Iranian Journal of Fuzzy Systems

Volume 20, Number 6, (2023), pp. 21-47

Original paper

University of Sistan and Baluchestan

High-quality visual cryptography of real-value images without pixel expansion using fuzzy random grids

M. Mokhtari Ardakan[1], R. Ramezani[2] and A. M. Latif[3]

[1,2] *Faculty of Computer Engineering, University of Isfahan, Isfahan, Iran*
[1] *Department of Computer Engineering and Information Technology, Payame Noor University, Tehran, Iran*
[3] *Department of Computer Engineering, Yazd University, Yazd, Iran*

mostafamokhtari@eng.ui.ac.ir, r.ramezani@eng.ui.ac.ir, alatif@yazd.ac.ir

Abstract

Visual cryptography is a method used to secure images by converting them into several shares that are finally stacked to recover the original image without any calculations. Most existing techniques that can encrypt gray and color images often convert them to binary or support only limited colors, which results in reducing the quality of recovered images. Pixel expansion is another problem with existing methods. Thus, a new approach is required to encrypt gray and color images with real value, without converting them to binary or limited-color images, and also without imposing any pixel expansions. Besides, generated shares should have security, and the recovered images should be of high quality. In this research, fuzzy random grids and a meta-heuristic algorithm are used for the share generation in the encryption step. Next, the decryption step uses the fuzzy OR operator to recover high-quality images. The evaluation results demonstrate the ability of the proposed solution in encrypting gray and color images without converting them to binary, and also without pixel expansion. Besides, the results show that the proposed method is secure as individual shares do not show any information from the original image. The quality of the decrypted images has also been evaluated using subjective and objective evaluation metrics, which prove the high quality of recovered images.

Keywords: Visual cryptography, pixel expansion, fuzzy random grid, fuzzy OR, visual quality.

1 Introduction

Data encryption is a way to securely transfer information over computers and networks. In this regard, the security of images, as a visual data type, should be guaranteed through encryption. Digital image encryption based on a Visual Secret Sharing scheme (VSS) has been one of the most successful and widely used methods for securing images. The basic idea of the digital image encryption based on VSS was introduced in 1987 by Kafri and Keren as random grids [1]. Then, in 1995, Naor and Shamir introduced a new method for encrypting digital images based on a VSS called Visual Cryptography Scheme(VCS) [2]. In both methods, a binary image is encrypted by several shares so that neither provides attackers with information about the encrypted image. The main advantage of this type of cryptography is that the decryption process does not require any complex calculations, and by stacking several shares on each other, the encrypted image is reconstructed. The difference between VCS and VSS is that VCS is based on basic matrices and uses a codebook for encryption; therefore, it suffers from pixel expansion.

With the development of the visual secret sharing technology, VSS can be applied to various fields such as digital watermarking [3], information concealment [4], authentication [5], etc. For example, an algorithm has been introduced to use visual cryptographic patterns for banking applications, which aimed to verify customer requests when using electronic banking applications [6].

Although VSS techniques have the advantage of simple retrieval, they suffer from codebook design, pixel expansion, and poor visual quality. The problems needing to design codebooks and pixel expansion can be solved for binary images

Corresponding Author: R. Ramezani
Received: September 2022; Revised: May 2023; Accepted: September 2023.
https://doi.org/10.22111/IJFS.2023.43474.7640

with random grids. However, the visual quality and color of secured images are still difficulties of this method. Various approaches have been proposed to mitigate the pixel expansion problem [7, 8, 9], but could not completely eliminate this defect. Thus, for the production of non-expanded shares, two models of VCS have been developed by researchers: (1) probabilistic VCS [10, 11, 12], and (2) random grid-based VCS (RG-VCS) [13, 14, 15, 16]. These models are only available for binary images, and thus, gray and color images should be first converted to binary before encryption (for example, halftoning [17, 18, 19], and dithering [20, 21]), which results in reducing the quality of recovered images. Thus, some researchers examined different types of VCS to improve the quality of the recovered image, including VCS with complete black pixel reconstruction [22], advanced contrast methods [23], reverse performance VCS [24, 26], and XOR-based VCS [25, 27, 28]. However, such VC methods can only encrypt images with limited colors. Therefore, the existing studies suffer from either of these problems:

- Requiring a codebook.
- Leading to pixel expansion.
- Having poor quality.
- Supporting only binary images.
- Supporting gray and color images, but requires converting images to binary or limited colors, which reduces the quality of recovered images significantly.

To solve these problems, fuzzy random grids have been introduced that not only do not require any codebooks for the encryption and any calculations for the decryption but also do not suffer from pixel expansion and could encrypt gray and color images without converting them to binary. Besides, generated shares should be secure so that no information from the original image is visible from the individual shares. Also, the recovered images should have a high quality. In the proposed solution, for a gray image, two random grids with fuzzy values are generated so that they do not provide any information about the original image individually, but it can be viewed by stacking the generated random grids. The same can be done for three channels of a color image, and at the end of the encryption step, two color fuzzy random grids are generated. In this step, the colors combination relationship has been used to generate the second fuzzy random grid. This work reduces the security of the second share, which was used a meta-heuristic algorithm to maintain the security. Finally, the fuzzy OR operator is used to perform the decryption step.

The proposed solution can encrypt and decrypt real-valued gray and color images directly and without pixel expansion. Besides, the security of shares generated during the encryption phase and the quality of recovered images has been evaluated using the PSNR and SSIM metrics. These metrics indicate that the security is fully established, and the images are recovered with the highest possible quality.

The structure of the paper is as follows: after the introduction, an overview of related works is presented in Section 2. Section 3 introduces the proposed cryptography method, and the proposed solution is evaluated in Section 4 and compared with other methods in Section 5. Finally, the paper concludes in Section 6.

2 Related works

The concept of visual secret sharing can be generally investigated in two main categories: visual cryptography based on basic matrices and visual cryptography based on random grids.

Visual cryptography based on basic matrices was first proposed by Naor and Shamir [2]. In this method, encrypting binary images required a codebook, and the generated shares imposed pixel expansion. Then, much research has been done to improve this approach. For example, Yang [29] used a new approach called the probabilistic method to eliminate pixel expansion in the visual cryptography of binary images. In this method, instead of expanding each pixel below the pixels, only one pixel was used to display one pixel of the original image. As a result, this approach does not have pixel expansion but recovered images still have low visual quality. Wu and Yang then proposed a Probabilistic Color Black and White Visual Cryptography Structure threshold (k, n) (PCBW-VCS) to reduce pixel expansion in CBW-VCS [12]. However, the image to be encrypted was still binary and this method cannot encrypt gray and color images. Using basic matrices for encryption, the poor quality of recovered images, and the fact that only black and white images can be encrypted are the most important disadvantages of the above methods. To improve the quality of the recovered image, Kang et al [30] presented a new method for the visual encryption based on ghost imaging. In this method, a hidden image is divided into two visual key images, one of which is encoded as a time-varying factor and loaded into Hadamard illumination patterns. High-quality image compositing can be achieved when illumination patterns are projected into another visual key image. This method has high scalability and wide application scenarios in ghost imaging broadcast

systems and information authentication, but it can be only used for the encryption of binary images. Another way to fix the pixel expansion problem is to use random grids. In the first method, developed by Kafri and Keren [1], a binary image was encrypted by two independent random grids in such a way that none of them alone provided the attacker with information from the original image, and decryption was performed using the OR operation. This method not only imposes no pixel expansion but also eliminates the need for a codebook. However, its main drawback is its inability to encrypt gray and color images. Also, the recovered images do not have the desired visual quality. To improve the quality of this method, Kumar and Sharma used the XOR operator to reconstruct the original image in the decoding process [31]. However, this method, like the original algorithm, could only encrypt binary images. Wu and Lai [16] developed the Color Black and White Visual Cryptography Scheme (CBW-VCS) using random grids. In this method, the concept of the random grid is extended to the color pixel domain, and the XOR operator is defined for color pixels. The pixel expansion problem can be solved by this method, but it can be only used for binary images (in fact, this method only produces shares with color pixels but cannot encrypt color images).

Although many researchers have proposed methods using random grids to solve the pixel expansion problem, they can only be used for binary images [15, 32, 33, 34]. To use the advantages of random grids in encrypting other types of images, most researchers used image conversion to binary, which results in reducing the image quality. For example, Shiyu [35] introduced a method for encrypting gray and color images based on random grids. In this method, to encrypt gray images, first, the image is converted to binary by halftoning technique, and then main random grids-based algorithms are used to encrypt the obtained binary image. Zhang et al. [36] proposed a method, for color image encryption called HP-VCS, which first converts the original image to binary by halftoning method and then solves the problem of pixel expansion by block-to-block mapping. Although this method solves the problem of pixel expansion in encrypting gray and color images, converting the original image to binary before encryption reduces the quality of the recovered image while increasing computations. Although the mentioned methods can solve the pixel expansion problem with random grids-based encryption, they could only be used for black and white image encryption, and to encrypt gray and color images, they convert the original image to binary, which causes to decrease the quality of the recovered image. Pan et al [37] were also able to solve the pixel expansion in the encryption of color images. However, in their proposed method, the image is converted into binary using halftoning, which reduces the quality of the recovered image. To improve the quality of recovered images in color image encryption, Aswad et al. [19] developed a scheme that uses the hash codebook technique on halftoned channels of the color image. Although it improves the quality of the recovered image, it still has pixel expansion and also requires converting the image data to binary. To overcome this limitation, Buckley et al. [38] proposed a real-valued visual cryptography algorithm, which works directly on gray values in each color channel and generates real-value basic matrices for this purpose. However, it still has the problem of pixel expansion and reduces the quality of the decrypted image. To encrypt both black/white and gray images, a combination of VCS and PSIS (Polynomial-based Secret Image Sharing) can be used where the former is used to recover a black/white secret image while the latter is used to recover a gray secret image. The Two-in-One Secret Image Sharing (TiOSIS) scheme is an example of such an approach. In this regard, Yang and Yang [39] presented a TiOSIS-based method with a good performance in decrypting binary and gray images by ensuring the correctness of the shares and offering VCS with t-error correction capability. However, as they use basic matrices, this approach requires a codebook which increases the computation. Besides, due to the large pixel expansion, the contrast of recovered images is very low.

Reviewing existing studies shows that each of the presented approaches has aimed at solving one or more problems of visual cryptography, but the researchers could not solve all these problems simultaneously. In other words, no method has been presented so far that has solved all the aforementioned challenges in the visual cryptography problem. This means that the existing methods have not been able to perform visual cryptography directly on real values of gray and color images without converting them to binary, and without pixel expansion while respecting the quality of recovered images. Therefore, a new approach is required to visual cryptography of all types of real-valued images without the need for conversions in such a way that while solving the problem of pixel expansion and maintaining security, the quality of recovered images is excellent.

3 The proposed method

In this section, a fuzzy random grid-based algorithm for visual secret sharing is presented which can encrypt gray and color images without pixel expansion and any image conversions in such a way that the image security is established and the quality of recovered images is very high. In the proposed solution, the encryption operation is performed on the original values of the image pixels without binary conversion, and two random grids with fuzzy values are generated.

In the encrypting step, the decimal values of the first fuzzy random grid are set randomly, but the values of the

second one are set using the color relationship rules between the first fuzzy random grid and the original image. This relationship follows the rules of how colors combine when light passes through two stacked transparent colored plates. At this step, a meta-heuristic algorithm is also used to maintain the security of the generated random grids. These random grids are the same size as the original image, so the problem of pixel expansion is solved. In addition, random grids are generated in such a way that they do not display any information about the original image separately, and only when stacked on top of each other, which is implemented with the fuzzy OR operator, the original image becomes visually visible. Also, due to the proposed relationship on the color combination for the proposed encrypting and decrypting steps, the quality of recovered images is at the highest possible level. In the following, random grids are described in detail. Then, the subjects of color, light, and the properties of their combination are investigated. Finally, the encryption and decryption steps of the proposed fuzzy-based visual cryptography method are presented.

3.1 Random grids

A random grid is a two-dimensional array of pixels so that each element can be completely dark (value 1) or light (value 0). The values of the random grid (i.e., the darkness or lightness of pixels) are set randomly. Therefore, for each pixel, the probability of being dark or light is equal and also there is no correlation between the values of pixels in the array. Let R be a random grid and T(R) be the average brightness in R. Thus, according to the probability of pixels being dark or light, T(R) = 0.5 [40].

