Enhanced Visual Cryptography Based on Arnold's Cat Map

[1]Hajir Alauldeen Al-Bayati, [1]Dalal N. Hamod, and [2]Lahieb M. Jawad
[1]Department of Computer Science, College of Science, Al-Nahrain University, Jadriya, Baghdad, 10011, Iraq.
[2]Department of Computer Networks Engineering, College of Information Engineering, Al-Nahrain University, Jadriya, Baghdad, Iraq.

Corresponding author: Hajir Alauldeen Al-Bayati (hajaralaa110@gmail.com)

Abstract The field of color visual cryptography has experienced significant growth, enabling the secure transmission of color images over the Internet. This innovative methodology partition images into shares, mirroring the principles of Naor and Shamir's approach but tailored specifically for color images. Color visual cryptography (VC) operate by divide color secret images into shares, treat each color pixel individually through the RGB and CMY channels. This study introduces an advanced CVC technique that integrate a chaotic encryption system, significantly enhance security measures. The proposed approach involves extract the channels component and apply a chaotic map to each channel with distinct masks, resulting in the generation of six shares (two for each color channel), subsequently XORing them with a randomly generated key matrix. This process creates new matrices, further enhance security. On the recipient's end, the secret color image is retrieved while maintaining high quality, as evaluated through metrics such as Peak Signal-to-Noise ratio PSNR, Mean Square Error MSE, Correlation Coefficients CC, Number of Pixels Changing Rate NPCR, and Unified Average Change Intensity UACI. Comparative analysis against existing methods demonstrates the superior efficient of this methodology in securely concealing color image secrets. Where the values of each metric were CC =1.0, MSE= 0.0 and PSNR= infinite. While, the best values of NPCR and UACI were 99.65%, 85.62% respectively these for the original channel and associated shares.

Index Terms: Visual Cryptography, Chaotic map, Encryption/Decryption, Shares, Security**,** Blockchain, Real Estate, Agriculture, Healthcare, E-Voting, Data security, Data Transparency.

1. INTRODUCTION

Nowadays, the Internet has gotten popular that it is used in practically every sector [1]. So in today digital world, data security is a serious concern [2]. Data is the raw material from which essential information is collected, therefore protects it security become crucial [3]. The dread worsens when dealing with shared information, particularly images. The expression "an image speaks a thousand words" emphasis the huge value of visual content [3]. However, this render an images more vulnerable to alteration, underlining the need for effective security measures [3]. Visual Cryptography (VC) emerges as a powerful solution, involve splitting an secret image into two chaotic images known as shares, with each one share going to one of participants [4]. Then decryption procedure involves overlapping these shares to retrieve the secret image [5]. VC just relies on encryption, which mean reducing the need for lengthy computations during decryption. This distinguishing characteristic makes VC extremely accessible to consumers with no cryptography skills. So this strategy is secure secret visual information in an exclusive manner that differs from other cryptography approaches as it decrypts secret information using human vision rather than sophisticated mathematical computations or decrypted machines [6].

Various techniques such as error diffusion, halftoning, and pixel expansion have been introduced to generate shares. While these methods improve security, they also increase complexity and cost [7]. and significantly reduce the quality of the decrypted image. Additionally, Visual cryptography approaches primarily handle black-and-white and grayscale images [8]. In address the challenge in the digital realm, conventional encryption methods such as symmetric which utilized single key and asymmetric encryption systems utilize public and private keys, are widely employed [9]. The proposed solution enables direct encryption and decryption of real-valued color images in RGB and CMY formats using a chaotic map alongside visual cryptography. This approach avoids pixel expansion and the need to convert images to binary, making it faster than traditional techniques. Besides, the security of the generated shares during encryption and the quality of the retrieved images have been assessed using PSNR, PNCR, UACI and Entropy metrics. These evaluations confirm that the solution provides robust security and retrieve images with optimal quality. In the realm of symmetric cryptography, data encryption techniques such as stream ciphers and block ciphers are widely utilized for their high-speed XOR and permutation operations. These methods have proven to be both effective and efficient, making them popular choices for securing sensitive information. Inspired by these established techniques, the proposed approach harnesses the power of the XOR operation.

Rijmen and Preneel's introduction of VC for color images marked a significant advancement in the field [10]. Building on, this paper explores a novel scheme to securely transfer secret color images in RGB and CMY formats. with significantly minimize complexity in transferring sensitive data. This research paper is organized into five parts: (1) Introduction, (2) Literature Review, (3) explain Chaotic System (chaotic map), (4) Proposed Approach, (5) Results and Discussion, and (6) Conclusion.

2. LITERATURE REVIEW

In the beginning, early VC (Visual Cryptography) approach were constrained to grayscale and binary images [11]. Subsequently, Hou extended the approach to include color images with multiple layers of transparency[11]. Recent suggestions from other authors have proposed adjustment to the encryption and decryption procedure, aiming to enhance security and image quality, respectively. Overall, the reviewed literature showcases various approaches to image encryption, each with its strengths and challenges. Methods like those based on algorithms and modulo encryption offer high security metrics like NPCR and UACI but often at the cost of computational complexity and image quality degradation, and vice versa when achieve good quality.

S. Fadhil and K Farhan [12] introduced digital image encryption method based on the Lorenz chaotic system. The encryption algorithm comprises three phases. Firstly, Black Mask Algorithm applied to the secret image, this algorithm generates four shares (C, M, Y, K). Next, the shares pixels generated by the black mask algorithm pass the Scrambling Process. Lastly, the Lorenz chaotic system is used to give more randomness to the scheme, then product the new secret keys via a logistic map to encrypt the four shares produced from previous stages (C, M, Y, and K), the program has been found to be resistant to differential attacks, it UACI was 33%. the Pixel to Signal Noise Ratio PSNR values achieved is 58.39 which mean lossy in retrieve the image quality, Mean Square Error MSE was 0.09 For applications that require high fidelity image retrieval, even minor losses can be significant. And Entropy 7.53 was good.

