positions to attack prey, which can be mathematically formulated as follows:

$$X = Y_{rabbit}(t) - Energy|JY_{rabbit}(t) - Y(t)|, \tag{7}$$

The most appropriate dive is chosen by comparing potential results to past dives. Hawks may suddenly increase their rapid diving behavior when conditions are unfavorable to catch prey through the Levy flight (*LF*) strategy, as shown in Equation (8):

$$W = X \times V \times LF(dimension), \tag{8}$$

Dimension refers to the dimensions of solutions, and *V* = A vector of random size 1 × *dim*, where *LF* is applied as follows:

$$LF(x) = 0.01 \times \frac{\cup \times \sigma}{|\cup|^{\frac{1}{\beta}}}, \sigma = \left[\frac{\tau(1+\beta) \times sin\left(\frac{\pi\beta}{2}\right)}{\tau\left(\frac{1+\beta}{2}\right) \times \beta \times 2^{\left(\frac{\beta-1}{2}\right)}} \right], \tag{9}$$

where β is a constant, and v and u are random values. Next, an update of the hawks' positions through progressive rapid dives is shown in Equation (10), where *X* and *W* are calculated by Equations (7) and (8). Thus, Equation (10) is calculated as follows:

$$Y(t+1) = \begin{cases} X & \text{if } F(X) < F(Y(t)) \\ W & \text{if } F(W) < F(Y) \end{cases}, \tag{10}$$

Finally, the last step employs Equation (11) to reduce the hawks' average location distance for approaching their prey as their prey lacks the energy to flee.

$$Y(t+1) = \begin{cases} X & \text{if } F(X) < F(Y(t)) \\ W & \text{if } F(W) < F(Y) \end{cases}, \tag{11}$$

where:

$$X = X_{rabbit}(t) - E|JX_{rabbit}(t) - X_m(t)|, \tag{12}$$

$$W = X + S \times LF(dimension), \tag{13}$$

Further, Algorithm 1 summarizes the original Harris hawks optimization algorithm (HHO).

Algorithm 1: HHO Algorithm [20]

```
Inputs: Hyperparameters for CNN.
Outputs: Optimized hyperparameters.
Initialize the population $Y_i$ ($i$ = 1, 2 . . . )
while condition is not being met do
    Determine the fitness rate of hawks.
    $Y_{rabbit}$ is chosen as the best position
    for every week $(Y_i)$ do
        Update the jump capacity $J$ and initial energy $Energy$
        Energy = 2rand () − 1, $J$ = 2(1 − rand ())
        Update $Energy$ using Equation (3)
    if $|Energy| \geq 1$ then
        Update the position vector using Equation (1)
    if $|Energy| < 1$ then
    if $s \geq 0.5$ and $|Energy| \geq 0.5$ then
        Update the position vector using Equation (4)
    else if $s \geq 0.5$ and $|Energy| < 0.5$ then
        Update the position vector using Equation (6)
    else if $s < 0.5$ and $|Energy| \geq 0.5$ then
        Update the position vector using Equation (10)
    else if $s < 0.5$ and $|Energy| < 0.5$ then
        Update the position vector using Equation (11)
```

4. Proposed Method

To determine color levels, the presented VC approach applies HHO to split a color image into several shares. Incorporating HHO is essential for enhancing encryption quality and reducing time complexity. Considering each color component (R, G, and B) entails deriving distinct matrices from the original colored secret image, where an element of each matrix represents a pixel value *Pval*. Then, these values are used to generate shared images, as illustrated in Figure 1. The following subsections discuss each significant phase in detail.

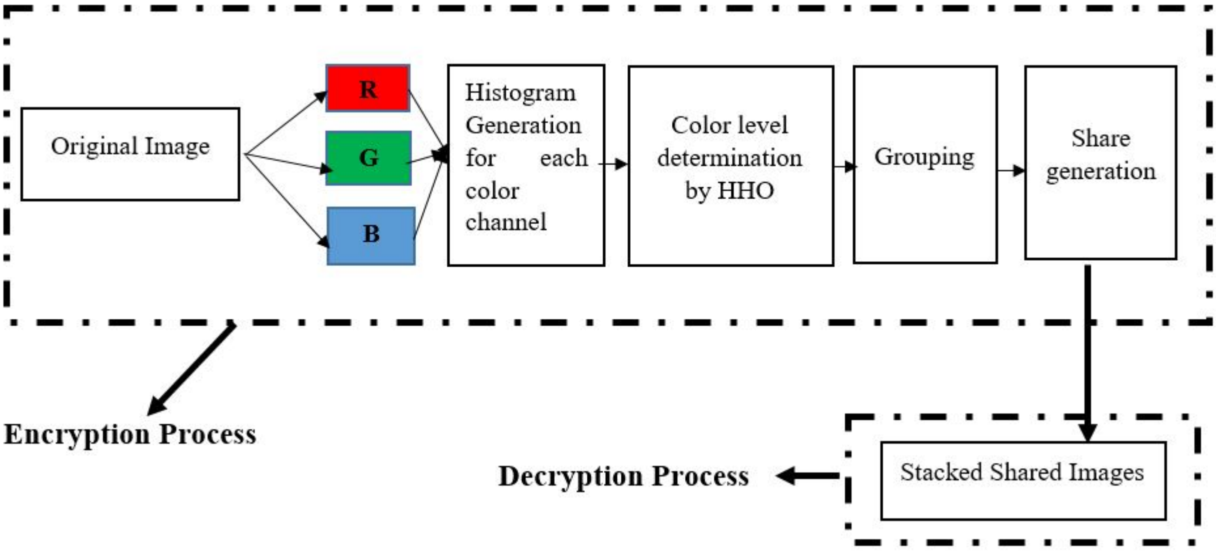


Figure 1. The proposed approach including both the stages of the encryption process and the decryption process.