Let R_1 and R_2 be two random grids that are independent and of equal size. Thus, if they are stacked in such a way that each pixel of R_1 corresponds to one pixel of R_2, the average transparency of stacked pixels will be 1/4, which denotes the average transmission transparency of two different stacked random grids. However, if two random grids are the same, the average transmission transparency will be 1/2. These average transmissions are the same as the OR binary operator on binary numbers 0 and 1 in different states. Let $\otimes$ denote the OR operation on two random grids. Table 1 shows the results of overlapping two corresponding pixels in random grids R_1 and R_2 as $r_1 \otimes r_2$ [40].

Table 1: OR operator

$r_1 \in R_1$	$r_2 \in R_2$	$r_1 \otimes r_2$
□	□	□
□	■	■
■	□	■
■	■	■

According to Table 1, it is clear that with the OR operator, only one of the four possible states is transparent. Therefore, the average brightness of $R_1 \otimes R_2$ will be 1/4.

Let $\oplus$ be the XOR operator. Thus, $R_1 \oplus R_2$ indicates the XOR operation on two independent random grids R_1 and R_2. The results of XOR on two corresponding pixels of random grids R_1 and R_2 are shown in Table 2. As this table shows, with the XOR operation, only two out of four possible states are transparent. In other words, if two corresponding pixels are of equal value, their XOR operation will be transparent [31].

Table 2: XOR operator

$r_1 \in R_1$	$r_2 \in R_2$	$r_1 \oplus r_2$
□	□	□
□	■	■
■	□	■
■	■	□

In the proposed solution of this research, to adopt random grids for different types of gray and color images, the fuzzy type of them is presented. Thus, fuzzy random grids and the required operators are introduced in the next section.

3.1.1 Fuzzy random grids

Images can be divided into three groups: binary (black and white), gray, and color. The pixels' value of a binary image is either 0 or 1. In contrast, the pixels of gray and color images have a value from 0.0 to 1.0, depending on their color

intensity. Colors can have different depths, and for example, in 8-bit gray and color images, 0 is the lowest pixel value (equivalent to 0.0) and 255 is the highest pixel value (equivalent to 1.0).

Zadeh [41] defined fuzzy sets as the class of objects with a continuum of grades of membership. Such a set is characterized by a membership function that assigns to each object a grade of membership ranging between 0.0 and 1.0. Therefore, gray and color images can be dealt with as fuzzy sets of their pixels' color [43]. As a result, the random grids that have been used in the encryption of these images are fuzzy random grids. A fuzzy random grid is a two-dimensional array with random decimal values from 0.0 to 1.0 in which 0.0 is completely light, 1.0 is completely dark, and other values in this range determine the darkness of the gray color. Existing studies that employ conventional random grids need to use the conventional OR operator to simulate the stacking of shares in the decryption step. However, since fuzzy random grids are employed in this research, a fuzzy OR operator should be used for decrypting of shares, as will be discussed in Section 3.4.

In the seminal work of Zadeh [41], the classical fuzzy OR operator is defined as the maximum value of two fuzzy sets. For example, if the classical fuzzy OR is implemented on two matrices with values of 0.5, the result is 0.5. However, this operator is not applicable to fuzzy random grids. For example, Figure 1 shows that when two gray images S_1 and S_2 with values of 0.5 are stacked, the result is a gray image with more intensity rather than S_1 and S_2. In fact, its gray intensity value is 0.75, not 0.5. Therefore, in this study, the classical fuzzy OR is redefined, denoted by $\otimes^{fuz}$, on two fuzzy random grids S_1 and S_2 as Eq. (1) [38].

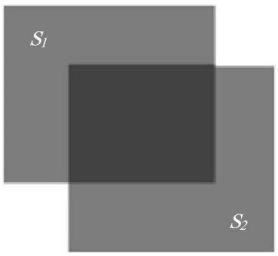


Figure 1: Stacking of two gray images with values of 0.5

$$S_1 \otimes^{fuz} S_2 = 1 - (1 - S_1)(1 - S_2). \tag{1}$$

To not lose generality, Eq. (1) can be defined for r random grids as Eq. (2).

$$\begin{aligned} &S_1 \otimes^{fuz} ... \otimes^{fuz} S_r = f(1 - (1 - S_i)(1 - S_{i+1})), i = 1, 2, ..., r - 1, \\ &f(S_j) = 1 - (1 - S_j)(1 - S_{j+1}), j = 1, 2, ..., r - 1. \end{aligned} \tag{2}$$

3.2 Color, light, and their combination properties

Color has always been of interest to humans. In many fields such as painting, printing, clothing, images, and screens, determining and changing colors are very important. This is challenging as the human eye is very sensitive to the frequency of light [42]. Light is a form of electromagnetic radiation that releases energy in small packets called photons. Different colors of light capture different amounts of energy in their photons. For example, the energy of purple-light photons is almost twice that of red-light photons. All materials absorb some of the photons' energy, but only materials that absorb visible light photons will have color [44]. So, in general, light is a flux of photons, where each photon has a specific energy (frequency). The energy of a photon corresponds to the color we see when that photon strikes the eye. The intensity of light depends on the number of photons. White light is the flux of photons of all possible visible frequencies (all colors) [45].

The behavior that different materials exhibit in the face of visible light rays is known as the optical properties of the material. The optical properties of materials include Light Reflection, Light Transmission, and Light Absorption. Light Absorption is one of the optical properties of a material that shows how much of it is absorbed relative to the light emitted to the object. It occurs for opaque materials on the surface of the material and translucent materials on the surface and inside the material or within its volume [46].

The color of an object is the color of light that is not absorbed and is reflected. For example, a green apple is seen as green because, from the light emitted to it, the green complements are absorbed by the apple, and the green light is reflected. The color of a transparent object is due to the light colors that can pass through that material. For example, white light passing through a glass of red liquid looks red because the red liquid absorbs other colors (red complements) and allows only red light to pass through. To see this, try looking at objects of different colors through

a piece of red cellophane. All colors except red disappear. This is because cellophane absorbs light in colors other than red. The absorbed color complements the color that passes through the material [44]. A soluble that looks like blue-green absorbs red light. A purple soluble absorbs green light (Table 3). A substance that selectively absorbs blue light does not look blue. Colors that are not absorbed are what we see. The observed color is said to complement the absorbed color.

Table 3: The absorbed color determines the observed color [44]

Absorbed color	Purple	Purple Blue	Blue	Green Blue	Green	Yellow Green	Yellow	Orange	Red
Observed color	Yellow Green	Yellow	Orange	Red	Purple	Purple	Purple Blue	Blue	Blue Green

Given the above, it can be said that if the white light shines on a transparent colored plate (or a colored liquid) with c color, the complements of c color are absorbed from white light and the rest are transported. This can be explained by the following relationships, according to Figure 2:

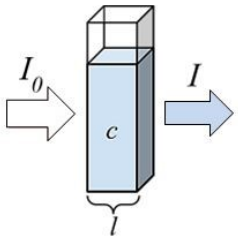


Figure 2: Absorption and transmission of light through matter

I0 = White light which is a combination of the main colors red, green, and blue in equal amounts.

c = the color of the transparent plate (or the liquid inside the container.)

I = the color of the light passing through the transparent plate.

Complement of color like c is a color that when combined with color c, their composition turns white, in other words:

Complement of c color = white – c

I = white - complement c color = white - (white - c) = c

As a result, when white light passes through a transparent screen with a c color, light with c color is seen. In this regard, if the light passes through two colored transparent plates, the color of the transmitted light will be a combination of the color of the two colored transparent plates. The way of combining the colors of several colored transparent plates and the color obtained for the final transmitted light through them is explained below.

3.2.1 Types of color models

When talking about colors outside of computers, like the colors used in printers or home painting, the three primary colors are Cyan, Magenta, and Yellow, which is indicated by triple (c, m, y). Then, other colors are secondary colors that are obtained by combining different intensities of the main colors. In this case, when the main colors are combined, the resulting color becomes darker and the combination of all three primary colors creates a black color. However, when it comes to colored lights, like the ones we see on a TV or computer screen, the three primary colors are Red, Green, and Blue, which is indicated by a triple (r, g, b). By combining these three colors and changing their intensity, any other color can be obtained. When colored lights are combined, the resulting light is brighter, and the perfect combination of the three main lights produces white light. Thus, the rules of color combination are different for painting colors and light colors. This is not too far-fetched, because when we mix the colors of a painting, the physical stimulus changes (mixing takes place outside the eye), and hence, it's a matter of physics. But in the case of the combination of lights, mixing takes place in the eye itself, and so we are dealing with a psychological phenomenon.

Mixing liquid colors and pigments are called subtractive, and mixing light is additive. The subtractive (Figure 3: left) is when the pigments are mixed or light passes through the color filters that are on top of each other; A combination of greenish blue (cyan) and yellow usually results in green, and a combination of complementary colors such as blue and yellow appears to be black. In the additive case (Figure 3: right), the lights are combined. For example, from the combination of red and green lights, the yellow color is obtained, and from the combination of red and blue lights, the purple color is obtained. In the middle, the color of the three-color overlap looks white [50].

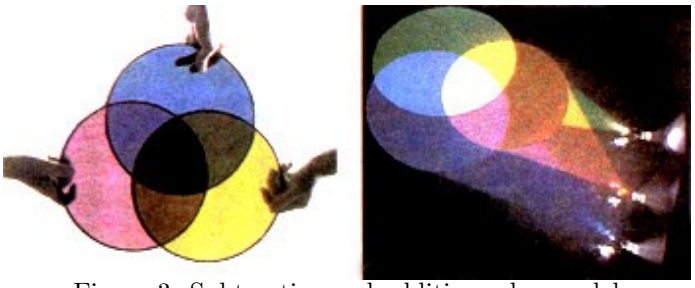


Figure 3: Subtractive and additive color model

As Figure 4 shows, subtractive and additive colors are complementary to each other, i.e. by combining two subtractive colors, an additive color is obtained, and vice versa, by combining two additive colors, a subtractive color is created. For example, with the combination of magenta and yellow, red color is created and with the combination of red and green, yellow color is produced.

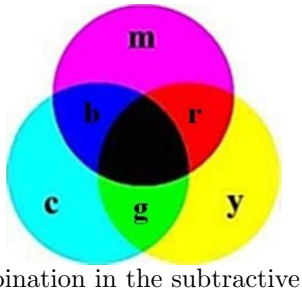


Figure 4: Color combination in the subtractive and additive model

3.2.2 Combination of colors

To get the result of combining colors in the computer, let $C_1 = (x_1, y_1, z_1)$ and $C_2 = (x_2, y_2, z_2)$ be two colors. The resulting color from the combination of these two colors can be expressed (approximately) as Eq. (3) [45]:

$$add(C1, C2) = (int(\frac{x_1 x_2}{L}), int(\frac{y_1 y_2}{L}), int(\frac{z_1 z_2}{L})), \tag{3}$$

where the 'int' function approximates its argument to the nearest integer and typically, for computers $L = 255$. In this equation, $add(C_1, C_2)$ (known as add operator) defines "color superposition". The add can naturally be applied to any number of colors. The add operation is interchangeable, so the order of stacked colors does not matter. As expected, $add(Y, M) = R$ and $add(R, G) = Y$ and $add(C, M, Y) = Black$. For example $add((63, 40, 65), (50, 92, 31)) = (31, 37, 20)$ [45].

This paper focuses on the subtractive model of color combination as color transparent pages are usually used in image visual cryptography. Thus, the "add operator" of Eq. (3), which is suitable for combining colors in the additive model, should be changed to combine colors in the subtractive model. The resulting equation [Eq. (4)] will be used to combine the colors of two color transparent pages stacked on top of each other. As mentioned before, additive and subtractive colors complement each other. In this case, to obtain Eq. (4), the complement of each parameter in Eq. (3) is obtained, and then complemented again to reach the final result.

$$\begin{aligned} &Complement(C) = 1 - C, \\ &sub_a dd(C_1, C_2) = 1 - ((1 - C_1)(1 - C_2)). \end{aligned} \tag{4}$$

In this equation, C_1 and C_2 are the colors of the two transparent pages and $sub_add(C_1, C_2)$ is the color observed from stacking these two pages. It is worth noting that this relation is the same as the fuzzy OR operator that mentioned in Section 3.1.1 which simulates the result of stacking the two shares obtained from the encryption step to recover the original images. In the following, the set of used images, the encryption and decryption steps of gray and color images, and the presented algorithms using Eq. (4) will be explained.