P. Saini, et al [13] suggests a modulo encryption-based Visual Secret Sharing (MEVSS) system for encrypting a secret image. The secret image is separated into two or four share images. Then the encryption of the secret image is generated by XOR operation, resulting in meaningless shares. The MEVSS algorithm, color images are encrypted using modulo encryption without being converted into any other form, such as binary or grayscale. By their approach demonstrated efficiency, evidenced by the near standard values of 99.604% and 33.4469% for the Number of Pixels Changing Rate NPCR and UACI respectively. Further, the correlation value (0.00007) indicating less predictability by third parties. Despite its advantages of the MEVSS technique, except the system reliance on modulo encryption may limit its adaptability to different types of images and encryption requirements. so, the approach may require significant computational resources, making it less suitable for real-time applications or devices with limited processing power.

The SKMSS system allows for the secure sharing of multiple secret images by dividing each image into shares that can only be retrieved when a sufficient number of shares are combined, as in [14] the authors used a mix of secret key management and Shamir's secret sharing algorithm to offer a reliable and secure private image sharing technique. They designed an encryption technique along with an efficient secured (k, k) multiple secret color images-based sharing (SKMSS) system. After each share is formed, it is encrypted using special keys generated by the Cuckoo Search Optimization Algorithm based on the SIMON cipher. The SIMON cipher is a lightweight block cipher designed for optimal performance in constrained environments, providing strong security. That scheme's achievement is assessed according to the metrics like peak signal-to-noise ratio (PSNR= 47.0149dB) indicating poor degree of quality to retrieve image, mean square error (MSE= 1.2930) suggests there is still some loss of quality. Finally, the use of multiple techniques (Shamir's secret sharing, Cuckoo Search Optimization, SIMON cipher) adds complexity to the system.

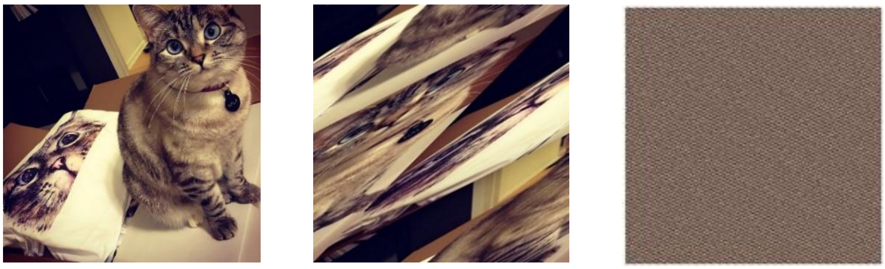
Ref. [15] Visual Cryptography and Elliptic Curve Cryptography (ECC) is employed to generate individual red, green and blue shares utilizing the Visual Secret Sharing (VSS) Scheme, their research introduces the application of the ECC method for both image encryption and decryption. They used for encryption a public key cryptography generator, while the ECC method's secret key generates the decryption process. The process involves dividing each RGB pixel value toward three shares, with subsequent encryption and decryption using the Rubik’s cube encryption algorithm applied to Elliptic Curve Cryptography shares. Their results of were PSNR and MSE were 92.0571 dB, 0.0277, however NPCR and UACI 44.44, 13.88 respectively, mean low security against attacks because the NPCR and UACI necessary to comprehensively assess the scheme's resilience against various cryptographic attacks.

Ref. [16] suggested a novel V-net convolutional neural network (CNN) based on four-dimensional hyperchaotic system for medical image encryption is presented in this study. Firstly, the plaintext medical images are processed into 4D hyperchaotic sequence images, including image segmentation, chaotic system processing, and pseudorandom sequence generation. Then, V-net CNN is used to train chaotic sequences to eliminate the periodicity of chaotic sequences. Finally, the chaotic sequence image is diffused to change the raw image pixel to realize the encryption processing. Simulation test analysis demonstrates that the proposed algorithm required high computational complexity and resource demands of the V-net CNN and 4D hyperchaotic system, which may limit its practicality for real-time or resource-constrained environments. They gated MSE value 0.8428, NPCR value 99.6102 and UACI value 33.4659.

3. CHAOTIC SYSTEM

Or Chaotic map, invented in the 1960s from mathematics and physics, explains the complex and allegedly irregular behavior exhibited in specific nonlinear dynamical systems [17][18]. The inherent unpredictability and complexity of chaotic behavior make the systems important for the development of cryptography techniques. Unlike typical cryptographic methods that rely on computational complexity [19]. chaotic maps use the chaotic character of certain mathematical equations to improve security [20]. There is different digitizing chaotic maps, such as the Tent map [21], Henon map [22], Logistic map [23], [24], Cat map, and Chua's attractor [25], Cat map, also known as Arnold map, gets applied to the original image along pixel locations are shuffled [26]. During several rounds, the image becomes irrelevant and twisted, and the association between neighboring pixels is entirely disrupted as in Fig. 1 illustrate number of iterations. In the context of the cat map, continually applying the transformation to a starting points (x, y) and (w, h) are the width and height of an image, result in an apparently random and unexpected set of points so, cat map is given by [27]:

$$Xn = (2x + y) \bmod w, \quad Yn = (x + y) \bmod h \qquad (1)$$



original image

with1 iterations

with10 iterations

Fig.1. Cat map iterations

4. PROPOSED APPROACH

The proposed approach a visual cryptography encryption/decryption strategy is employed to securely transmit sensitive images between sender and receiver in two formats RGB and CMY. Color images are employed to generate shares. Fig. 2. illustrate the key steps of the proposed methodology, outline the major processes on the sender's side and receiver side.