4.1. Decomposing Color Image

At the initial stage of the process, the original image color is represented by RGB pixel values *I*. Then additional matrices are derived from *I* to indicate RGB pixel values as R_p, G_p, and B_p elements separately. These elements have the same dimensions as *I*. *H* is the height of the secret image, and *W* is the width of the secret image, respectively. The image's original pixel values are represented as shown in Figure 2, Lena's image. Equation (14) represents the extracted pixels of the colored secret images which consist of red, green, and blue pixels.

$$P_{val} = \sum(R_p + G_p + B_P), \tag{14}$$

Figure 2. The image of Lena.

4.2. Generating Histograms

Histograms representing intensity distributions are created following the color decomposition phase for each color channel. As seen in the preceding image (Figure 2), each color channel's distribution is represented by one of the three histograms in Figure 3. In the R histogram, the R's intensity values are indicated on the *X*-axis, with a scale from 0 to 255 being used. The frequency of each intensity is reflected on the *Y*-axis. The same axes are displayed in the G and B histograms measuring data related to G and B.

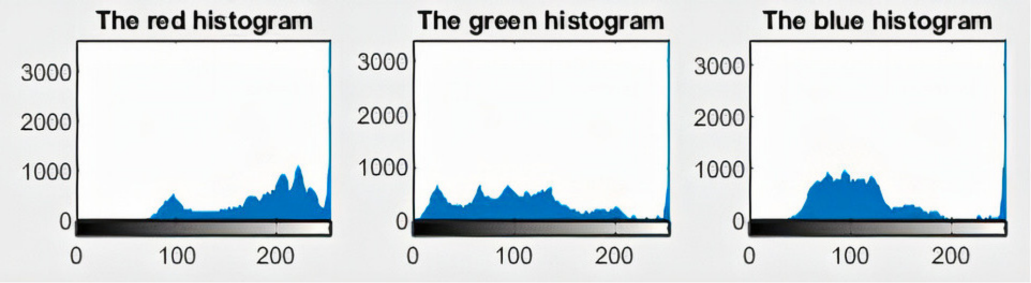


Figure 3. This figure shows the histogram of Lena's image for red, green, and blue histograms.

Histograms, which represent the proportion of pixels with a given color for each intensity level, are necessary to understand the intensity distribution for each channel.

4.3. Color Determination Level

One of the proposed scheme's most crucial features is using an optimized algorithm to identify color levels during the encryption process. HHO is a well-known illustration of an optimization algorithm for choosing levels of channel intensity. Color levels are selected using HHO to reduce the *PSNR*.

The *PSNR* is obtained by comparing the shared and source images (Section 5 provides more details about the image share generation). The large difference between the source image and the shared image is indicated by low *PSNR* values, which leads to a high level of encryption quality and security. For each color channel, the operation of the HHO runs synchronously. Individual color levels X_R, X_G, and X_B are represented by eight-bit values (with a scale of 0–255), with 24 bits in total. Three hawks are designated as $X_{R1} \ldots X_{Rn} \ldots X_{G1} \ldots X_{Gn}$, and $X_{B1} \ldots X_{Bn}$, where $n = 8$. By running HHO a thousand times, the CC and *PSNR* act as fitness functions to determine the optimal color level. The technique of determining the color level for each color using HHO is illustrated in Figure 4, in which the best location is selected as the best color level.

4.4. Grouping

For all N_x segments, where N refers to the number of pixels in the same segment with a similar total pixel count, it is necessary to resolve the issue of pixel expansion. As mentioned previously, the proposed approach's goal of eliminating pixel expansion is to reduce time complexity. It also enhances the quality of the reconstructed image by generating the same proportion of shares as that of the source of the secret image.

4.5. Generating Share

A share-generation process is used separately for each color channel. During the first phase, a combination of Boolean matrices, ShareR1, ShareG1, ShareB1 and ShareR2, ShareG2, and ShareB2, for each color channel is produced. Having the same proportions between each share and the hidden image, each share's pixel is calculated based on the probability of color levels determined by a probability solution in HHO [3]. As shown in Figure 5, the encrypted images look like disordered images.