3.2.3 Set of images

To visually evaluate the presented algorithms in encrypting and decrypting gray and color images, the set of images in Figure 5 will be used that has been gained from SIPI [49] and KODAK [48] image databases. These images will be fed as the input of the encryption algorithm that for simplicity their size has been set as 200×200.



Figure 5: Set of gray and color images as secret images

3.3 Encryption step

The human eye can see objects and images by recognizing the color of light reflected from objects and images. In addition, when light passes through a color transparent page, colored light reaches the human eye, which leads to seeing objects with the color of that transparent page [50]. However, if the light passes through two color transparent pages, a combination of their colors is visible, which Eq. (4) models this combination. This is what happens in image visual cryptography.

On the other hand, if the color of one of the transparent pages and the final color to be seen are available, the color of the second transparent page can be obtained. To do this, Eq. (5) has been presented to calculate the color of the second transparent color page using Eq. (4). Following this idea, an encryption algorithm has been proposed in this study for the visual cryptography of gray and color images using fuzzy random grids.

$$\begin{aligned} I &= 1 - ((1 - RC_1)(1 - R_2)), \\ RC_2 &= 1 - (\frac{1 - I}{1 - RC_1}). \end{aligned} \tag{5}$$

In this equation, I is the main image, RC_1 is the color on the first transparent page, and RC_2 is the color on the second transparent page.

As mentioned in Section 2, existing studies in encrypting gray and color images that eliminate pixel expansion problem using the random grid, need to convert the input image to binary before encryption, which leads to quality loss. To solve these challenges, in this study, fuzzy random grids are generated with decimal values from 0.0 to 1.0 to encrypt gray and color images. Thus, a matrix (as a fuzzy random grid) should be created first with the same size as the original image and with random decimal values. This matrix will be the first share for the visual cryptography of a gray or color image. The main challenge in this step is the way of creating the second share so that the main image will be reconstructed by stacking two shares, while the image is not visible from none of the individual shares. The

following are the encryption and decryption steps of gray and colored images using Eq. (5) with the attributes that the images will be encrypted without pixel expansion and without converting to binary while maintaining the security feature. In addition, the original image will be retrieved with the highest possible quality in the decryption step.

3.3.1 Gray image encryption

In the proposed solution, to create fuzzy random grids from a gray image, first, the input image is displayed as a matrix with fuzzy values. Then, the first share is generated as a fuzzy random grid with the same size as the original image and with completely random decimal values between 0.0 and 1.0. Finally, the second share is created using Eq. (5). The steps of the encryption phase are shown in Algorithm 1 whose input is a gray image. In the first line of the algorithm, a fuzzy representation of the input image is obtained. This operation does not perform any conversions on the image and only scales the pixels' value of the input image in the range of 0.0 and 1.0. In the second line, a fuzzy random grid with the same size as the input image with random decimal values between 0.0 and 1.0 is generated as the first share. Then, in line three, the second share is created using Eq. (5). Finally, the outputs of this algorithm are two fuzzy random grids as separate shares.

Algorithm 1 Encryption process for gray images

1: Input: Gray secret image G (w × h)
2: Output: R_1, R_2
3: FG = FuzzyFication (G) // *Dividing the values of G pixels by 255*
4: Generate Fuzzy R_1 randomly // *R_1[i, j] = Random_pixel (0 to 1), 1 <= i <= w, 1 <= j <= h)*
5: Generate Fuzzy R_2 using R_1 and FG as follows:
6: **for** *eachpixel*$FG[i, j], 1 <= i <= w, 1 <= j <= h$ **do**
7: R_2[i, j] = 1 - (1 - FG[i,j] / 1 - R_1[i, j])
8: **end for**
9: return R_1 and R_2

The results of applying Algorithm 1 to the gray images of Figure 5 are shown in Figure 6. The results show the presence of some visual information from the original image in the second share (third column), which cast doubt on the security of the proposed method. To solve this problem, some changes must be made in the production of the first fuzzy random grid so that the security of the method is not endangered in the production of the second fuzzy random grid. To do this, a meta-heuristic algorithm has been used in this study.

Genetic algorithm (GA) is one of the most popular meta-heuristic algorithms used to optimize functions defined on a limited domain. The implementation of this algorithm usually starts with the generation of a population of chromosomes. Each chromosome is an example of the answer to the problem to be optimized, and the initial population of chromosomes is usually generated randomly. In the next step, the generated chromosomes are evaluated by a fitness function so that the chromosomes that can better represent the optimal answer of the target problem are selected to produce the next generation. Other important parameters of the genetic algorithm include the population size, the combination probability, the mutation probability, and the number of iterations, which can be adjusted when evaluating the performance of the algorithm in several test periods. In this research, the genetic algorithm has been used to improve the security of the second share. For this purpose, the first random grid is considered a chromosome whose genes are random values inside. As the second random grid is built from the first random grid, by changing the values of the first random grid in the iterations of the genetic algorithm, it is possible to generate the second random grid with high security. In these steps, the fitness of the chromosomes is the dissimilarity of the first and second random grids to the original image to satisfy the required security of the second share. To calculate the similarity of two images in the fitness function, PSNR and SSIM (These metrics are fully explained in Section 4.1.2) have been used. Therefore, the fitness function of the GA algorithm is defined as Eq. (6):

$$\begin{aligned} FitnessFunction(OI, FRG_1, FRG_2, \alpha, \beta) = \alpha.PSNR(OI, FRG_1) + \beta.SSIM(OI, FRG_1) \\ +\alpha.PSNR(OI, FRG_2) + \beta.SSIM(OI, FRG_2), \end{aligned} \tag{6}$$

where OI, FRG_1, and FRG_2 are the original image, the first fuzzy random grid, and the second fuzzy random grid, respectively. Alternatively, α and β are adjustment parameters that should be set by the end user. In the experiments, α is set as 1, and β is set as 32 by a trial-and-error process. It should be noted that the smaller the value obtained from this function, the higher the fitness of the answer.

Therefore, to solve the security problem and optimize it in production shares, several samples of the first random grid are generated and assigned to a GA. Since the goal is to increase security, the fitness function should calculate the

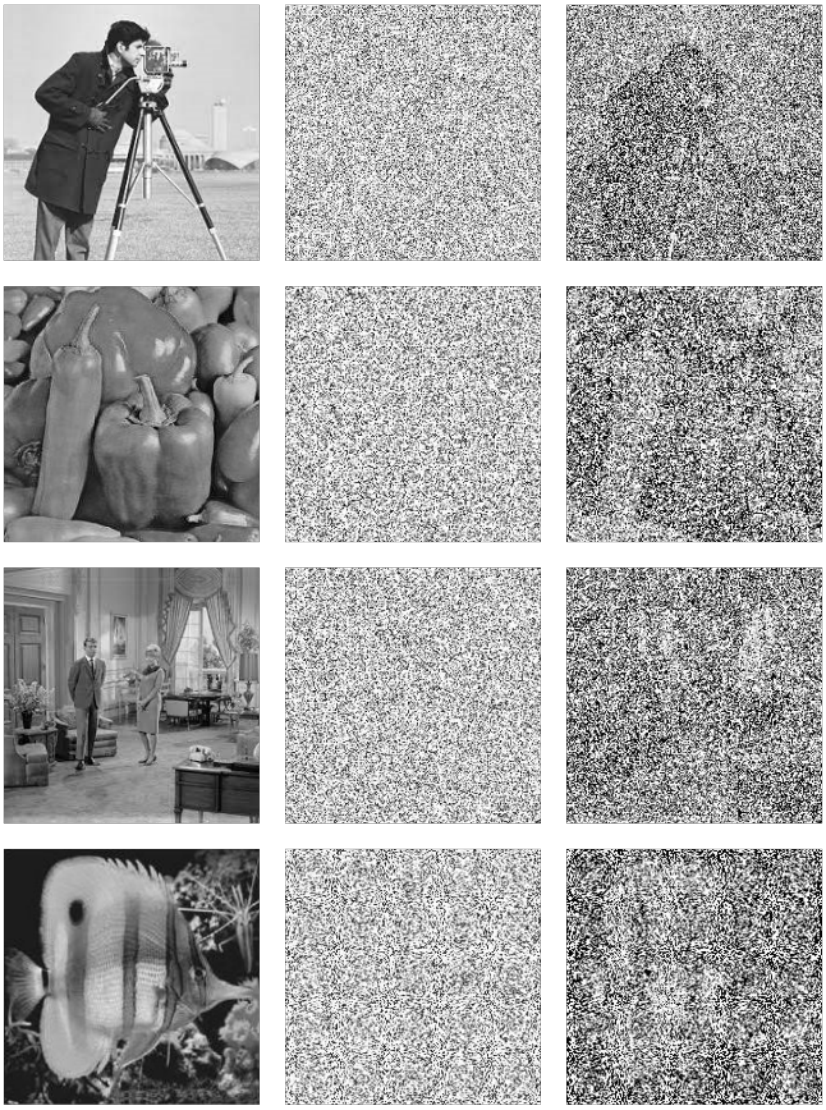


Figure 6: Results of implementation of Algorithm 1 on gray images and production of two shares

security of two random grids. Better fitness value should correspond to lower information of the original image in the first random grid as well as the second random grid, obtained from Eq. (6).

Thus, the method for encrypting a gray image would look like Algorithm 2; first, a gray image is taken as input. In the first line, the input image is presented in fuzzy form by dividing its pixel value by 255, and in the second line, the image size is obtained. Then, in the 3rd line, the fuzzified input image with its length and width, and adjustment parameters (n, k) are sent to the genetic algorithm (Algorithm 3). The output of this algorithm is two matrices equal in size to the original image and with decimal random values as fuzzy random grids (R_1 and R_2), with the feature that visual encryption security is respected in them.

The adjustment parameters in the Genetic Algorithm are n and k, where n is the number of samples of the initial answer (R_{1s} and R_{2s}) to be determined by the user and k is the number of iterations of the algorithm to achieve the final answer. In this algorithm, in the first line, n matrices with size w $\times$ h and decimal random values are generated as the first random grids (R_{1s}). In the second line, the repetition of the next steps is controlled k times. In the 3rd line, the second random grids (R_2) are generated using Eq. (5) concerning the first random grids (R_1) and the original image. Then, in lines 4 and 5, the fitness of the initial matrices (R_{1s} and R_{2s}) is calculated using Eq. (6), and the best ones are selected for the next iteration. Crossover and mutation operations will be used to modify the selected samples in the 6th line. These steps are repeated k times and finally, two matrices (R_1 and R_2) with the best fitness value (highest security) are extracted as two fuzzy random grids.

Algorithm 2 Encryption process for gray images using Genetic Algorithm

1: Input: Gray secret image G (w × h)
2: Output: R_1, R_2
3: FG = FuzzyFication (G) // Dividing the values of G pixels by 255
4: [w,h] = Size (FG)
5: [R1, R2] = GA (FG,w,h,n,k)
6: return R_1 and R_2

Algorithm 3 Genetic Algorithm (GA)

1: Input: FG and Size of FG (w, h) and n, k//n: number of RG, k: time of repeat
2: Output: R_1, R_2
3: Generate n Fuzzy R_{1s} randomly // R_1[i, j]=Random_pixel (0 to 1), 1 <= i <= w ,1 <= j <= h)
4: Repeat the following steps 3-6// k times
5: Generate n Fuzzy R2 using R1 and FG as follows:
6: **for** $eachpixelFG[i, j], 1 <= i <= w, 1 <= j <= h$ **do**
7: R_2[i,j] = 1 - FG[i,j] / 1 - R_1[i,j];
8: **end for**
9: Calculate Fitness of R_{1s}, R_{2s} // FitnessFunction(FG, R_1, R_2, α, β)
10: Select n/2 Best R_{1s}, R_{2s}
11: Change in R_{1s} // Crossover & Mutation
12: Generate n/2 Fuzzy R_{1s} randomly // R_1[i,j]=Random_pixel (0 to 1), 1 <= i <= w ,1 <= j <= h)
13: return R_1 and R_2

The results of applying Algorithm 2 to the gray images of Figure 5 are shown in Figure 7. The results show that no information from the original image is visible in the two shares generated by the proposed method. Thus, the security is fully established and the proposed method is safe.

3.3.2 Color image encryption

As mentioned before, the color images viewed on a computer screen are additive and have three main components: Red, Green, and Blue. However, when they are painted with liquid, they are of a subtractive type and have three main components: Cyan, Magenta, and Yellow. As the proposed algorithms are executed on digital images, to encrypt a color image, it is decomposed into three main components Red, Green, and Blue channels, and Algorithm2 is applied to each channel separately. However, Eqs. (4 and 5) used in this algorithm are implemented in such a way that the existing physical laws for subtractive color images are applied to the visual encrypting of a color image.