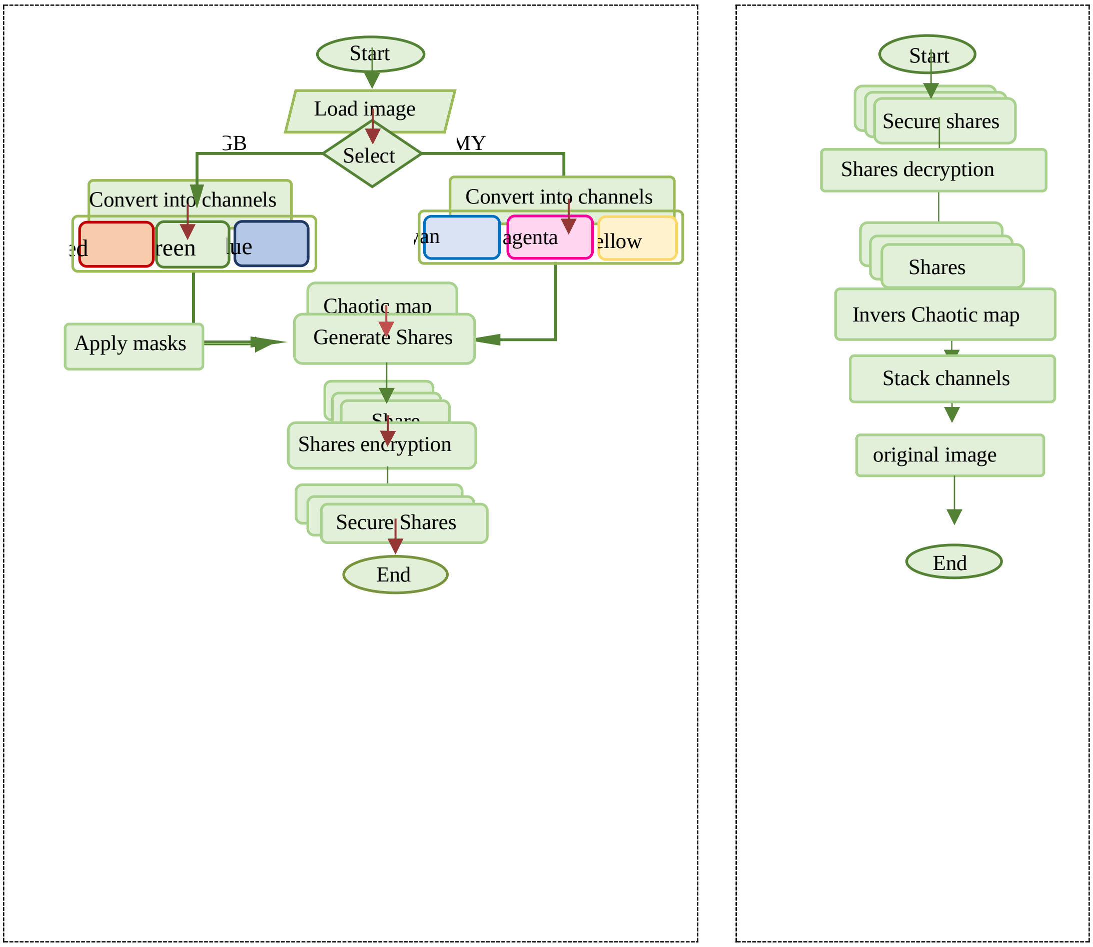


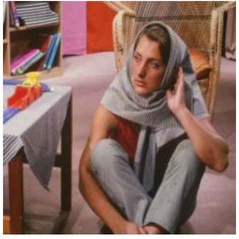
Fig.2. proposed flowchart, a) sender side and b) receiver side.

4.1. Sender Side

4.1.1 Load Image

In this step, the secret color images that used in security domains is loaded, and this image is selected to prepare it to the next step, the test is done on several images and different sizes with image file types JPEG (or JPG), PNG, and JFIF. Such Lena, peppers, Barbara, house, baboon and plane as illustrated in Fig.3.

Lena 256*256


Barbara 474*474

House 156*156

Peppers 347*347

Baboon 900*900

Birds 192*192

Fig.3. Test images.

4.1.2 Select Channels

The proposed approach handled with two formats RGB and CMY, so channels of the secret color image is extracted to produce three unique matrices, each representing a color component of the image. The following Algorithm 1 is used to extract the separate color component.

Algorithm 1: Extract and Display RGB or CMY Channels

Input: Secret image, channel_type (RGB or CMY)

Output: Display the selected channel

```
processes: (steps)
Start:
Step 1: load secret color image
Step 2: If channel_type = "RGB" then
            //Extract the blue channel (B) from secret image as a float array
            B =  secret_image[:, :, 0]
            //Extract the green channel (G) from secret image as a float array
            G =  secret_image[:, :, 1]
            // Extract the red channel (R) from secret image as a float array
            R =  secret_image[:, :, 2]
      Else If channel_type = "CMY" then
           // Extract cyan channel (C) by subtracting the red channel from 255
           C = 255 -  secre _image[:, :, 2]
           //Extract magenta channel (M) by subtracting green channel from 255
           M = 255 -  secret_image[:, :, 1]
           //Extract yellow channel (Y) by subtracting blue channel from 255
           Y = 255 - o secret_image[:, :, 0]
        End If
Step 3: If channel_type ="RGB" then
                Display the blue channel (B)
                Display the green channel (G)
                Display the red channel (R)
             Else If channel_type is "CMY" then
                Display the cyan channel (C)
                Display the magenta channel (M)
                Display the yellow channel (Y)
            End If
End
```

4.1.3 Cat Map

Here the Cat Map function implementation is designed to handle individual RGB or CMY channels derived from the secret image. These channels are considered as numerical arrays, and the Cat Map function is applied sequentially to each channel for the specified number of iterations is determined by 100 this ensure that each pixel undergoes to processing based on the cat map equation and resulting a highly scrambled image due to the chaotic nature of the map, as demonstrated in Algorithm 2. Where Ch1, Ch2, Ch3 are the channels of Red, Green, Blue or Cyan, Magenta, Yellow.

```
Algorithm 2: Cat Map Function
Input: Ch1, Ch2, Ch3 are the channels of CMY or RGB channels, iterations (100)
Output: Cat-mapped channels
processes: (steps)
Start
Step 1: Set Ch=Channel
        Set W= W_Channel       // W_Channel is a width of Channel
        Set H=H_Channel        //H_Channel is a height of Channel
Step 2: for n=1 to 100
        Step2.1 Create mesh grids X and Y of Ch
        Step 2.2 $X1= (2 * X+ Y) \% W$
                 $Y1=(X + Y) \% H$
        // Update x and y using the Cat Map formula.
        Step2.3: Cat_Ch2=store (X1, Y1)
        End For
Step3: Return Cat_Ch2
        //the updated image values at coordinates [x, y]
End
```