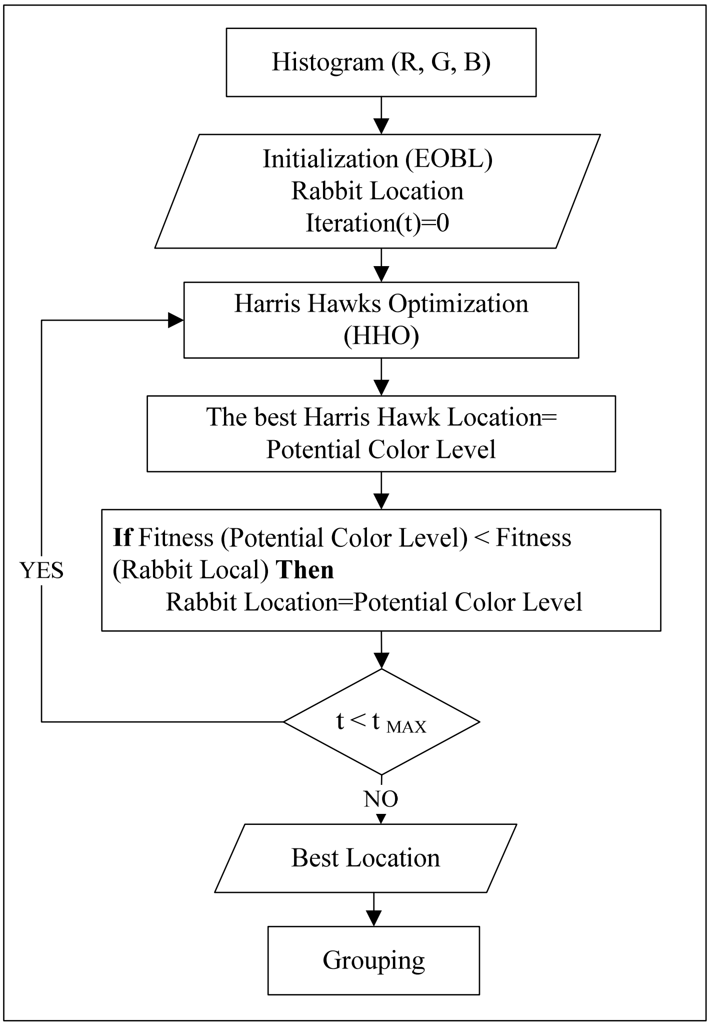


Figure 4. The technique of determining the color level for each color using Harris hawk optimization (HHO).

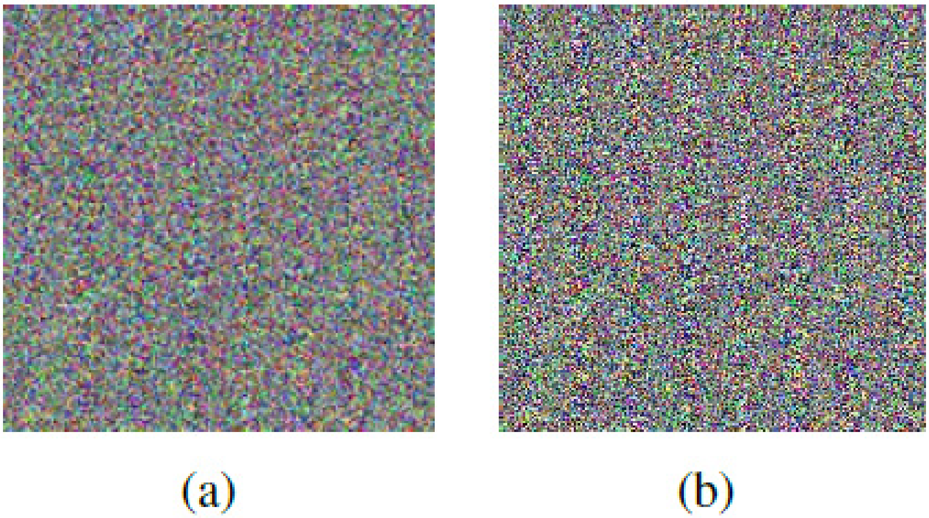


Figure 5. Encrypted images illustrating Share 1 (**a**) and Share 2 (**b**).

4.6. The Process of Decryption

Equation (15) describes the mathematical method for digitally overlapping shares as part of the decryption process, as shown in Figure 6, the decrypted image.

$$Recovered\ image = Share1 \oplus Share, \tag{15}$$

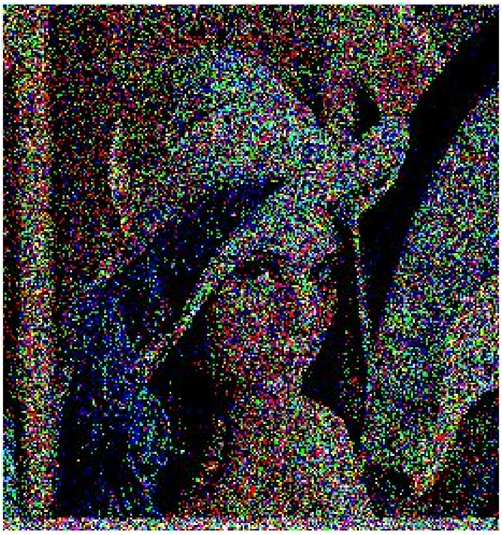


Figure 6. The recovered image of Lena.