To encrypt a color image in Algorithm 4, three fuzzy matrices FC_r, FC_g, and FC_b are obtained by decomposing the original color image into three channels and dividing the pixels' value of each channel by 255 in lines 1 and 2. Then, in lines 3 to 5, six fuzzy random grids are created; for each channel, two fuzzy random grids of the same size as the original image are generated using Algorithm 2. In other words, random grids R_1^r, R_1^g, and R_1^b are generated as components of the first color share, and three random grids R_2^r, R_2^g, and R_2^b are generated as components of the second color share. Finally, the color share R_1 is produced by joining the components of the first share, and the color share R_2 is produced by joining the components of the second share, in lines 6 and 7.

The results of applying Algorithm 4 to color images of Figure 5 are shown in Figure 8. As the results show, the original image is not visible from any of the shares individually, which means that the proposed method is secure for color images likewise. In addition, the shares are the same size as the original image and have no pixel expansion.

3.4 Decryption step

As shown in Section 3.1 and Table 1, the classical OR operator can be used to simulate the share stacking task in the decrypting step of visual cryptography. However, as in this study, the values of generated shares are fuzzy in the range of 0.0 to 1.0, instead of the classical OR operator, the fuzzy OR operator, presented in Eq. (1), must be used for the decryption phase. Thus, as Algorithm 5 shows, in the proposed solution, the fuzzy OR operator is performed on the generated shares to decrypt the secured image. In this algorithm, R1 and R2 are the input shares that are generated from the encryption step (see Algorithm 2 for gray images and Algorithm 4 for color images). The fuzzy OR operator

Algorithm 4 Encryption process for color images

Input: Color secret image C
Output: R_1, R_2
Decompose C into three channels C_r, C_g, and C_b.
$[FC_r, FC_g, FC_b]$ = FuzzyFication (C_r, C_g, C_b) //Dividing the values of $[C_r, C_g, C_b]$ pixels by 255
$[R_1^r, R_2^r]$ = Algorithm 2 (FC_r) //Generating fuzzy random grids R_1^r and R_2^r
$[R_1^g, R_2^g]$ = Algorithm 2 (FC_g) //Generating fuzzy random grids R_1^g and R_2^g
$[R_1^b, R_2^b]$ = Algorithm 2 (FC_b) //Generating fuzzy random grids R_1^b and R_2^b
R_1 = Join(R_1^r, R_1^g, R_1^b //Joining three fuzzy random grids R_1^r, R_1^g, and R_1^b
R_2 = Join(R_2^r, R_2^g, R_2^b) //Joining three fuzzy random grids R_2^r, R_2^g, and R_2^b
return R_1 and R_2

Algorithm 5 Decryption Process

Input: R_1, R_2
Output: Secret image C
Apply fuzzy OR operator to all R_1 and R_2 R2 pixels
for each pixel R_1[i,j], R_2[i,j], 1 <= i <= w ,1 <= j <= h **do**
    C = 1 - [(1 - R_1)(1 - R_2)] //$R_1 \otimes^{fuz} R_2$
end for
return C

is then applied to these two shares to decrypt and recover the secret image as output. To decrypt a gray image using Algorithm 5, the proposed fuzzy OR is applied directly to the shares generated from the encryption step to obtain the recovered image. In contrast, for decrypting a color image, the fuzzy OR operator is applied to the three channels of the shares separately, and the three results are then joined to obtain the final color image.

The decryption of the generated shares for the gray and color images shown in Figures 7 and 8 is illustrated in Figures 9 and 10, respectively. As the results show, the recovered images are visible and have high quality without imposing any pixel expansions. The security of generated shares and the quality of recovered images will be assessed with objective metrics in the next section.

3.5 Parameters of the proposed algorithms

In this research, two encryption and decryption algorithms are presented followed by using a genetic algorithm to improve the security of the shares generated in the encryption step. Encryption and decryption algorithms do not have any tunable parameters. The encryption algorithm takes an image and produces two shares. Alternatively, the decryption algorithm takes two shares and recovers the original image. However, the genetic algorithm has several hyper parameters. In this research, PSNR and SSIM metrics are used in the fitness function. Due to the dissimilarity in the scale of these two metrics, two parameters α and β have been used to unify the scale of the fitness function. We set $\alpha = 1$ and $\beta = 32$ using a trial-and-error process to ensure that the fitness function works properly. Another parameter of the genetic algorithm is n, which is the size of the initial population (the number of chromosomes of the first generation), which can be determined by the user. The appropriate size of the population depends on the optimization problem under consideration. The larger the population, the easier it is to explore the search space; but more time is required for the genetic algorithm to converge. Therefore, this number should not be so small that two useful parents cannot be selected from this population. It also should not exceed a certain value because otherwise, it causes the genetic algorithm to work slowly. The last parameter is k, which sets the number of iterations of the genetic algorithm steps. The larger this parameter, the more the algorithm is iterated and as a result, it reaches a better solution, but high iterations increase the execution time. Therefore, this parameter should not be very small so that the accuracy is dropped, nor too large so that the execution time becomes very high.

4 Analysis and evaluation

Common criteria that can be used for evaluating a visual cryptography method include the ability to encrypt gray and color images without converting them to binary, pixel expansion, security, visual quality, and time complexity. As illustrated in the previous section, the proposed method meets all these parameters well by using fuzzy random grids. In

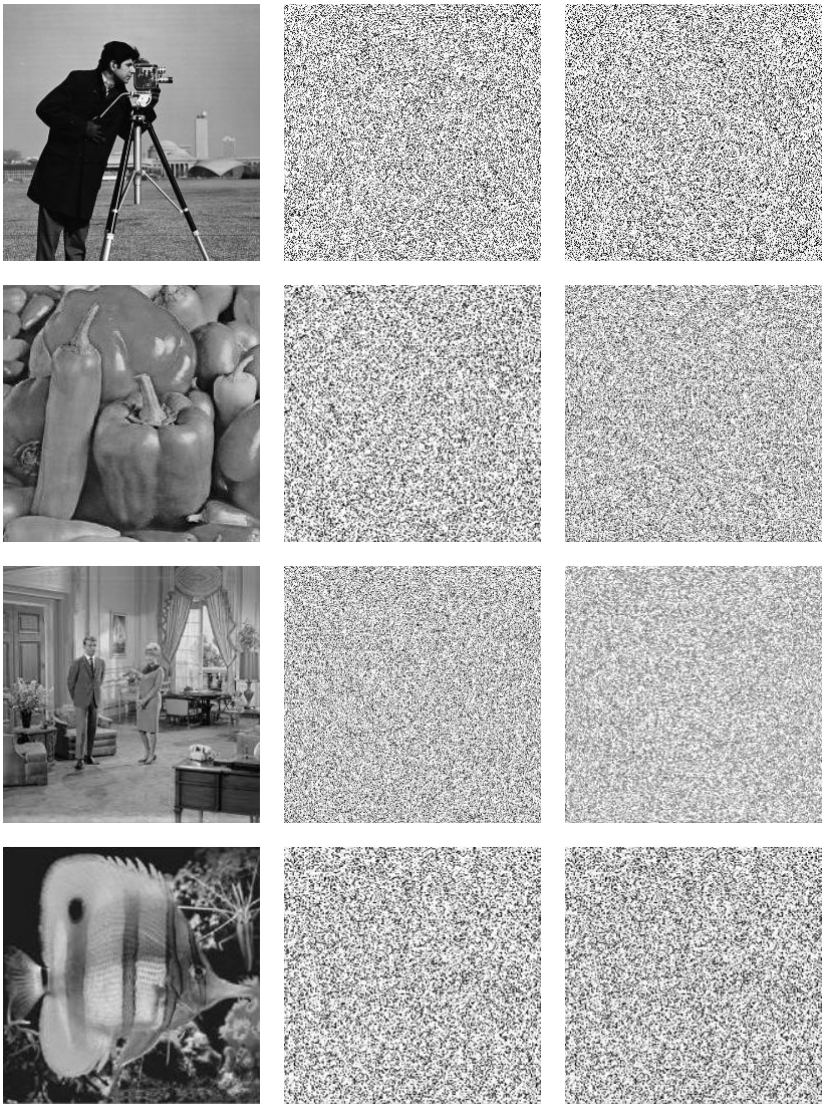


Figure 7: Results of implementation of Algorithm 2 on gray images and production of two shares

other words, it can encrypt real-value gray and color images without converting them to binary, which brings important benefits such as no significant drops in the image quality. It also completely solves the problem of pixel expansion, which results in reducing memory consumption and provides better-quality images by preventing image resizing. In addition, Figures 7 and 8 showed that the generated shares are secure, and Figures 9 and 10 showed that the recovered images are of high quality. However, due to the use of a genetic algorithm to improve the security of shares, the run time of the proposed method has been prolonged, which is fully investigated in Section 4.4.

However, to obtain robust results, it is still required to assess the security of generated shares and the quality of recovered images using more subjective and objective evaluation metrics. Thus, in the following, the security and visual quality of gray and color images are formulated and evaluated. Security means that the original image should not be recognizable from each of the random grids alone. Visual quality means the degree of similarity between the recovered image and the original image; the higher the similarity, the higher the visual quality. Also, in the following, correlation analysis and histogram analysis have been used to check security and quality.

4.1 Security and quality metrics

As the proposed solution does not impose pixel expansion, and as a result, the generated shares and the recovered image are same sizes as the original image, comparative parameters can be used to evaluate the security and quality. In this regard, the security assessment can be done by comparing the original image with the shares produced in the

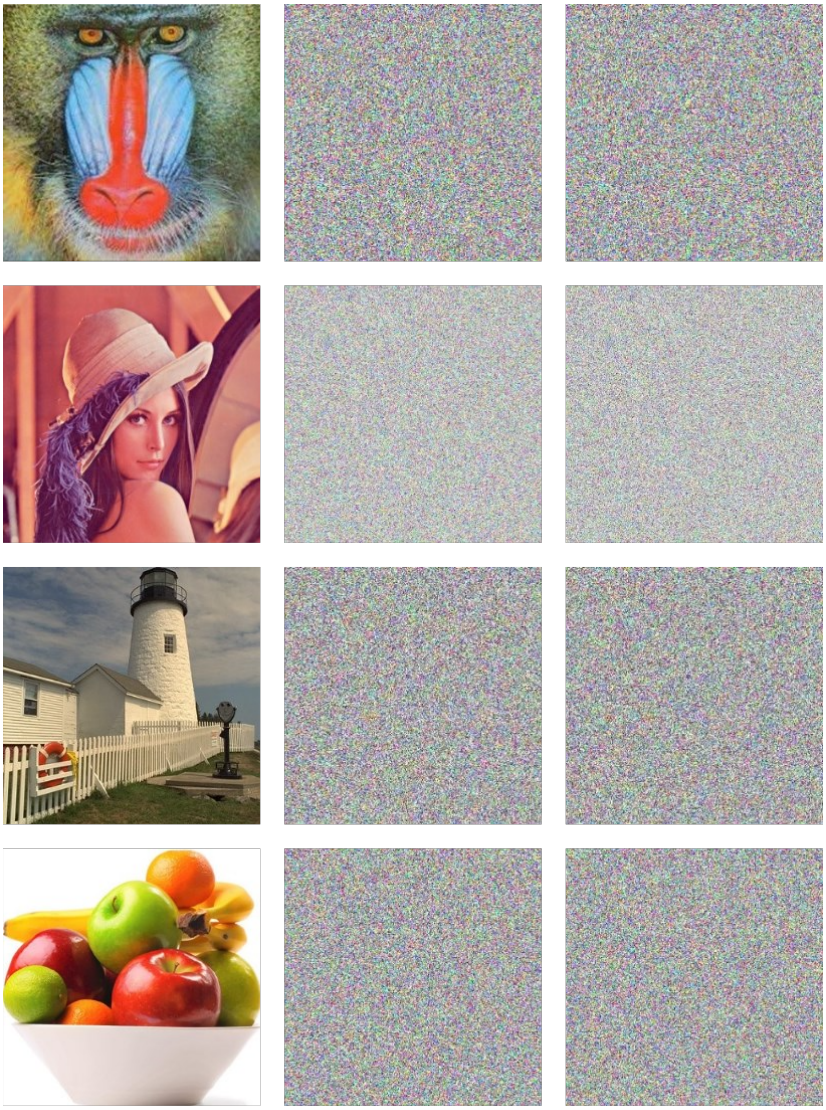


Figure 8: Results of implementation of Algorithm 4 on color images and production of two shares

encryption phase, and the quality evaluation can be done by comparing the original image with the image recovered from the decryption phase. For this purpose, Image Quality Assessment (IQA) methods have been used for evaluation purposes of both security and quality. IQA methods can be categorized into subjective and objective methods. Since human observers are the end users in most multimedia applications, subjective evaluation is the most accurate and reliable way to assess the quality of images. However, subjective evaluations are expensive and time-consuming, making them hard to apply in real-world applications. Therefore, it is necessary to design mathematical models to accurately and automatically predict the quality assessment of an average human observer, which is the goal of the objective IQA methods. Based on the availability of a reference image which is undistorted and of excellent quality, objective quality assessment methods can be classified into three categories. 1) Full-reference image quality assessment (FR-IQA), where the reference image without distortion (with excellent quality) is fully available. 2) Reference-reduced image quality assessment (RR-IQA), where the reference image is not fully available. Instead, some features are extracted from the reference image. These features are then employed by the quality assessment method as the side information for evaluating the quality of the test image. 3) No-reference image quality assessment (NR-IQA), where there is no access to the reference image and the quality evaluation is solely based on the test image [47]. In the following, the employed subjective IQA method is briefly explained. Then, due to the availability of the reference image (the main secret image in visual cryptography), an objective IQA method with full reference (FR-IQA) is elaborated on.