4.1.4 Shares Generation

The custom mask generating process involve identifying the shifting between pixels to identify pixel values in the channel as belonging to Mask 1 or Mask 2. Where For each pixel at position (i, j):

- These masks are initially filled with zeros.
- If the sum of the indices (i + j) is even, mask1 at (i, j) is set to 0. And the odd values, mask1 set to 1.
- If the sum of the indices (i + j) is even, mask2 at (i, j) is set to 1. And the odd values, mask2 set to 0.
- This results in a checkerboard pattern where mask1 and mask2 alternate between 1s and 0s.

mask1 represents the regions covered by Share 1, while mask2 represents the regions covered by Share 2. As in Algorithm 3, this distinction allows for the precise differentiation and allocation of specific areas to each share, ensuring the integrity and uniqueness of the generated shares in the visual cryptography approach. Consequently, after completing the mentioned step, resulting in the creation of 2 shares for each, totaling 6 shares overall (2^3 = 6), as illustrated in Algorithm 4.

```
Algorithm 3: Generate Masks
Input: mask1,mask2 (initial two matrix as zero matrix)
Output: Mask1, Mask2
```

```
Processes:
Step 1: Set Mask1= zeros _array
           Set Mask2= zeros _array
Step 2: for i=1 to Hight_Mask1
      Step 2.1:  For j=1 to Width_Mask1
      begin
         Step 2.1.1: sum=i+j
         Step 2.1.2: If the (sum = even)
             Set mask1[i, j] = 1
         Else IF
            Set mask2[i, j] =1
      End IF
       Next j
    End For j
  Next i
End For i
Step 3: return Mask1, Mask2
End
```

Algorithm 4: Generate Shares by Masks

```
Input: Cat-mapped channels, mask1, mask2
Output: Shares for each channel
```

```
processes: (steps)
Start
Step 1: Set channel1=Cat_Ch1
Set channel2=Cat_Ch2
          Set channel3=Cat_Ch3
Step 2: Call:: Generate Masks(mask1,mask2)
//Algorithm (3.6) generate masks that used mask1 and mask2 as initial //masks with zero values and returns Mask1 and Mask2 as a masks
    begin
          Step 2.1:  share1 = (channel1 * Mask1)
          Step 2.2:  share2 = (channel 1* Mask2)
          Step 2.3: Share3 = (channel 2 * Mask1)
          Step 2.4:  share4 = (channel 2* Mask2)
          Step 2.5: Share5 = (channel 3 * Mask1)
Step 2.6: Share6 = (channel 3 * Mask2)
Step 2.7: store share1, share2, share3, share4, share5, and share6
Step 3: Display (share1, share2, share3, share4, share5, share6)
End
```

4.1.5 Shares Encryption

Once the share manufacturing procedure is done, these six previously formed shares are additionally encrypted using the XOR technique to provide more Security [28][29]. This is accomplished by generating random key matrix Ki of the identical size as the channel matrices. As in Aalgorithm 5. this key matric is XORed with each share matrices to create the new matrix Sk1 and Sk2, ….Sk6. respectively.

Algorithm 5: Shares Encryption

Input: Ch1_share1 and Ch1_share2, Ch2_share1 and Ch2_share2, Ch3_share1 and Ch3_share2 (from algorithm 4).

Output: final shares

```
processes: (steps)
Start
    Step 1: Generate a random key matrix
    Step 2: Perform bitwise XOR operation between shares from Algorithm 4 and
    the key matrix
            Sk1 = bitwise_xor (B_share1, reshaped_key_matrix[0])
            Sk2 = bitwise_xor (B_share2, reshaped_key_matrix[1])
            Sk3 = bitwise_xor (G_share1, reshaped_key_matrix[2])
            Sk4 = bitwise_xor (G_share2, reshaped_key_matrix[3])
            Sk5 = bitwise_xor (R_share1, reshaped_key_matrix[4])
            Sk6 = bitwise_xor (R_share2, reshaped_key_matrix[5])
    Step 3: Display the share of Sk1   //share1 of Blue channel
    Step 4: Display the share of Sk2   //share2 of Blue channel
    Step 5: Display the share of Sk3   //share1 of Green channel
    Step 6: Display the share of Sk4   //share2 of Green channel
    Step 7: Display the share of Sk5   //share1 of Red channel
    Step 8: Display the share of Sk6   //share2 of Red channel
End
```

4.2 Recipient Side: Decryption Process

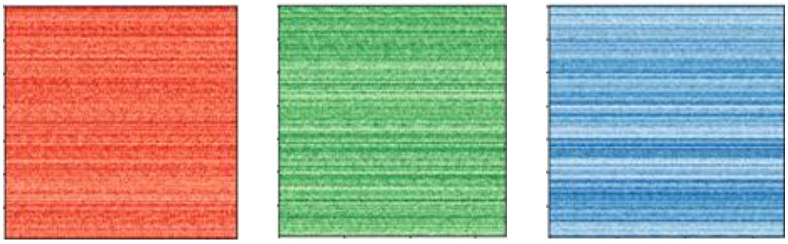
During the share retrieval phase, shares which encoded by both the cat map and XOR operation, then followed by decryption techniques include invers cat map and XORing operation. Once the decryption procedure is completed utilizing the*se* reverse method, CMY or RGB channels values will be extracted from these shares, to reobtained the secret image. without needing to apply masks again as descripted about feature of VC that once stacked the decrypted shares, the original channels is retrieved. lastly stack the channels to provide a full and accurate retrieval of the secret image.

5. RESULTS AND DISCUSSIONS

The system was developed utilizing the suggested technique on test several images and different sizes such Lena, peppers, Barbara, house, baboon and plane. we used peppers image as example to display shares image.