5. Experimental Analysis and Results

In this section, the results confirm that the presented approach is accurate and efficient. We evaluate the proposed (2, 2) VC approach's performance using a variety of statistical-based techniques and compare the results with those of other VC approaches that have recently been introduced [21,36]. To confirm the efficiency of the presented approach, the quality of shared and recovered images will suffer if the pixel expansion parameter is set to $m \geq 1$. In contrast to the original image size, the shared and recovered image size will be doubled or tripled, increasing the memory requirements of the scheme. According to the proposed algorithm, the pixel expansion equals 1, which means that the recovered image will be identical to the original image, and there will be no memory consumption. In addition, most studies utilize Lena, Jet, Barbara, and Sailboat photos for performance evaluation.

5.1. Analysis of NPCR and UACI

The *NCPR* (the number of pixel change rate) and *UACI* (the unified averaged changed intensity) measures are used to quantitatively analyze the differences between the original and shared images. To determine the quality of defense against differential attacks, large values of the *NPCR* and *UACI* are frequently used. This ensures that any small change to the secret image results in entirely different shares [36]. Equations (16) and (18) show the *NPCR* and *UACI* formulas.

$$NPCR = \frac{\sum_{i,j}^{M,N} D(i,j)}{M \times N} \times 100\%, \tag{16}$$

$$\left\{ D(i,j) = \begin{cases} 1, \text{ if } C_I \neq C_{sh} \\ 0, \text{ if } C_I = C_{sh,} \end{cases} \right. \tag{17}$$

$$UACI = \frac{1}{M \times N} \sum_{i,j}^{M,N} \frac{|C_I(i,j) - C_{sh}(i,j)|}{255} \times 100\% \tag{18}$$

As a result, the original and shared image pixels are expressed as C_I and C_{sh}. The width and height are abbreviated as M and N. Values of 99.95% and 33.4635% are considered necessary for the *NPCR* and *UACI* [26]. The *NPCR* and *UACI* values are relatively close to the optimum values, as detailed in Table 1. As the results indicate, when significantly altering the pixel locations and values, the proposed method is sensitive to changes in the original image. Further, this indicates that the suggested technique is resilient to differential attacks. The results of the analysis of four images using the proposed approach based on *NPCR*, *UACI*, and the coefficient of correlation (*CC*) are shown in Table 1.

Table 1. Results of analysis based on *NPCR*, *UACI*, and coefficient of correlation (*CC*).

Original Test Images	*UACI* (%)	*NPCR* (%)	*CC*
Jet	32.33	99.90	0.0060
Lena	32.00	99.90	0.0009
Barbara	32.30	99.90	0.0010
Sailboat	32.33	99.90	0.0040

5.2. Correlation Analysis

The correlation coefficient was tested between the shared and original images. A pair of variables' statistical links are measured by the correlation coefficient (CC). The proposed approach is evaluated based on the CC between the shares and the source image. Indicating no statistically significant correlation between the original image and the shares, the ideal *CC* value for VC is zero [36]. Equation (19) shows the *CC* mathematical formula.

$$CC = \frac{cov(A,B)}{\sqrt{var(A)}\sqrt{var(B)}}, \tag{19}$$

Shared and original images are abbreviated as A and B, respectively. Table 1 shows the *CC* values for each of the four test photos. The *CC* values are all close to zero, indicating a performance that is close to optimal.

5.3. Quality of Encryption

Encryption quality could be assessed by comparing the original and shared images' *PSNR* values (the peak signal-to-noise ratio). A lower *PSNR* value is preferred when measuring the effectiveness of encryption using *PSNR*. In the case of an infinite *PSNR*, both the shared and the source images must be the same. The *PSNR* is determined as follows:

$$PSNR = 10 \times log_{10} \frac{255^2}{MSE}, \tag{20}$$

The index of the current share and number of shares are denoted as I and n, respectively. Equation (21) shows the *MSE* formula (the mean square error).

$$MSE = \frac{1}{W \times L} \sum_{k=1}^{W} \sum_{j=1}^{L} \left(S_{j,k} - R_{k,j}\right)^2, \tag{21}$$