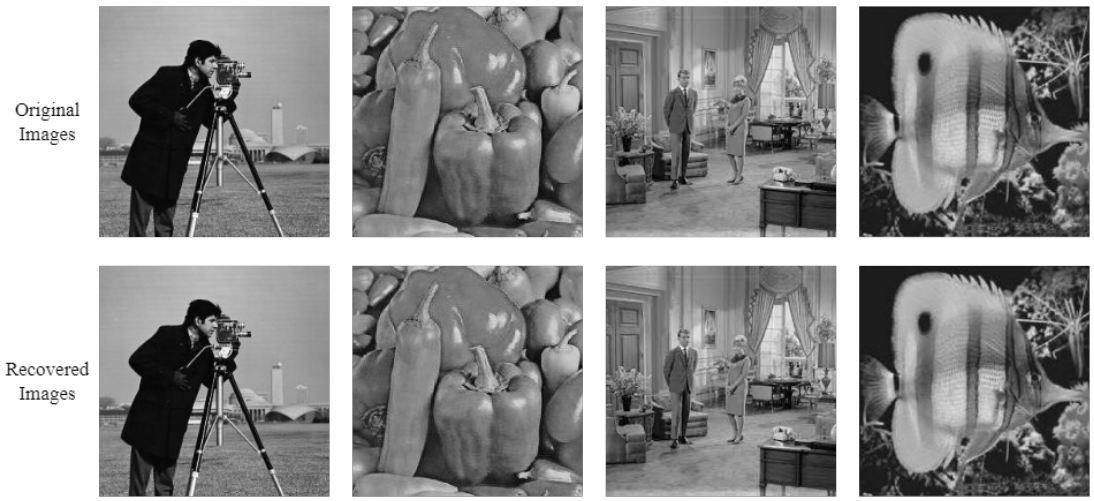


Figure 9: Results of decrypting generated shares on gray images



Figure 10: Results of decrypting generated shares on color images

4.1.1 Subjective evaluation

In the subjective evaluation, a group of people is asked to express their opinion about the quality of each image. To perform a mental image quality evaluation, several international standards, such as ITU-R BT.500-11, ITU-T P.910, ITU-R BT.814-1, and ITU-R BT.1129-2 have been proposed to obtain robust results. Some of the standardized subjective IQA methods are [51]:

1) Single stimulus categorical rating: in this method, test images are displayed on a screen for a fixed amount of time. After that, they disappear from the screen, and the observers are asked to rate the quality of images on an abstract scale, containing one of the five categories: excellent, good, fair, poor, and bad. The test images are displayed randomly.

2) Double stimulus categorical rating: this method is similar to the single stimulus method. However, in this method, both the reference and test images are displayed for a fixed amount of time. After that, both images disappear from the screen and the observers are asked to rate the quality of the test image.

3) Ordering by force-choice pair-wise comparison: in this type of subjective assessment, two images of the same scene are displayed to observers. Afterward, they are asked to choose an image with a higher quality. Observers are always required to choose one image even if both images possess no difference. There is no time limit for observers to make the decision.

4) Pair-wise similarity judgments: in this method, observers are asked not only to choose the image with higher quality but also to indicate the level of difference between them on a continuous scale. The difference scale can then be mapped to categorical scales such as: excellent, good, fair, etc.

4.1.2 Objective evaluation

There are many metrics for objective evaluations, especially for FR-IQA, five examples of which include mean square error (MSE), structural similarity index (SSIM), multi-scale structural similarity index (MS-SSIM), feature similarity index (FSIM), and peak signal-to-noise ratio (PSNR) [51]. MS-SSIM and FSIM metrics are similar to SSIM, and PSNR is more complete than MSE. Therefore, PSNR and SSIM metrics are used in this study, as they have been used by many researchers as well for objective image quality evaluation purposes [14, 19, 36, 52, 53, 54, 55].

PSNR is the most common metric to measure image quality, which in common sense, can measure the quality of a manipulated image relative to the original image. The value of PSNR is the ratio of signal to noise and is measured by decibels (dB). In fact, the higher the amount of this metric, the higher similarity between the two images being compared. In other words, high-quality images require high PSNR values, and high-secure images require low PSNR values. Eq. (7) calculates PSNR of recovered image Y w.r.t. the original image X in which MAX is the maximum value of pixels in both images [57].

$$\begin{aligned} PSNR &= 10log_{10}\frac{MAX^2}{MSE}, \\ MSE &= \frac{1}{w \times h}\sum_{i=1}^{w}\sum_{j=1}^{w}(X(i,j)-Y(i,j))^2, \end{aligned} \tag{7}$$

where the size of images is w × h.

PSNR only considers the values of the pixels and ignores the dependencies between neighboring pixels. This means that moving of pixels will not affect the PSNR, but it can be detected by the HVS. Also, PSNR does not take the location of pixels into account which is very important for quality and security assessment. Thus, in this study, in addition to PSNR, the SSIM metric has also been used for quality and security evaluation. Structural Similarity (SSIM) tries to consider the dependencies of the spatially neighboring pixels in natural images. This parameter was developed by Wang et al. [58] to assess the perception of the image quality by the human visual system. Instead of using traditional error summation methods, SSIM is designed by modeling any image distortion as a combination of three factors l, c, and s as Eq. (8).

$$SSIM(X,Y) = [l(X,Y)]^{\alpha}.[c(X,Y)]^{\beta}.[s(X,Y)]^{\gamma}, \tag{8}$$

where l is the luminance (to compare the brightness between two images), c is the contrast (to differentiate the range between the brightest and darkest areas of two images), s is the structure (to compare the local luminance pattern between two images to find the similarity and dissimilarity of the images), and α, β, and γ are positive constants.

Comparing the luminance of two images X and Y based on the brightness parameter (μ), the contrast based on the standard deviation (σ), and the structure based on the correlation coefficient can be expressed separately as Eq. (9).

$$l(X,Y) = \frac{2\mu_X\mu_Y + C_1}{\mu_X^2 + \mu_Y^2 + C_1}, c(X,Y) = \frac{2\sigma_X\sigma_Y + C_2}{\sigma_X^2 + \sigma_Y^2 + C_2}, s(X,Y) = \frac{\sigma_{XY} + C_3}{\sigma_{XY} + C_3}, \tag{9}$$

where μ_x and μ_y are local means, σ_x and σ_y are standard deviations, and σ_{xy} is the cross-covariance of images X and Y. If the value of the constants is 1 ($\alpha = \beta = \gamma = 1$), the SSIM is simplified as Eq. (10) [59].

$$SSIM(X,Y) = \frac{(2\mu_X\mu_Y + C_1)(2\sigma_X\sigma_Y + C_2)}{(\mu_X^2 + \mu_Y^2 + C_1)(\sigma_X^2 + \sigma_Y^2 + C_2)}. \tag{10}$$

It should be noted that the constant values C_1, C_2, and C_3 are used to avoid the zero denominator whose default values are $C_1 = 0.01255)^2$, $C_2 = (0.03255)^2$, and $C_3 = C_2/2$ [58]. The value of SSIM is in the range of [0, 1], where 0 means that there is no relation between images, and 1 means that the two images are completely identical.

The metrics explored so far are applicable to single-channel images, such as binary and gray images. Thus, they should be adapted for color images that have three channels. The PSNR for two color images X and Y can be calculated according to Eq. (11) [60].

$$\begin{aligned} PSNR &= 10log_{10}\frac{MAX^2}{MSE}, \\ MSE &= \frac{1}{w \times h \times o}\sum_{i=1}^{w}\sum_{j=1}^{h}\sum_{k=1}^{o}(X(i,j,k)-Y(i,j,k))^2. \end{aligned} \tag{11}$$

where w and h are the width and length of images, and o is the number of channels, which is three in this study.

Similarly, SSIM should be adapted for color images as Eq. (12) in which means locals, standard deviations, and the variance between two color images are obtained for all channels [60].

$$\begin{aligned}\mu_x &= \frac{\sum_{i=1}^{w}\sum_{j=1}^{h}\sum_{k=1}^{o} x}{m \times n \times o},\\ \sigma_x^2 &= \frac{\sum_{i=1}^{w}\sum_{j=1}^{h}\sum_{k=1}^{o}(x-\mu_x)^2}{m \times n \times o},\\ \sigma_x y &= \frac{\sum_{i=1}^{w}\sum_{j=1}^{h}\sum_{k=1}^{o}(x-\mu_x)(y-\mu_y)}{w \times h \times o}.\end{aligned} \tag{12}$$

The PSNR and SSIM metrics will be used in the next sections to evaluate the security and the quality of the proposed solution.

4.1.3 Correlation analysis

Correlation coefficient analysis is a technique used to assess the statistical correlation between the pixels in an image. Since, there is a strong correlation between the pixels of an image, attackers may attempt to infer neighboring pixel values using probability theory. However, a robust image encryption algorithm should be able to disrupt the high correlation between adjacent pixels of the image and yield a very low correlation value, approaching the value of zero, to destroy statistical attacks and achieve stronger image security. The correlation coefficients between adjacent pixels of an image can be obtained in three horizontal, vertical, and diagonal directions, given by Eq. (13). The correlation value is between -1 and +1, which shows a perfect negative and positive linear relationship, respectively. The absolute value of a correlation coefficient less than 0.09 can be considered as no correlation [61].

$$\begin{aligned}r_{\alpha\beta} &= \frac{cov(\alpha,\beta)}{\sqrt{D(\alpha)}\sqrt{D(\beta)}}, \qquad E(\alpha) = \frac{1}{N}\sum_{i=1}^{N}\alpha_i,\\ D(\alpha) &= \frac{1}{N}\sum_{i=1}^{N}(\alpha - E(\alpha))^2,\\ cov(\alpha,\beta) &= \frac{1}{N}\sum_{i=1}^{N}(\alpha_i - E(\alpha))(\beta_i - E(\beta)),\end{aligned} \tag{13}$$

where cov(α, β) is the covariance between the original and the encrypted image, D(α) is the variance of the image, and E(α) is the mean of the pixel values of the image.

4.2 Security evaluation

In visual cryptography, the security criterion is defined as do not display any information from the original image in the produced shares. Since the size of the secret image and the shares are the same, it is possible to compare the secret image with the shares to check the security criteria. The two best parameters for comparing images are PSNR and SSIM. According to the definition of PSNR and SSIM metrics, the low value of PSNR and SSIM over the original image and the produced shares indicates that the shares are completely noisy which results in high-secure shares. For this reason, these two parameters have been evaluated for the gray and color images, and their generated shares are shown in Figure 7 and Figure 8, the results of which are shown in Table 4.

Values less than 10 for PSNR and very small values close to zero for SSIM indicate high noise in the images that have been compared. Thus, it can be concluded from the results of Table 4 that the generated shares from gray and color images using the proposed method have high noise which results in providing high security.