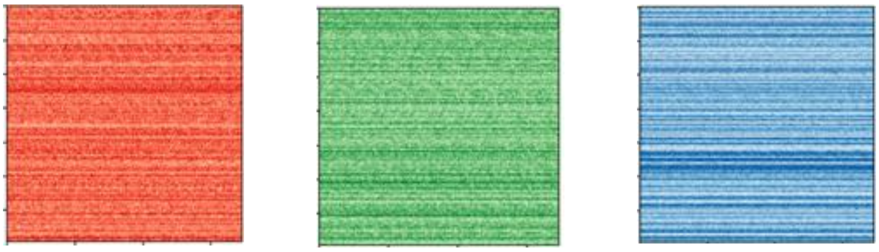
5.1 Shares of color image

Fig. 4 and Fig. 5 illustrate the first and second RGB shares created using the proposed VC approach for the peppers image example. Also, in Fig. 6 and Fig. 7 represent the first and second shares respectively for the CMY channel images example. So shows the difference in RGB and CMY channels.



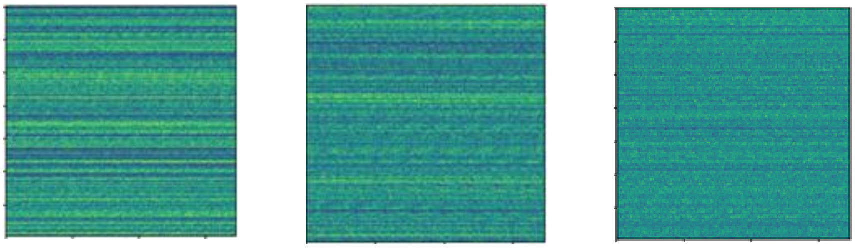
Red channel Green channel Blue channel

Fig.4. First Shares for RGB Channels.



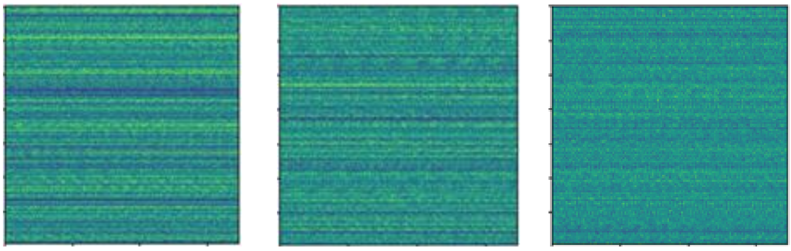
Red channel Green channel Blue channel

Fig.5. Second Shares for RGB Channels.



Cyan channel Magenta channel yellow channel

Fig.6. First Shares for CMY Channels.

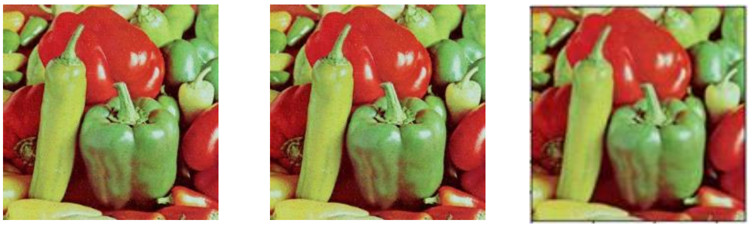


Cyan channel Magenta channel yellow channel

Fig.7. Second Shares for CMY Channels

5.2 Resultant images

According to the scenarios stated above, there will be a retrieved when the shares are gathered together. In Fig. 8 provide peppers image is an example, (a) shows an example of a Secret image, whereas (b) shows when the image is retrieved when using RGB format. (c) shows the retrieved secret image for CMY format.



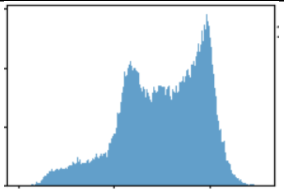
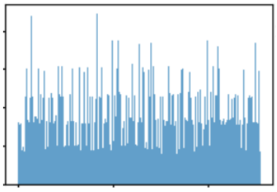
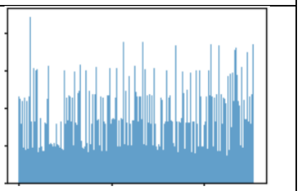
(a) (b) (c)

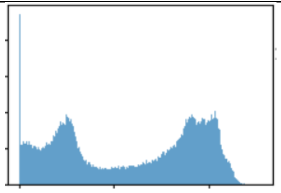
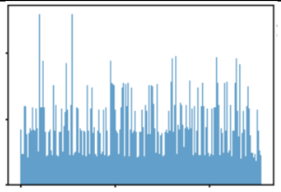
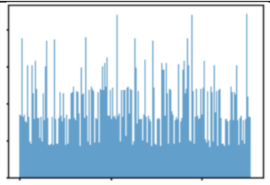
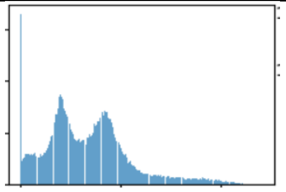
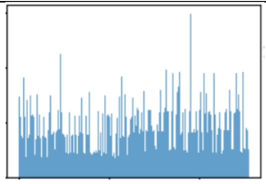
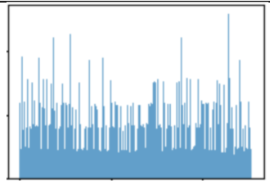
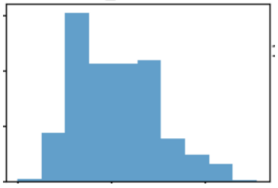
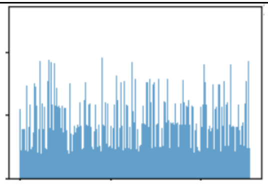
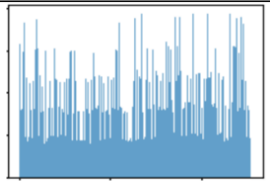
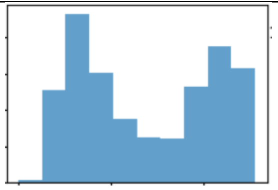
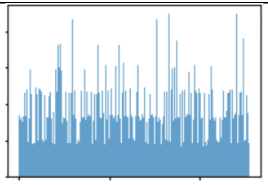
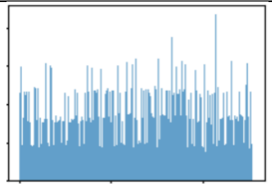
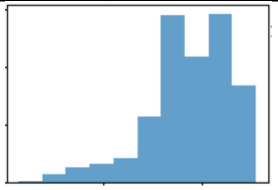
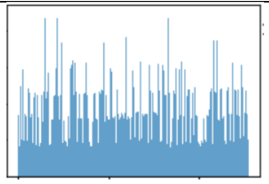
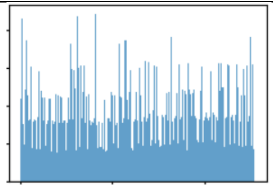
Fig.8. Result of Retrieval image (a) Secret image, (b) RGB Retrieved image, (c) CMY Retrieved image.