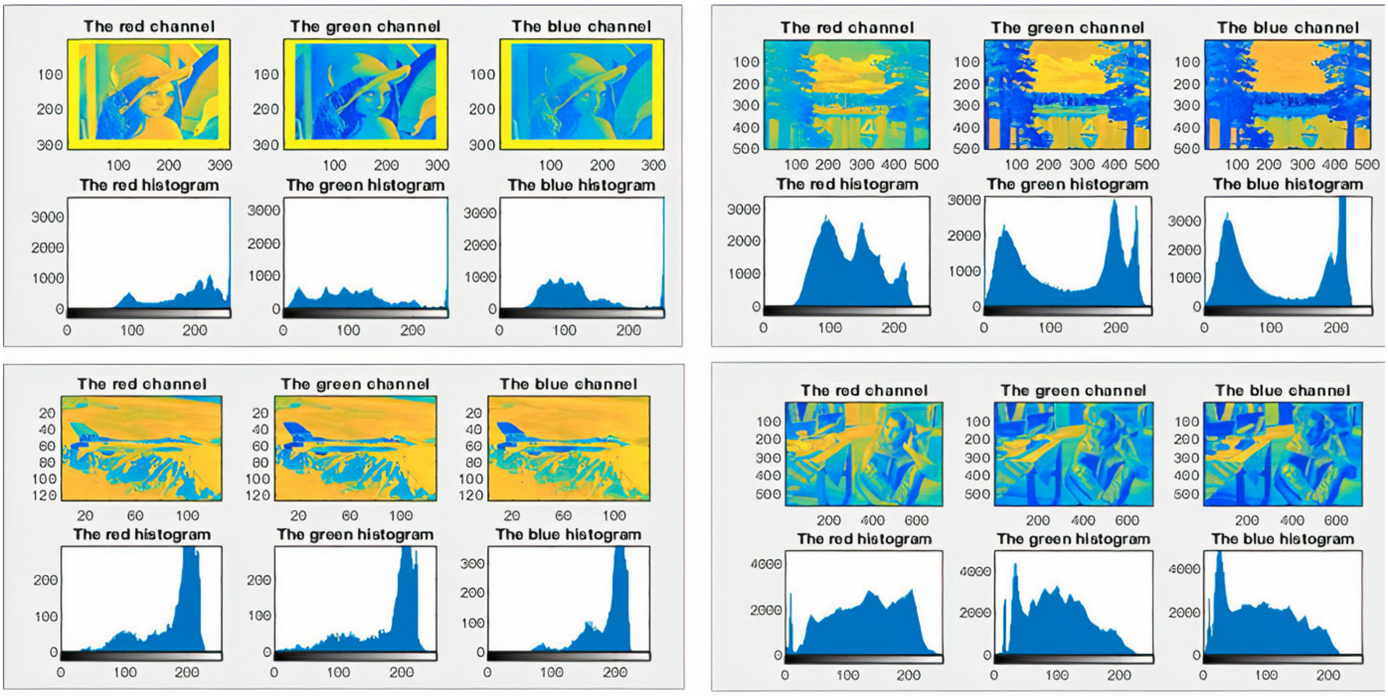
The pixels of the original image, the reconstructed pixel value, the original picture's width and length, the pixel's row and column values, and the decrypted image's pixel value are abbreviated as S, R, W, L, x, and y, respectively. For each share, the *MSE* is determined using Equation (21). Table 2 shows the results of the *PSNR* and *MSE*. Using the proposed approach, the results of the four tested images show a low *MSE* and *PSNR*, demonstrating how comparable the original and recovered images are. This indicates that the proposed approach can provide high-quality reconstructed images.

Table 2. *PSNR* and *MSE* results.

Image	*PSNR*	*MSE*
Lena	6.1811	4.2012
Jet	6.0010	4.2000
Barbara	6.2013	4.0001
Sailboat	6.0011	4.1001