Table 4: Assessing the security of produced shares (PSNR and SSIM between secret/share images)

	Image (1): gray (Cameraman)		Image (2): gray (Pepper)		Image (3): gray (Fish)		Image (4): color (Baboon)		Image (5): color (Fruit)		Image (6): color (Lena)	
	Share 1	Share 2	Share 1	Share 2	Share 1	Share 2	Share 1	Share 2	Share 1	Share 2	Share 1	Share 2
PSNR	8.5138	9.3381	9.0624	8.3942	8.2953	8.7341	7.0113	7.0012	7.0927	6.4407	6.9147	7.0005
SSIM	0.0104	0.0412	0.0172	0.0102	0.0152	0.0209	0.0047	0.0039	0.0196	0.0089	0.0096	0.0105

4.2.1 Correlation analysis for the security evaluation

To measure the security of the produced shares, the correlation coefficients of both the original images and the shares obtained from the encryption stage are given in Table 5 and Table 6, respectively. As Table 5 shows, the correlation coefficients of the original images are higher than 0.75, which indicates a high correlation between pixels. However, the correlation coefficients of the generated shares (Table 6) are very low (0.09, on average). This indicates that the correlation between adjacent pixels is very low, and thus the shares are almost uncorrelated. Therefore, the presented encryption algorithm can eliminate the correlation, which indicates the high security of the shares against attacks.

Table 5: Correlation coefficient of original images

	Image (1): gray (Cameraman)	Image (2): gray (Pepper)	Image (3): gray (Fish)	Image (4): color (Baboon)	Image (5): color (Fruit)	Image (6): color (Lena)
Horizontal	0.8843	0.9375	0.9347	0.8836	0.8421	0.9173
Vertical	0.8956	0.9627	0.9418	0.7931	0.7836	0.9429
Diagonal	0.7835	0.9023	0.8947	0.7658	0.8015	0.8963

Table 6: Correlation coefficient of shares

	Image (1): gray (Cameraman)		Image (2): gray (Pepper)		Image (3): gray (Fish)		Image (4): color (Baboon)		Image (5): color (Fruit)		Image (6): color (Lena)	
	Share 1	Share 2	Share 1	Share 2	Share 1	Share 2	Share 1	Share 2	Share 1	Share 2	Share 1	Share 2
Horizontal	0.0032	-0.0047	0.0031	0.0060	0	0.0009	-0.0051	0.0082	-0.0143	0.0073	0.0058	-0.0083
Vertical	-0.0153	0.0026	-0.0084	0.0039	0.0092	-0.0041	-0.0038	0.0036	0.0072	0.0038	0.0074	0.0046
Diagonal	-0.0006	-0.0007	0.0014	0.0010	0.0031	-0.0003	-0.0024	0.0009	-0.0017	-0.0004	0.0019	-0.0009

4.3 Visual quality evaluation

As mentioned before, image quality assessment (IQA) methods are categorized into subjective and objective methods. For the subjective evaluation, based on the Double Stimulus Categorical Rating standard, 20 volunteers have been selected to compare the quality of recovered images to the original ones, shown in Figures 9 and 10. To make the comparisons, visual quality parameters such as color intensity, brightness, and image contrast have been considered. By viewing each image and comparing it with the original image, each volunteer assessed the quality of the recovered image based on five scales (very bad, bad, middle, good, and excellent), whose results are in shown Table 7.

Table 7: Subjective quality evaluation of images in Figures 4 and 5

	Very Bad	Bad	Middle	Good	Excellent
Cameraman	0	0	0	4	16
Pepper	0	0	1	2	17
Couple	0	0	0	2	18
Fish	0	0	1	4	19
Baboon	0	0	1	1	18
Lena	0	0	0	0	20
Lighthouse	0	0	1	2	17
Fruit	0	0	0	3	17
Mean	0	0	0.5	1.750	18.250

The results obtained from the Mean row in Table 5 show that most of the tested people (91.2 %) have evaluated the quality of recovered images as excellent, which demonstrates the appropriateness of the proposed solution for the visual cryptography of gray and color images. However, this evaluation method is expensive and time-consuming. Thus, a mathematical method of objective evaluation is needed, for which PSNR and SSIM metrics have been used in this study. These parameters can also be used to evaluate the visual quality of an image. The larger the value obtained from comparing the decrypted image to the secret image using the PSNR, the lower the noise and therefore the greater the similarity, and if this value tends to be infinite, it indicates that the two images are completely similar. Also, the large

value obtained from SSIM in comparing two images means that the structural similarity of the two images is high, and if this value tends to 1.0, it indicates that the two images being compared are structurally quite similar. Therefore, the images obtained from the decrypting phase in Section 3.4 (Figures 9, 10) have been compared with the original images using these two parameters, the results of which are shown in Table 8.

Table 8: Assessing the visual quality of recovered images (PSNR and SSIM of secret/recover images)

	Image (1): gray (Cameraman)	Image (2): gray (Pepper)	Image (3): gray (Fish)	Image (4): color (Baboon)	Image (5): color (Fruit)	Image (6): color (Lena)
PSNR	327.2931	331.0563	325.4890	325.4007	332.1082	326.7829
SSIM	1.0	1.0	1.0	1.0	1.0	1.0

Table 8 contains a lot of interesting results. The value obtained from the PSNR is very high for all the recovered images, and these values indicate there is very little noise in the decrypted images, resulting in the highest possible quality for them. Also, the values obtained from SSIM for all tested samples are 1.0, which indicates a complete structural similarity between secret images and decrypted images. As a result, it can be concluded that the proposed method can visually encrypt a variety of gray and color images so that the decrypted image has the highest possible visual quality.

4.3.1 Histogram analysis

The histogram of an image is a graphical representation of the frequency distribution of pixels' intensity value in a digital image. Ideally, the histogram of an encrypted image should be spread evenly and bear no resemblance to the histogram of the original image [61]. Therefore, to demonstrate the security of the generated shares and the quality of the recovered images, the histogram of original images, the histogram of the shares generated by the proposed encryption algorithm, and the histogram of the recovered images are shown in Table 9.

As it is clear from Table 9, the histogram of shares of gray images is uniform and it is normal for color images. In addition, the distribution of pixel values is completely different than that of the original image, which indicates that the attack based on histogram analysis is difficult to attackers. In other words, shares do not provide any information about the original image and the proposed scheme is robust enough and has a high security against statistical attacks. Besides, the histograms of the decrypted images are very similar to those of the original images, which indicates the high quality of recovered images.

Furthermore, for the quantitative analyses of the image histograms, a metric called the variance of the histogram (var), is used to evaluate the uniformity of the pixel values of the encrypted images. The higher the uniformity of encrypted images, the lower the value of variances of the histogram. The variance of a histogram can be computed as Eq. (14):

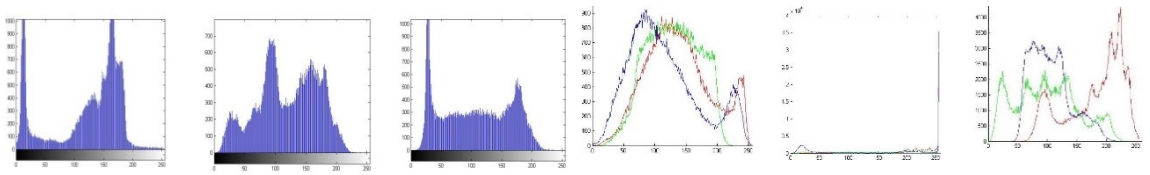
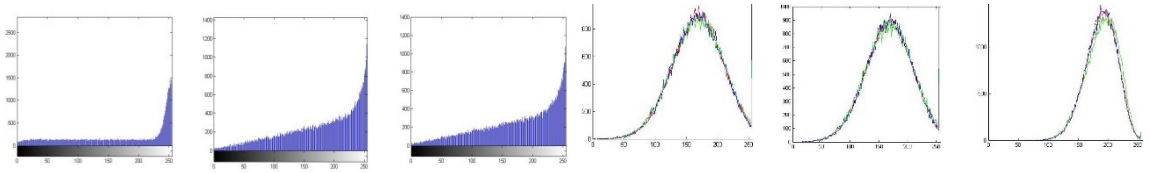
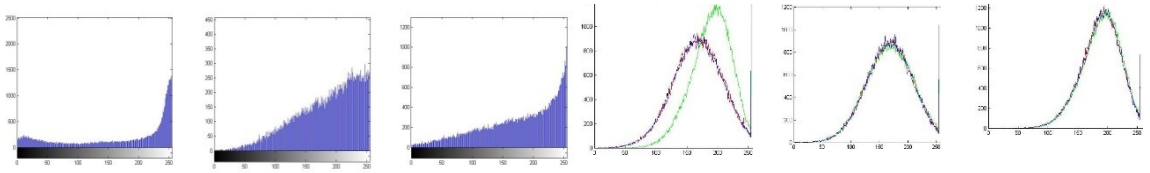
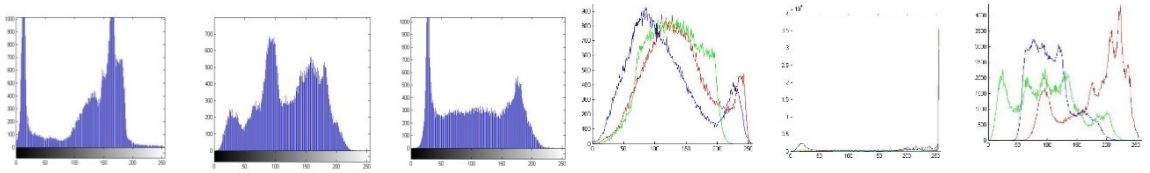
$$var(H) = \frac{1}{n}\sum_{i=1}^{N}\sum_{j=1}^{N}\frac{1}{2}(h_i - h_j)^2, \tag{14}$$

where H is a one-dimensional array of the histogram values, N is the number of possible pixel intensity values (usually 256 for 8-bit images), i and j are intensity values ranging from 0 to N-1, and h_i and h_j are the frequencies of occurrence of intensity values i and j, respectively. Table 10 shows the values of histogram variance for the experimented gray and color images and their shares. The obtained values indicate that the variance of shares is greatly reduced when compared with the variance of those images before the encryption. This large difference between the variance of the original image and its shares demonstrates the robustness of the proposed method against the attacks.

4.4 Time complexity and run-time of algorithms

Algorithm 2 is used for encrypting gray images and also for encrypting three channels of color images. The main part of this algorithm is given to a genetic algorithm (Algorithm 3). Therefore, the run time of Algorithm 2 is dominated by the time complexity of Algorithm 3. The time complexity of the genetic algorithm depends on two parameters, the first is the number of repetitions of its steps and the second is the number of generation samples that are considered in this research as k and n respectively, which will be set by the user. The remaining parts of this algorithm has a constant order. Therefore, the time complexity of this Algorithm 3 has the order of O(k $\times$ n), which is relatively time-consuming. However, since in this field, the security and quality of the encryption/decryption process are much more important

Table 9: Histogram of gray and color images and their shares and recovered images

	Image (1): gray (Cameraman)	Image (2): gray (Pepper)	Image (3): gray (Fish)	Image (4): color (Baboon)	Image (5): color (Fruit)	Image (6): color (Lena)
Original Image						
Share 1						
Share 2						
Recovered Image						

than its run time, such an increased computation time is negligible w.r.t. overcoming different challenges such as the use of code books, pixel expansion, conversion of gray and color images into binary, and reduction of image quality.

4.5 Robust analysis against differential and noise attacks

The differential attack is a special type of selected plaintext attacks that analyzes the effects of a slight change in the original image on the encrypted image. An encryption algorithm is resistant to this attack if the method is very sensitive to changes. This means that a small change in the original image should have a global effect on the encrypted image. In addition, to prevent tampering with the encrypted image, a suitable anti-attack should be provided. Therefore, to check the robustness of an encryption method against a noise attack, noise is added to the encrypted image and then decryption is performed. An encryption algorithm is resistant to this attack if the original image can still be recovered after applying noise to the encrypted image.