5.3Histogram Analysis

analyze the histogram of the secret image and its corresponding share images for each channel, as illustrated in Table 1. The shares exhibit no similarity to the original channel image, which prevents to gathering any information about the secret image from individual shares. The histogram also demonstrates the encryption quality of the proposed approach. Furthermore, the histograms for Share1 and Share2 differ, ensure that each contains distinct information.

Table 1. Histogram analysis of channels and their shares

channel	Original Channel	Share1	Share2
Red			

Green			
Blue			
Cyan			
Magenta			
Yellow			

5.4 Experimental Results

there is clarification is done between RGB and CMY color image and values in terms of the metrics Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE), Correlation Coefficient (CC), Number of Pixels Changing Rate (NPCR) and Unified Averaged Changed Intensity (UACI) and following results are found.

MSE: is the measure which represents the cumulative squared error between the secret image and resultant image. Equation (2) measured the MSE value for retrieved images. Where Xi denotes the original sample data, Yi refers to the processed one and n is the shape of the secret image.

$$MSE = \frac{1}{n}\sum_{i=1}^{n}(X_i - Y_i)^2 \qquad (2)$$

PSNR: is usually expressed in terms of the logarithmic decibel. The higher the PSNR, the better will be the quality of the secret image.

$$\text{PSNR} = 10 * \log_{10}\left(\frac{\text{MAX}^2}{\text{MSE}}\right) \qquad (3)$$

Correlation coefficient (CC) measures to analyze the retrieved image. Ideally, a VC scheme should have a CC value near from one, CC is calculated as:

$$CC = \frac{\sum(X_i - \bar{X})(Y_i - \bar{Y})}{\sqrt{\sum(X_i - \bar{X})^2\sum(Y_i - \bar{Y})^2}} \qquad (4)$$

Where Xi and Yi: These variables represent in the context of visual cryptography, X and Y could be pixel values from different shares of an image. $\bar{X}$ and $\bar{Y}$: These symbols represent the mean (average) values of the images X and Y.

In Table 2. The suggested approach achieves higher potential PSNR and MSE values for all test images, indicating that the original and retrieved images are extremely match. This means that the proposed approach can consistently provide high-quality retrieved images. Also, CC had 1 value for all tested image, indicates a perfect positive linear correlation.

Table 2. Performance Metrics

Image	MSE	PSNR	CC
pepper	0.0	inf dB	1.0
Lena	0.0	inf dB	1.0
house	0.0	inf dB	1.0
peppers	0.0	inf dB	1.0
Baboon	0.0	inf dB	1.0
Birds	0.0	inf dB	1.0

The aim is to guarantee that even a slight alteration to the secret image yield entirely different shares, a characteristic indicated by significant NPCR and UACI values. NPCR and UACI are calculated as:

$$UACI = \frac{\sum C1(i,j) - C2(i,j)}{N} \qquad (5)$$

In (5) sum up all the absolute intensity (C) differences. Then divide the sum by the total number of pixels (N) to get the average intensity difference. Equation (6) count the number of pixels that have changed between the two images.

$$\text{NPCR} = \left(\frac{\text{Num. of Changed Pixel}}{\text{Total Num. of Pixel}}\right) * 100\% \qquad (6)$$

NPCR and UACI Analysis: The number of changing pixels rate (NPCR), and unified averaged changed in-tensity (UACI) metrics are used to quantitively analyze the differences between the original channel and share images. These metrics are also commonly used as a measure of resistance against differential attacks. The aim is to guarantee that even a slight alteration to the secret image yield entirely different shares, a characteristic indicated by significant NPCR and UACI values. NPCR and UACI are calculated as:

$$UACI = \frac{\sum C1(i,j) - C2(i,j)}{N * 255} \times 100\% \qquad (7)$$

In (7) sum up all the absolute intensity (C) differences. Then divide the sum by the total number of pixels (N) to get the average intensity difference. Equation (8) count the number of pixels that have changed between two images.

$$\text{NPCR} = \left(\frac{\text{Num. of Changed Pixel}}{\text{Total Num. of Pixel}}\right) * 100\% \qquad (8)$$

From Table 3. the NPCR values, we observe that both RGB and CMY channels have very high NPCR values, indicating that a large percentage of pixels have changed between the original and encrypted images. However, there is no significant difference in NCPR values between RGB and CMY channels. Looking at the UACI values, we can see that both RGB and CMY channels have varying UACI values across the channels. However, CMY is a little higher in points.

Table 3. Security Analysis by NPCR and UACI

Channels	NPCR		UACI	
	Share1	Share2	Share1	Share2
Red	99.59%	99.61%	30.00%	29.82%
Green	99.63%	99.59%	32.94%	33.84%
Blue	99.57%	99.62%	33.69%	33.21%
Cyan	99.60%	99.61%	28.06%	28.56%
Magenta	99.59%	99.65%	33.83%	33.14%
Yellow	99.61%	99.62%	33.55%	33.15%

In Fig.9. NPCR values (close to 100%) across all color channels and shares, suggesting strong encryption performance. UACI also are similar, and there is little difference between the values of different color channels.