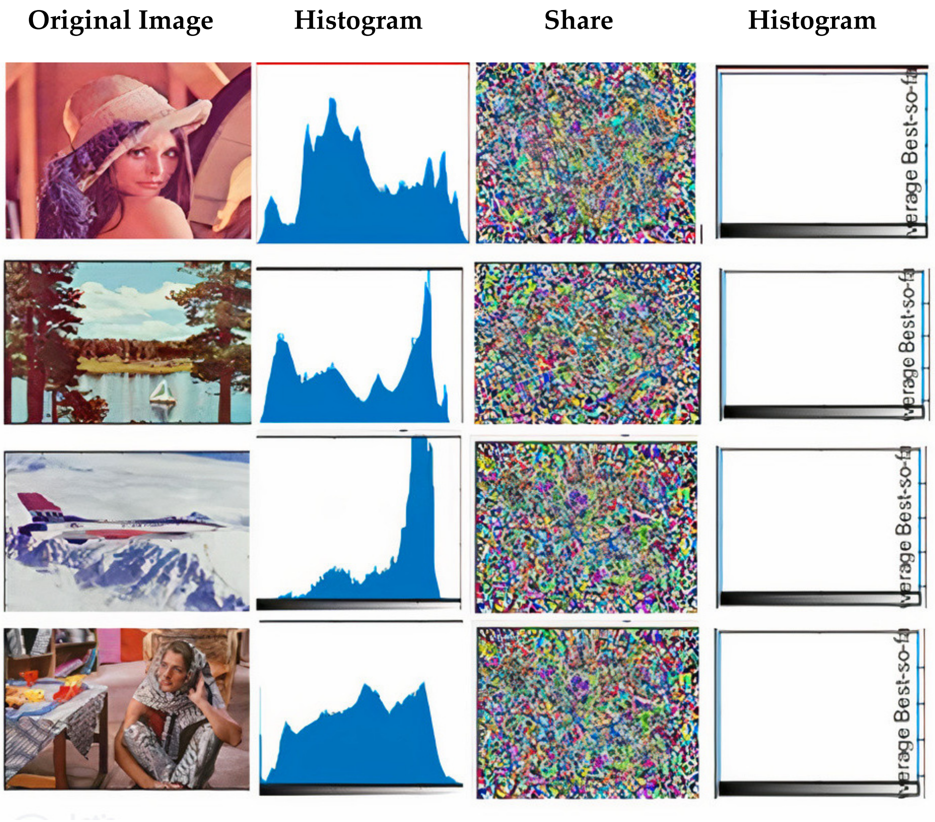
5.4. Histogram Analysis

From the histograms in Figure 6, the secret image and its corresponding shared images are examined. The shared images no longer resemble the original secret image. This ensures that the secret image is not disclosed to an enemy if they are able to access separate shares of the image. Additionally, histograms demonstrate how well-protected the proposed scheme's encryption is, producing shares that are entirely distinct from the original image. Since Share1 and Share2's histograms are comparable, only one of them is displayed in the diagram. Figure 7a shows the histograms for each original image with their color channel histograms. Figure 7b shows the histogram for each color image with a histogram for its shared image. Hackers cannot infer information about secret images from shared images since the two histograms are not matched.



(**a**)

Figure 7. *Cont.*



(**b**)

Figure 7. This figure compares the histogram of the four tested images: (**a**) Four test images and their corresponding share images analyzed by histograms; (**b**) Histogram analysis of test images and their shares.

5.5. Comparative Analysis

In this section, we contrast the suggested (2, 2) color visual cryptography approach with cutting-edge approaches. As illustrated in Table 3, the proposed (2, 2) VC system is contrasted with current techniques. Table 3 evaluates the effectiveness and quality of encryption, respectively. Moreover, the security of the various systems is compared in Table 4. Overall, both tables' results show that the suggested scheme performs on par with or better than competing schemes on several criteria. Table 3 showing the *PSNR* and CC results demonstrates that the proposed approach can extract the hidden image with little to no noise. This can be observed by lower *PSNR* and *CC* values in contrast with other systems [3,39]. In Table 4, the *NPCR* and *UACI* results of the proposed approach are compared with those of previous schemes [21,36,40]. The results are close to the ideal, showing significant resistance to differential cryptanalysis.

Table 3. Comparison based on *PSNR* and the coefficient of correlation measures between the proposed approach and state-of-the-art schemes.

Technique	Coefficient of Correlation	*PSNR* (db)
[21]	0.0011	6.1315
[36]	0.0018	7.5500
[40]	0.9643	7.1242
Proposed approach	0.0009	6.0010

Table 4. Comparison based on *NPCR* and *UACI* measures between the proposed approach and state-of-the-art schemes.

Technique	***UACI*** **(%)**	***NPCR*** **(%)**
[21]	32.66	99.68
[36]	32.58	99.60
[40]	33.73	99.60
Proposed approach	32.00	99.90

6. Conclusions

This study presents a novel two-out-of-two VC approach based on the Harris hawks optimization algorithm (HHO) for color images. Several exciting features of the proposed (2, 2) VC color scheme are demonstrated, including reliable encryption and security and lower memory requirements; additionally, it simplifies computation, rendering pixel expansion and pre-processing steps unnecessary. The proposed approach uses the well-known HHO's optimization capabilities to determine the color level, which improves the recovered image quality without slowing down the calculation or adding extra pixels. The approach was applied to a set of well-known benchmark images. According to the performed experimental study, the proposed approach demonstrated a near-ideal performance in several metrics, including *NPCR*, *UACI*, and *PSNR*, overcoming the results of current state-of-the-art approaches. Additionally, it has shown a high resilience to noise attacks.

As part of future research, the proposed approach will be improved to generate a variety of color picture formats, such as the subtractive color model, or to generate significant shares in a meaningful way. The quality of the decrypted image may be improved by using another efficient and accurate optimization algorithm at the color level determination stage.

Author Contributions: Conceptualization, D.I. and R.S.; methodology, D.I. and R.S.; software, R.S.; validation, D.I., R.S. and M.M.; formal analysis, R.S.; investigation, A.A.; resources, K.A.Z.A.; data curation, A.A.; writing—original draft preparation, D.I., A.A. and M.M.; writing—review and editing, D.I., R.S., A.A. and K.A.Z.A.; visualization, M.M.; supervision, K.A.Z.A.; project administration, K.A.Z.A.; funding acquisition, K.A.Z.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by Universiti Kebangsaan Malaysia (UKM), grant numbers GUP-2019-062 and UKM-TR-022.

Data Availability Statement: Not applicable.

Acknowledgments: The authors gratefully acknowledge the financial support for this project from Universiti Kebangsaan Malaysia (UKM), grant number GUP-2019-062 and UKM-TR-022, for supporting this work.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Alhabeeb, O.H.; Fauzi, F.; Sulaiman, R. A Review of Modern DNA-Based Steganography Approaches. *Int. J. Adv. Comput. Sci. Appl.* **2021**, *12*, 184–196. [CrossRef]
2. Ghoul, S.; Sulaiman, R. Imperceptible Image Steganography Technique Using a Novel PIT-Based Technique. In Proceedings of the 2022 International Conference on Cyber Resilience (ICCR), Dubai, United Arab Emirates, 6–7 October 2022; pp. 1–7.
3. Kamil, S.; Abdullah, S.N.H.S.; Hasan, M.K.; Bohani, F.A. Enhanced Flipping Technique to Reduce Variability in Image Steganography. *IEEE Access* **2021**, *9*, 168981–168998. [CrossRef]
4. Gutub, A. Enhancing Cryptography of Grayscale Images via Resilience Randomization Flexibility. *Int. J. Inf. Secur. Priv.* **2022**, *16*, 1–28. [CrossRef]
5. Ibrahim, D.R.; Teh, J.S.; Abdullah, R. An Overview of Visual Cryptography Techniques. *Multimed. Tools Appl.* **2021**, *80*, 31927–31952. [CrossRef]
6. Naor, M.; Shamir, A. Visual Cryptography. In *Advances in Cryptology—EUROCRYPT '94, Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques, Perugia, Italy, 9–12 May 1994*; Springer: Berlin/Heidelberg, Germany, 2006; pp. 1–12.
7. Shankar, K.; Eswaran, P. Sharing a Secret Image with Encapsulated Shares in Visual Cryptography. *Procedia Comput. Sci.* **2015**, *70*, 462–468. [CrossRef]