To examine the resistance of the proposed method against differential attacks, first, the median filter is applied to the original image before encryption. Next, the changes in the attacked encrypted image is compared to the original encrypted image. For this purpose, two coefficients of NPCR (Number of Pixel Change Rate) and UACI (Unified Average Changing Intensity) are used, which are calculated as Eq. (15).

$$D(i,j) = \begin{cases} 1 & X(i,j) \neq Y(i,j) \\ 0 & X(i,j) = Y(i,j) \end{cases} \qquad NPCR = \frac{\sum_{i=1}^{w}\sum_{j=1}^{h} D(i,j)}{w \times h} \times 100.$$
$$UACI = \frac{1}{w \times h}\left(\sum_{i=1}^{w}\sum_{j=1}^{h} \frac{|X(i,j) - Y(i,j)|}{255}\right) \times 100. \tag{15}$$

where X and Y are pixels of the original image and the modified image, respectively, whose size is w × h. NPCR

Table 10: Variance of the histogram for gray and color images and their shares

	Image (1): gray (Cameraman)	Image (2): gray (Pepper)	Image (3): gray (Fish)		Image (4): color (Baboon)	Image (5): color (Fruit)	Image (6): color (Lena)
Original Image	99168.835	187124.526	100553.724	**R**	69320.234	111309.273	70845.519
				G	494614.518	352386.197	350824.091
				B	1021324.832	457505.935	1382757.324
Share 1	9607.438	25328.150	39091.309	**R**	10250.437	9686.957	10305.618
				G	99895.237	96327.136	102878.316
				B	123302.092	112239.384	129621.112
Share 2	9524.523	22796.916	28658.735	**R**	10220.438	9722.001	10376.263
				G	100326.281	95809.932	102075.183
				B	163262.451	162215.178	164318.292

value close to 100% and UACI value close to 33.5% represent the greater sensitivity of the method to obvious image changes [62]. In other words, with the high sensitivity of an encryption method to changes in the original image, that method is resistant to differential attack. The NPCR and UACI values between the first share of the original encrypted image and the attacked one are tabulated in Table 11. As the results show, the proposed method is very sensitive to the change in the original image; and thus, it is resistant to this type of attack.

Table 11: Comparison of the original share1 and the attacked share1 by NPCR and UACI

	Image (1): gray (Cameraman)	Image (2): gray (Pepper)	Image (3): gray (Fish)	Image (4): color (Baboon)	Image (5): color (Fruit)	Image (6): color (Lena)
NPCR	97.237	97.625	96.935	97.104	95.458	97.356
UACI	31.895	32.037	31.937	32.183	30.993	32.261

Next, to examine noise attacks, a salt and pepper noise attack is used to evaluate the robustness of the proposed method against these attacks. For this purpose, after encrypting the image and generating two shares, salt and pepper noise has been added to one of the shares. Then, the image is decrypted using the shares whose results are shown in Figure 11. The results show that the recovered images are completely recognizable and have an acceptable quality. Therefore, it can be concluded that the proposed method is resistant to noise attack; and thus, it is robust.

5 Comparison with other studies

To show the advantages and features of the proposed method, it is compared with several state-of-the-art studies [1, 9, 16, 15, 19, 35, 36, 38, 39]. Features considered in this comparison include the type of secret image, the need to convert the image to binary, requiring a codebook, the pixel expansion, the quality of recovered images, and finally time complexity. First, brief explanations of these criteria are given. Next, they are summarized in Table 12.

1- Types of images: Generally, there are three types of images, black and white, gray, and color, where nowadays, the first type is used much less than the two others. However, due to the larger data contained in gray and color images, they are more difficult to process. Thus, efficient cryptography methods are required to encrypt them. Among the competitive works [1, 9, 16, 15] can be applied only to black and white images, and cannot encrypt gray and color images. However, the proposed method of this study can encrypt all types of images.

2- The need to convert to binary: Most of the visual encryption methods that have been presented so far for gray and color images first convert the image to binary, which significantly reduces the image quality. As a result, it is very important if a method can encrypt gray and color images with real values. For example, [35, 36] encrypts gray and color images, but due to the conversion to binary, the recovered image has a low quality, or the generated shares have pixel expansion [19]. Our proposed method and the method presented in [38] both can encrypt gray and color

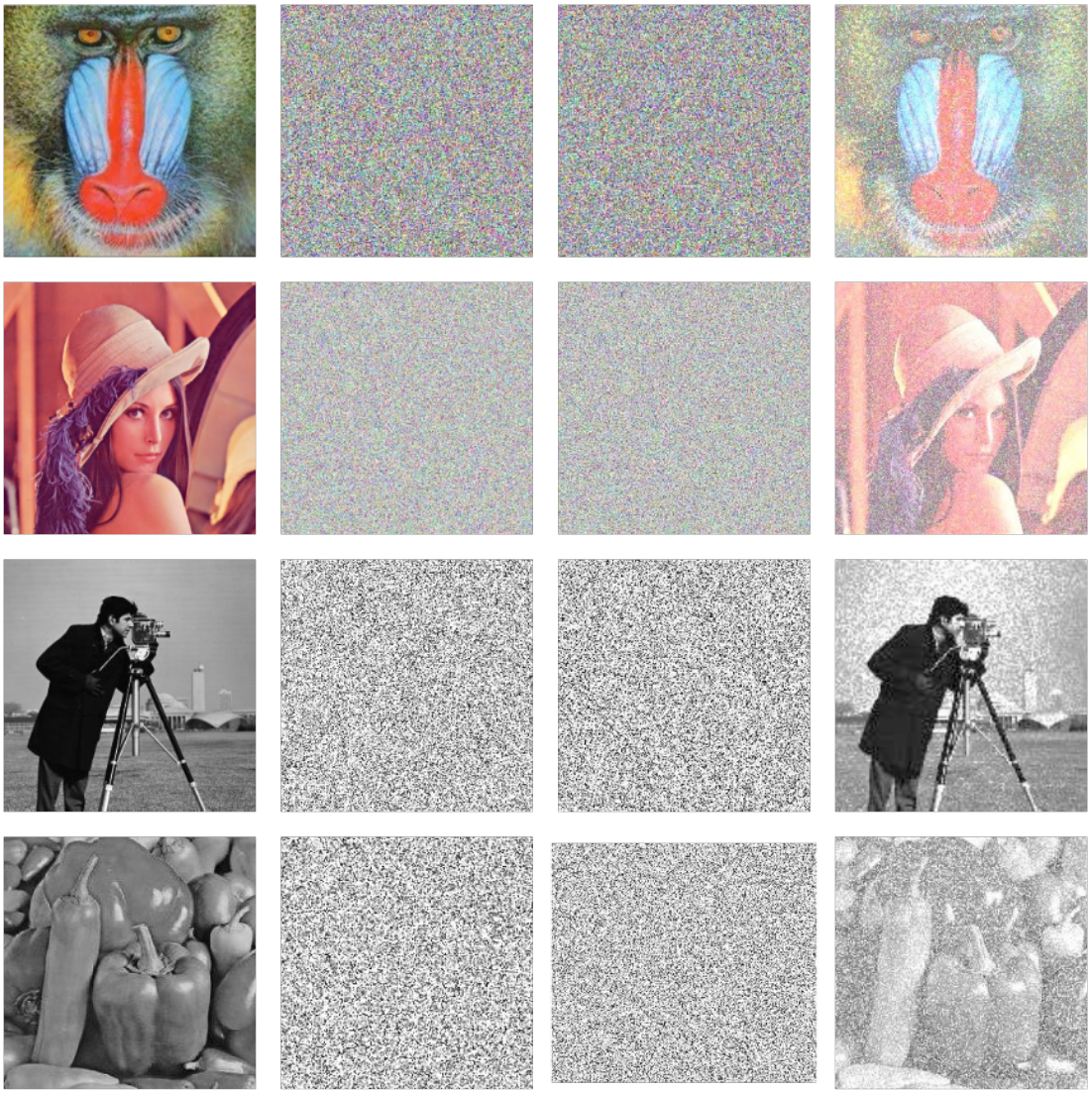


Figure 11: Robustness analysis of salt and pepper noise attacks

images with real values and without converting them to binary. However [38] has a codebook, pixel expansion, and low quality.

3- Codebook design: If a cryptography method uses basic matrices in the image encrypting step, the design has a codebook that causes the problem of pixel expansion. Methods such as [9, 19, 38, 39] still have a codebook that causes pixel expansion and low quality in the recovered image. However, the proposed method has no codebook and therefore does not suffer from pixel expansion.

4- Pixel expansion: This criterion is one of the main drawbacks of many existing studies. While numerous methods have addressed this problem, most of them are either only applicable to binary images [1, 16, 15] or, if can deal with color images, the quality of their recovered image is low [36]. In contrast, the proposed solution, due to using fuzzy random grids for image encryption, has eliminated the pixel expansion problem, and also it can encrypt gray and color images without reducing the quality.

5- Visual quality of recovered images: As explained above, the methods provided for the cryptography of gray and color images, as well as the elimination of pixel expansion, usually reduce the visual quality of the recovered image. In addition, to obtain high quality, other criteria should not be undermined. For example, while the quality of recovered images in method [19] is good, it uses a binary conversion, has a code book, and still has pixel expansion. Similarly, the method presented in [16], which has a good quality in recovered images, is only suitable for black and white images. However, due to using the fuzzy OR operator, the quality of the images recovered by the proposed method is very high, which outperforms existing methods.

6- Time complexity algorithm: To compare the time complexity of different visual cryptography algorithms, it is assumed the size of the input image is $w \times h$. The computation order of the competitive algorithms is given in Table 12. As explained before, the time complexity of the proposed algorithm depends on two parameters of the genetic algorithm, (i.e., k and n). Thus, the total computation order of the proposed algorithm is $O(w \times h \times k \times n)$ which is relatively longer compared to other algorithms.

Table 12: Comparisons of our proposed method with existing studies (A=the minimal qualified set Γ_0 [15], m=pixel expansion, i is SA iteration [38])

	Images type			Preventing image conversion	No code-book	No pixel expansion	Recovered images quality	Time complexity
	B&W	GS	RGB					
Kafri and Keren [1]	✓	✗	✗	NA	✓	✓	low	$O(w \times h)$
Shyu and Chen [9]	✓	✗	✗	NA	✗	Reduce	low	$O(w \times h \times m)$
Wu and Lai [16]	✓	✗	✗	NA	✓	✓	good	$O(w \times h)$
Liu et al [15]	✓	✗	✗	NA	✓	✓	low	$O(w \times h \times \lvert A \rvert)$
Yang and Yang [39]	✓	✓	✗	✓	✗	✗	low	$O(w \times h \times m)$
Zhang et al [36]	✗	✓	✓	✗	✓	✓	low	$O(w \times h)$
Aswad et al [19]	✗	✓	✓	✗	✗	✗	good	$O(w \times h \times m)$
Shyu [35]	✗	✓	✓	✗	✓	✓	low	$O(w \times h)$
Buckley et al [38]	✓	✓	✓	✓	✗	✗	low	$O(w \times h \times m \times i)$
Proposed Method	✓	✓	✓	✓	✓	✓	excellent	$O(w \times h \times k \times n)$

As the results show, there was no way so far to encrypt gray and color images that have all the required criteria at the same time and also provide decrypted images with high visual quality while establishing security. The proposed method provides all these features simultaneously and has the highest possible visual quality for the recovered images. In contrast to these advantages, the proposed method suffers from the long run time, which is due to the use of the genetic algorithm.

In addition, to more accurately compare the quality of images recovered by the proposed method with existing studies using PSNR and SSIM metrics, a number of them that do not have pixel expansion have been selected. For example, the quality of images recovered by methods [9, 19, 38, 39] is not comparable using PSNR and SSIM as they have pixel expansion. Similarly, some other works, such as [1, 16, 15], cannot be compared as they are only for encrypting black and white images. Thus, we have encrypted and then decrypted some gray and color images (for example, Couple, Fish, Lena, and Fruit in Figure 5) using our proposed method, and also using the methods of Shyu [33] and Zhang et al [34], whose results are shown in Table 13. As the results show, the PSNR of the images recovered by the proposed method is very high and the SSIM of them is 1.0 that indicates the visual quality obtained by our proposed solution is much higher than that of other methods. These results demonstrate the usefulness of the proposed algorithms in the cryptography of gray and color images using fuzzy random grids and the fuzzy OR operator.

According to the objective and subjective evaluations, as well as the correlation and histogram statistical analysis, our proposed method not only does not impose any pixel expansions but also features security and quality at the highest possible level. However, it suffers from an increased computation run time.

6 Conclusion

Many encryption methods have been proposed by researchers to ensure the security of images, but visual cryptography is of particular importance as it can recover the original image only by stacking the generated shares. Several methods have been provided for the visual encryption of black and white images. However, there is no method applicable to gray color images that can perform encryption without converting the original image to binary and without pixel expansion so that the recovered image has good quality. For this purpose, a method has been presented in this study to encrypt gray and color images without converting them to binary and without pixel expansion using fuzzy random grids. The most important feature of the proposed method is the use of color combination rules in the image encrypting stage.