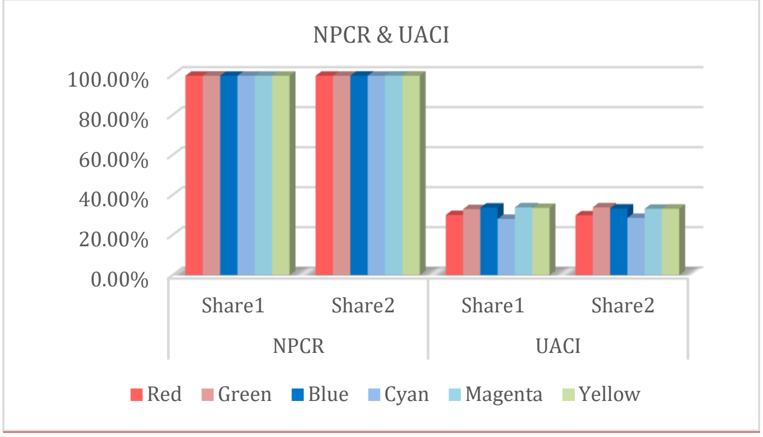


Fig.9. NPCR & UACI compression

Additionally, the **Entropy:** measures the uncertainty or randomness in an image. In Table 4. demonstrate the entropy values across RGB and CMY channels and their corresponding shares, high entropy reflects robust security measures, making it challenge for attackers to decipher the secret image without combine shares. In Fig.10. Overall, for all color channels, the entropy values are high, and observe that share2 of Blue channel is highest one.

Table 4. Entropy values for shares

Channels	Entropy	
	Share1	Share2
Red	7.8636	7.8750
Green	7.8683	7.8578
Blue	7.8568	7.8859
Cyan	7.8612	7.8590
Magenta	7.8577	7.8490
Yellow	7.8824	7.8717

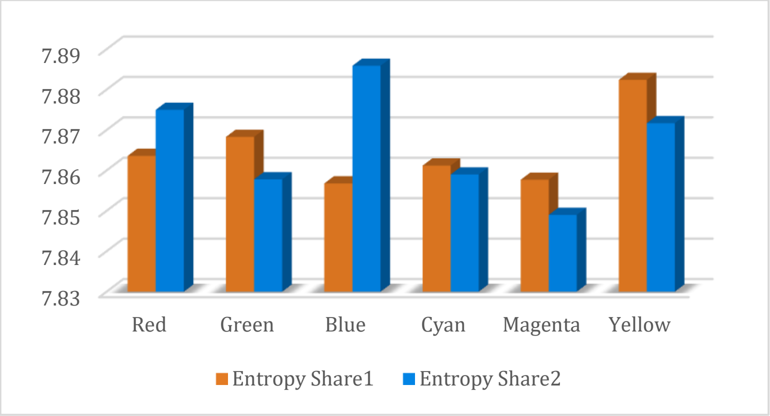


Fig.10. Entropy Comparison

5.5 Time Complexity Analysis

The time complexity of the cryptography approach, which involves chaotic map transformations and XOR operations, is summarized in the table below Table 5. providing a comprehensive view of the time complexity.

This analysis demonstrates that the performance of the proposed approach is linearly dependent on the number of iterations of the Cat Map transformation and quadratically dependent on the size of the image.

Table 5. Time complexity

Process	Process Step	Operation	Number of Operations	Time Complexity
Encryption Process	Cat Map Transformations	Per channel (B, G, R)	$3 \times k \times n^2$	$O(k*n^2)$
	Bitwise XOR Operations	6 XOR operations	$6 \times n^2$	$O(n^2)$
	Total Encryption Complexity			$O(k*n^2)$
Decryption Process	Bitwise XOR Operations	6 XOR operations	$6 \times n^2$	$O(n^2)$
	Inverse Cat Map Transformations	Per channel (B, G, R)	$3 \times k \times n^2$	$O(k*n^2)$
	Reconstruct Image	Merging RGB channels	n^2	$O(n^2)$
	Total Decryption Complexity			$O(k*n^2)$

5.6 Comparison of the Proposed approach and Existing Methods

The simulation results presented in this section compare the performance of the proposed approach with other existing schemes, highlighting key metrics and observations.

Table 6. show that the suggested strategy outperforms other schemes across various metrics. Notably, the PSNR and CC values reveal that the retrieve images have extremely high fidelity relative to the originals, with no noise or distortion, reflecting greater PSNR and CC values than techniques referenced in [13], [14] and [15]. Also, the security analysis shows that the proposed approach achieves near-maximal NPCR value for it shares, comparable to the other schemes [13], [15] and [16]. This indicates that the shares have a high level of security, as they lack statistical information that may be used to obtain knowledge about the secret image. Moreover, in terms of image quality MSE values 0.0 indicate retrieval without any pixel value differences, according to another study in [12], [14] and [16]. additionally proposed approach achieved closer to ideal CC values are 1.0 confirming the high fidelity of the retrieval, further underline it effectiveness and robustness. Additionally, comprising the highest UACI value for each research and found that proposed approach achieves best difference between the two images.

Overall, the simulation results affirm the superiority of the proposed method in terms of both image retrieved and security attributes when compared to existing schemes.

Table 6. Comparison Metrics

Schemes	MSE	PSNR	CC	NPCR	UACI
Proposed approach	0.0	Inf	1.0	99.65%	33.84%
[12]	0.09	58.39	--	--	__
[13]	--	100.00	0.000073	99.604%	33.446%
[14]	1.2930	47.0149	0.9997	--	__

[15]	93.44 %	69.91	--	92.16%	13.88%
[16]	0.8428	__	__	99.610%	33.465%

CONCLUSION

In this paper, a novel visual cryptography approach optimized for color images is introduced, which uses a cat map to improve image security. The suggested approach divides a secret image into RGB or CMY format to generate six shares, improving image security and resilience against unauthorized access. Furthermore, the use of the XOR operation strengthens security measures, particularly for color images, by introducing complexities that increase encryption strength. This combination of chaotic map-based transformation and XOR operation not only provides strong image security but also achieves a balance between security and computational efficiency. Experimental analysis of the proposed approach has shown that it achieves ideal results in various metrics such as NPCR, CC, UACI, and PSNR and outperforms many of its peers marking a valuable contribution to the field of image encryption and security which the best values of each metric was NPCR 99.65%, UACI= 85.62%, CC =1.0, MSE= 0.0 and PSNR= infinity. For future work, the proposed scheme will be enhanced to generate shares with an additional strong cryptography algorithm.