8. Chen, S.-K.; Ti, Y.-W. A Design of Multi-Purpose Image-Based QR Code. *Symmetry* **2021**, *13*, 2446. [CrossRef]
9. Nag, A.; Biswas, S.; Sarkar, D.; Sarka, P.P. Secret Image Sharing Scheme Based on a Boolean Operation. *Cybern. Inf. Technol.* **2014**, *14*, 98–113. [CrossRef]
10. Khanan, A.; Abdullah, S.; Mohamed, A.H.H.M.; Mehmood, A.; Ariffin, K.A.Z. Big Data Security and Privacy Concerns: A Review. In *Smart Technologies and Innovation for a Sustainable Future, Proceedings of the 1st American University in the Emirates International Research Conference, Dubai, United Arab Emirates, November 2017*; Springer: Berlin/Heidelberg, Germany, 2019; pp. 55–61.
11. Wang, L.; Yan, B.; Yang, H.-M.; Pan, J.-S. Flip Extended Visual Cryptography for Gray-Scale and Color Cover Images. *Symmetry* **2020**, *13*, 65. [CrossRef]
12. Sihwail, R.; Solaiman, O.S.; Omar, K.; Ariffin, K.A.Z.; Alswaitti, M.; Hashim, I. A Hybrid Approach for Solving Systems of Nonlinear Equations Using Harris Hawks Optimization and Newton's Method. *IEEE Access* **2021**, *9*, 95791–95807. [CrossRef]
13. Sihwail, R.; Said Solaiman, O.; Zainol Ariffin, K.A. New Robust Hybrid Jarratt-Butterfly Optimization Algorithm for Nonlinear Models. *J. King Saud Univ. Comput. Inf. Sci.* **2022**, *34*, 8207–8220. [CrossRef]
14. Purushothaman, R.; Rajagopalan, S.P.; Dhandapani, G. Hybridizing Gray Wolf Optimization (GWO) with Grasshopper Optimization Algorithm (GOA) for Text Feature Selection and Clustering. *Appl. Soft Comput. J.* **2020**, *96*, 106651. [CrossRef]
15. El-Shorbagy, M.A.; Farag, M.A.; Mousa, A.A.; El-Desoky, I.M. A Hybridization of Sine Cosine Algorithm with Steady State Genetic Algorithm for Engineering Design Problems. In *Advances in Intelligent Systems and Computing, Proceedings of The International Conference on Advanced Machine Learning Technologies and Applications (AMLTA2019), Cairo, Egypt, 28–30 March 2019*; Springer: Berlin/Heidelberg, Germany, 2020; Volume 921, pp. 143–155.
16. Cimato, S.; De Santis, A.; Ferrara, A.L.; Masucci, B. Ideal Contrast Visual Cryptography Schemes with Reversing. *Inf. Process. Lett.* **2005**, *93*, 199–206. [CrossRef]
17. Ibrahim, D.R.; Abdullah, R.; Teh, J.S.; Alsalibi, B. Authentication for ID Cards Based on Colour Visual Cryptography and Facial Recognition. In Proceedings of the 3rd International Conference on Cryptography, Security and Privacy, Kuala Lumpur, Malaysia, 19–21 January 2019; ACM: New York, NY, USA, 2019; pp. 164–167.
18. Pawlak, M.; Poniszewska-Marańda, A.; Kryvinska, N. Towards the Intelligent Agents for Blockchain E-Voting System. *Procedia Comput. Sci.* **2018**, *141*, 239–246. [CrossRef]
19. Ibjaoun, S.; Abou El Kalam, A.; Poirriez, V.; Ait Ouahman, A. Biometric Template Privacy Using Visual Cryptography. In *Innovations in Bio-Inspired Computing and Applications, Proceedings of the International Conference on Innovations in Bio-Inspired Computing and Applications, Marrakech, Morocco, 11–13 December 2017*; Springer: Berlin/Heidelberg, Germany, 2018; pp. 309–317.
20. Islam, M.A.; Riad, M.A.-A.K.; Pias, T.S. Enhancing Security of Image Steganography Using Visual Cryptography. In Proceedings of the 2021 2nd International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST), Dhaka, Bangladesh, 5–7 January 2021; pp. 694–698.
21. Mondal, U.K.; Pal, S.; Dutta, A.; Mandal, J.K. A New Approach to Enhance Security of Visual Cryptography Using Steganography (VisUS). *arXiv* **2021**, arXiv:2103.09477.
22. Fu, Z.; Cheng, Y.; Yu, B. Perfect Recovery of XOR-Based Visual Cryptography Scheme. *Multimed. Tools Appl.* **2019**, *78*, 2367–2384. [CrossRef]
23. Ibrahim, D.R.; Abdullah, R.; Teh, J. Sen An Enhanced Color Visual Cryptography Scheme Based on the Binary Dragonfly Algorithm. *Int. J. Comput. Appl.* **2022**, *44*, 623–632. [CrossRef]
24. Thaher, T.; Heidari, A.A.; Mafarja, M.; Dong, J.S.; Mirjalili, S. Binary Harris Hawks Optimizer for High-Dimensional, Low Sample Size Feature Selection. In *Evolutionary Machine Learning Techniques: Algorithms and Applications*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 251–272.
25. Mafarja, M.; Mirjalili, S. Whale Optimization Approaches for Wrapper Feature Selection. *Appl. Soft Comput. J.* **2018**, *62*, 441–453. [CrossRef]
26. Sihwail, R.; Omar, K.; Akram, K.; Ariffin, Z. Improved Harris Hawks Optimization Using Elite Opposition-Based Learning and Novel Search Mechanism for Feature Selection. *IEEE Access* **2020**, *8*, 121127–121145. [CrossRef]
27. Elgamal, Z.M.; Yasin, N.M.; Sabri, A.Q.; Sihwail, R. Improved Equilibrium Optimization Algorithm Using Elite Opposition-Based Learning and New Local Search Strategy for Feature Selection in Medical Datasets. *Computation* **2021**, *9*, 68. [CrossRef]
28. Shapi'i, A.; Pichak, S.; Baharuddin, M.S.; Iida, H. Comparative Study of 3D Reconstruction Methods from 2D Sequential Images in Sports. *Asia-Pac. J. Inf. Technol. Multimed.* **2020**, *9*, 40–57. [CrossRef]
29. Ihsan, A.; Rainarli, E. Optimization of k-Nearest Neighbour to categorize Indonesian's news articles. *Asia-Pac. J. Inf. Technol. Multimed.* **2021**, *10*, 43–51. [CrossRef]
30. Said Solaiman, O.; Sihwail, R.; Shehadeh, H.; Hashim, I.; Alieyan, K. Hybrid Newton–Sperm Swarm Optimization Algorithm for Nonlinear Systems. *Mathematics* **2023**, *11*, 1473. [CrossRef]
31. Alabool, H.M.; Alarabiat, D.; Abualigah, L.; Heidari, A.A. Harris Hawks Optimization: A Comprehensive Review of Recent Variants and Applications. *Neural Comput. Appl.* **2021**, *33*, 8939–8980. [CrossRef]
32. Hou, Y.-C. Visual Cryptography for Color Images. *Pattern Recognit.* **2003**, *36*, 1619–1629. [CrossRef]
33. Wu, X.; Yang, C.-N. Probabilistic Color Visual Cryptography Schemes for Black and White Secret Images. *J. Vis. Commun. Image Represent.* **2020**, *70*, 102793. [CrossRef]
34. Aswad, F.M.; Salman, I.; Mostafa, S.A. An Optimization of Color Halftone Visual Cryptography Scheme Based on Bat Algorithm. *J. Intell. Syst.* **2021**, *30*, 816–835. [CrossRef]