Table 13: Comparing the visual quality of our proposed solution and existing studies (NM: Not Measurable, OBW: Applicable Only for B&W images)

	Visual quality of the gray image (Couple)		Visual quality of the gray image (Fish)		Visual quality of the color image (Lena)		Visual quality of the color image (Fruit)	
	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM
Buckley et al [38]	NM	NM	NM	NM	NM	NM	NM	NM
Shyu [9]	NM	NM	NM	NM	NM	NM	NM	NM
Aswad et al [19]	NM	NM	NM	NM	NM	NM	NM	NM
Yang and Yang [39]	NM	NM	NM	NM	NM	NM	NM	NM
Kafri and Keren [1]	OBW	OBW	OBW	OBW	OBW	OBW	OBW	OBW
Wu and Lai [16]	OBW	OBW	OBW	OBW	OBW	OBW	OBW	OBW
Liu et al [15]	OBW	OBW	OBW	OBW	OBW	OBW	OBW	OBW
Shyu [35]	17.1609	0.5473	15.9067	0.4408	17.9305	0.4971	18.3206	0.5008
Zhang et al [36]	23.0615	0.6025	21.6291	0.5934	21.9481	0.6136	24.1037	0.6752
Proposed Method	324.4192	1.0	325.4890	1.0	326.7829	1.0	332.1082	1.0

Besides, by using a fuzzy OR operator in the decrypting step, the recovered images have excellent quality. To evaluate the performance of the proposed solution, subjective and objective evaluation methods (PSNR and SSIM metrics) have been used, which in both methods, high-quality images were displayed after decrypting while respecting the image security. Correlation and histogram analyses also showed the security and quality of the proposed method. Also, the robustness of the method against differential and noise attacks was checked, which proved that this method is also robust against attacks. As mentioned before, due to using the genetic algorithm, the run time of the proposed method is long, and in the next research, it is expected that by providing the main features of visual cryptography, new algorithms are presented that have an appropriate run time.

Acknowledgement

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

References

[1] F. M. Aswad, I. Salman, S. A. Mostafa, *An optimization of color halftone visual cryptography scheme based on Bat algorithm*, Journal of Intelligent Systems, **30**(1) (2021), 816-835.

[2] H. Ayad, M. Khalil, *Qam-dwt-svd based watermarking scheme for medical images*, International Journal of Interactive Multimedia and Artificial Intelligence, (2018), 81-89.

[3] C. S. Baird, *Absorption of electromagnetic radiation*, AccessScience, 2019.

[4] J. Blesswin, M. Kumar, *Secured communication method using visual secret sharing scheme for color images*, Journal of Internet Technology, **22**(4) (2021), 803-810.

[5] C. Blundo, S. Cimato, A. De Santis, *Visual cryptography schemes with optimal pixel expansion*, Theoretical Computer Science, **369**(1-3) (2006), 169-182.

[6] N. Buckley, A. K. Nagar, S. Arumugam, *On real-valued visual cryptographic basis matrices*, Journal of Universal Computer Science, **21**(12) (2015), 1536-1562.

[7] B. Champagne, M. Guillaume, F. Zutterman, *TDDFT investigation of the optical properties of cyanine dyes*, Chemical Physics Letters, **425**(1-3) (2006), 105-109.

[8] J. Chandrasekaran, *Chemistry of colours*, Resonance, **6**(3) (2001), 66-75.

[9] J. J. Chang, B. Y. Huang, J. S. Juan, *A new visual multi-secrets sharing scheme by random grids*, Cryptography, **2**(3) (2018), 24.

[10] H. C. Chao, T. Y. Fan, *Random-grid based progressive visual secret sharing scheme with adaptive priority*, Digital Signal Processing, **68** (2017), 69-80.

[11] H. C. Chao, T. Y. Fan, *XOR-based progressive visual secret sharing using generalized random grids*, Displays, **49** (2017), 6-15.

[12] H. C. Chao, T. Y. Fan, *Generating random grid-based visual secret sharing with multi-level encoding*, Signal Processing: Image Communication, **57** (2017), 60-67.

[13] T. H. Chen, Y. S. Lee, C. H. Lin, *On the difficulty of aligning VSS random grids*, Signal Processing: Image Communication, **44** (2016), 101-107.

[14] P. L. Chiu, K. H. Lee, *Efficient constructions for progressive visual cryptography with meaningful shares*, Signal Processing, **165** (2019), 233-249.

[15] S. Cimato, R. De Prisco, A. De Santis, *Probabilistic visual cryptography schemes*, The Computer Journal, **49**(1) (2006), 97-107.

[16] S. Cimato, R. De Prisco, A. De Santis, *Colored visual cryptography without color darkening*, Theoretical Computer Science, **374**(1-3) (2007), 261-276.

[17] M. A. Duraisamy, M. M. Sathiyamoorthy, M. S. Chandrasekar, *Protection of privacy in visual cryptography scheme using error diffusion technique*, International Journal of Computer Science and Network, **2**(2) (2013).

[18] P. A. Eisen, D. R. Stinson, *Threshold visual cryptography schemes with specified whiteness levels of reconstructed pixels*, Designs, Codes and Cryptography, **25**(1) (2002), 15-61.

[19] R. Franzen, *Kodak lossless true color image suite*, http : / / r0k . us / graphics / kodak. (accessed:08.30.2023).

[20] A. Giri, *Development of digital half toning techniques for Grayscale image*, PhD thesis, 2014.

[21] M. Gupta, et al., *An efficient image encryption technique based on two-level security for internet of things*, Multimedia Tools and Applications, **82**(4) (2023), 5091-5111.

[22] C. Hegde, et al., *Secure authentication using image processing and visual cryptography for banking applications*, 2008 16th International Conference on Advanced Computing and Communications, (2008), 65-72.

[23] A. Hore, D. Ziou, *Image quality metrics: PSNR vs. SSIM*, 2010 20th International Conference on Pattern Recognition, (2010), 2366-2369.

[24] Y. C. Hou, *Visual cryptography for color images*, Pattern Recognition, **36**(7) (2003), 1619-1629.

[25] H. Hu, et al., *General construction for XOR-based visual cryptography and its extended capability*, Multimedia Tools and Applications, **75** (2016), 13883-13911.

[26] B. Hu, et al., *Subjective and objective quality assessment for image restoration: A critical survey*, Signal Processing: Image Communication, **85** (2020), 115839.

[27] O. Kafri, E. Keren, *Encryption of pictures and shapes by random grids*, Optics Letters, **12**(6) (1987), 377-379.

[28] Y. Kang, et al., *Visual cryptography based on ghost imaging and Hadamard transform*, Quantum Information Processing, **22**(2) (2023), 116.

[29] S. Kumar, R. Sharma, *Improving contrast in random grids based visual secret sharing*, International Journal of Security and Its Applications, **6**(1) (2012), 9-28.

[30] P. Li, et al., *A construction method of (2, 3) visual cryptography scheme*, IEEE Access, **8** (2020), 32840-32849.

[31] C. C. Lin, W. H. Tsai, *Visual cryptography for gray-level images by dithering techniques*, Pattern Recognition Letters, **24**(1-3) (2003), 349-358.

[32] Z. Liu, et al., *Weighted visual secret sharing for general access structures based on random grids*, Signal Processing: Image Communication, **92** (2021), 116129.

[33] N. A. E. S. Mohamed, A. Youssif, H. A. G. El-Sayed, *Fast and robust image encryption scheme based on quantum logistic map and hyperchaotic system*, Complexity, **2022** (2022). DOI: 10.1155/2022/3676265.

[34] P. Mohammadi, A. Ebrahimi Moghadam, S. Shirani, *Subjective and objective quality assessment of image: A survey*, arXiv preprint arXiv:1406.7799, (2014).

[35] M. Naor, A. Shamir, *Visual cryptography*, Advances in Cryptology–EUROCRYPT'94: Workshop on the Theory and Application of Cryptographic Techniques Perugia, Italy, May 9–12, 1994 Proceedings 13. Springer, (1995), 1-12.

[36] J. S. Pan, et al., *Visual cryptography scheme for secret color images with color QR codes*, Journal of Visual Communication and Image Representation, **82** (2022), 103405.

[37] C. S. Sanaboina, S. R. Odugu, G. Vanamadi, *Secret image sharing using visual cryptography shares with acknowledgment*, International Journal of Innovative Technology and Exploring Engineering, **8**(11) (2019), 3474-3481.

[38] U. Sara, M. Akter, M. S. Uddin, *Image quality assessment through FSIM, SSIM, MSE and PSNR–a comparative study*, Journal of Computer and Communications, **7**(3) (2019), 8-18.

[39] D. R. I. M. Setiadi, *PSNR vs SSIM: Imperceptibility quality assessment for image steganography*, Multimedia Tools and Applications, **80**(6) (2021), 8423-8444.

[40] G. Shen, et al., *Perfect contrast XOR-based visual cryptography schemes via linear algebra*, Designs, Codes and Cryptography, **85** (2017), 15-37.

[41] H. Shi, et al., *A robust and secure zero-watermarking copyright authentication scheme based on visual cryptography and block GH feature*, Multimedia Tools and Applications, **81**(26) (2022), 38019-38051.

[42] S. J. Shyu, *Image encryption by random grids*, Pattern Recognition, **40**(3) (2007), 1014-1031.

[43] S. J. Shyu, *Image encryption by multiple random grids*, Pattern Recognition, **42**(7) (2009), 1582-1596.

[44] S. J. Shyu, M. C. Chen, *Minimizing pixel expansion in visual cryptographic scheme for general access structures*, IEEE Transactions on Circuits and Systems for Video Technology, **25**(9) (2015), 1557-1561.

[45] P. Singh, B. Raman, *Reversible data hiding based on Shamir's secret sharing for color images over cloud*, Information Sciences, **422** (2018), 77-97.

[46] USC University of Southern California. The USC-SIPI Image Database. url: http://sipi.usc.edu/database. (accessed: 08.30.2023).

[47] Z. Wang, et al., *Image quality assessment: From error visibility to structural similarity*, IEEE Transactions on Image Processing, **13**(4) (2004), 600-612.

[48] Z. Wang, G. R. Arce, G. Di Crescenzo, *Halftone visual cryptography via error diffusion*, IEEE Transactions on Information Forensics and Security, **4**(3) (2009), 383-396.

[49] D. S. Wang, et al., *Optimal contrast grayscale visual cryptography schemes with reversing*, IEEE Transactions on Information Forensics and Security, **8**(12) (2013), 2059-2072.

[50] D. S. Wang, F. Yi, X. Li, *Probabilistic visual secret sharing schemes for grey-scale images and color images*, Information Sciences, **181**(11) (2011), 2189-2208.

[51] G. Wei, *Some similarity measures for picture fuzzy sets and their applications*, Iranian Journal of Fuzzy Systems, **15**(1) (2018), 77-89.

[52] X. Wu, Z. R. Lai, *Random grid based color visual cryptography scheme for black and white secret images with general access structures*, Signal Processing: Image Communication, **75** (2019), 100-110.

[53] X. Wu, W. Sun, *Improving the visual quality of random grid-based visual secret sharing*, Signal Processing, **93**(5) (2013), 977-995.

[54] X. Wu, W. Sun, *Extended capabilities for XOR-based visual cryptography*, IEEE Transactions on Information Forensics and Security, **9**(10) (2014), 1592-1605.

[55] X. Wu, C. N. Yang, *Invertible secret image sharing with steganography and authentication for AMBTC compressed images*, Signal Processing: Image Communication, **78** (2019), 437-447.

[56] X. Wu, C. N. Yang, *Probabilistic color visual cryptography schemes for black and white secret images*, Journal of Visual Communication and Image Representation, **70** (2020), 102793.

[57] C. N. Yang, *New visual secret sharing schemes using probabilistic method*, Pattern Recognition Letters, **25**(4) (2004), 481-494.

[58] C. N. Yang, T. S. Chen, *Aspect ratio invariant visual secret sharing schemes with minimum pixel expansion*, Pattern Recognition Letters, **26**(2) (2005), 193-206.

[59] C. N. Yang, C. C. Wang, T. S. Chen, *Visual cryptography schemes with reversing*, The Computer Journal, **51**(6) (2008), 710-722.

[60] C. N. Yang, Y. Y. Yang, *On the analysis and design of visual cryptography with error correcting capability*, IEEE Transactions on Circuits and Systems for Video Technology, **31**(6) (2020), 2465-2479.

[61] L. A. Zadeh, *Fuzzy sets*, Information and Control, **8**(3) (1965), 338-353.

[62] D. Zhang, et al., *HP-VCS: A high-quality and printer-friendly visual cryptography scheme*, Journal of Visual Communication and Image Representation, **78** (2021), 103186.