35. Karolin, M.; Meyyappan, T. Authentic Secret Share Creation Techniques Using Visual Cryptography with Public Key Encryption. *Multimed. Tools Appl.* **2021**, *80*, 32023–32040. [CrossRef]
36. Ahmad, S.; Hayat, M.F.; Qureshi, M.A.; Asef, S.; Saleem, Y. Enhanced Halftone-Based Secure and Improved Visual Cryptography Scheme for Colour/Binary Images. *Multimed. Tools Appl.* **2021**, *80*, 32071–32090. [CrossRef]
37. Heidari, A.A.; Mirjalili, S.; Faris, H.; Aljarah, I.; Mafarja, M.; Chen, H. Harris Hawks Optimization: Algorithm and Applications. *Future Gener. Comput. Syst.* **2019**, *97*, 849–872. [CrossRef]
38. Shankar, K.; Eswaran, P. A New k out of n Secret Image Sharing Scheme in Visual Cryptography. In Proceedings of the 2016 10th International Conference on Intelligent Systems and Control (ISCO), Coimbatore, India, 7–8 January 2016; pp. 1–6.
39. Wu, Y.; Noonan, J.P.; Agaian, S. NPCR and UACI Randomness Tests for Image Encryption. Cyber journals: Multidisciplinary journals in science and technology. *J. Sel. Areas Telecommun.* **2011**, *1*, 31–83.
40. Rani, N.; Sharma, S.R.; Mishra, V. Grayscale and Colored Image Encryption Model Using a Novel Fused Magic Cube. *Nonlinear Dyn.* **2022**, *108*, 1773–1796. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.