REFERENCES

[1] Nabi, A. U., Ahmed, M., & Abro, A. (2022). An Overview of Firewall Types, Technologies, and Functionalities. International Journal of Computing and Related Technologies, 3(1), 10-16.

[2] Khan, H., Shaikh, S., Siddiqui, S., & Baksh, G. (2023). A Systematic Review of Block-chain Technology. International Journal of Computing and Related Technologies, 4(1), 1-12.

[3] A. Z. Liu, L. Logeswaran, S. Sohn, and H. Lee, "A picture is worth a thousand words: Language models plan from pixels," *arXiv preprint arXiv:2303.09031,* 2023.

[4] A. Gutub, "Boosting image watermarking authenticity spreading secrecy from counting - based secret - sharing," *CAAI Transactions on Intelligence Technology,* vol. 8, no. 2, pp. 440-452, 2023.

[5] B. Kukreja and S. Malik, "Triple Layered Security for Data Hiding Using Steganography and Visual Cryptography," *Authorea Preprints,* 2024.

[6] Somwanshi, Datta R., and Vikas T. Humbe. "An Optimal (2, 2) Visual Cryptography Schemes For Information Security." First International Conference on Advances in Computer Vision and Artificial Intelligence Technologies (ACVAIT 2022). Atlantis Press, (2023).

[7] John, B. A., Christhu, R., Rajeev, S., & Selva, M. G. (2020). Enhanced semantic visual secret sharing scheme for the secure image communication. Multimedia Tools and Applications, 79(23-24), 17057-17079.

[8] Karolin M, Meyyappan T (2019) Image encryption and decryption using RSA algorithm with share creation techniques. Int J Eng Adv Technol 9(2):2797–2800. https://doi.org/10.35940/ijeat.B4021.129219

[9] D. R. Ibrahim, J. S. Teh, and R. Abdullah, "An overview of visual cryptography techniques," *Multimedia Tools and Applications,* vol. 80, pp. 31927-31952, 2021.

[10] Karolin, M., & Meyyappan, T. , (20.19), 'Image encryption and decryption using RSA algorithm with share creation techniques'. Int J Eng Adv Tech, 9(2), 2797-2800.

[11] R. Karthik, et al., " "Image security based on rotational visual cryptography."," *Springer Nature Singapore,* pp. 87-96, 2022.

[12] S. A. Fadhil and A. K Farhan, "Color visual cryptography based on three dimensional chaotic map," *Iraqi Journal of Computers, Communications, Control and Systems Engineering,* vol. 22, no. 2, pp. 1-12, 2022.

[13] P. Saini, K. Kumar, S. Kashid, and A. Negi, "MEVSS: Modulo Encryption Based Visual Secret Sharing Scheme for Securing Visual Content," in *International Conference on Deep Learning, Artificial Intelligence and Robotics*, 2022: Springer, pp. 24-35.

[14] Shankar, K., Taniar, D., Yang, E., & Yi, O. (2021). Secure and optimal secret sharing scheme for color images. Mathematics, 9(19), 2360.2021)).

[15] Karolin, M., & Meyyappan, T. (2022), Visual Cryptography Secret Share Creation Techniques with Multiple Image Encryption and Decryption Using Elliptic Curve Cryptography. IETE Journal of Research, 1-8.

[16] Wang, Xiaowei, et al. (2022), "A New V - Net Convolutional Neural Network Based on Four - Dimensional Hyperchaotic System for Medical Image Encryption." Security and Communication Networks 2022.1 : 4260804. https://doi.org/10.1155/2022/4260804

[17] M. Bertaccini, *Cryptography Algorithms: A guide to algorithms in blockchain, quantum cryptography, zero-knowledge protocols, and homomorphic encryption*. Packt Publishing Ltd, 2022.

[18] Liu, J., Zhang, J., & Yin, S. (2023). Hybrid chaotic system-oriented artificial fish swarm neural network for image encryption. Evolutionary Intelligence, 16(1), 77-87.

[19] Mashkour, M. M., Jawad, L. M., & Sulong, G. (2023). A Secure Data Hiding For H. 264 Video Based on Chaotic Map Methods and RC4 Algorithm. Iraqi Journal of Information and Communication Technology, 6(3), 50-64.

[20] X. Ren and W. Yu, "The novel image encryption scheme based on three-dimentional coupled chaotic system," in *Journal of Physics: Conference Series*, 2021, vol. 2079, no. 1: IOP Publishing, p. 012027.

[21] S. S. da Silva, "A comparison analysis of using different numerical representations in digital chaotic maps," 2023.

[22] B. Abdulwahid Hameed and E. K. Gbashi, "A review of Chaotic Maps used for Generating Secure Random Keys," in *BIO Web of Conferences*, 2024, vol. 97: EDP Sciences, p. 00070.

[23] D. He, R. Parthasarathy, H. Li, and Z. Geng, "A Fast Image Encryption Algorithm based on Logistic Mapping and Hyperchaotic Lorenz System for Clear Text Correlation," *IEEE Access*, 2023.

[24] Fadhil, Meryam Saad, Alaa Kadhim Farhan, and Mohammad Natiq Fadhil. "Designing substitution box based on the 1D logistic map chaotic system." IOP Conference Series: Materials Science and Engineering. Vol. 1076. No. 1. IOP Publishing, 2021.

[25] R. S. Abdulaali and R. K. Jamal, "A comprehensive study and analysis of the chaotic Chua circuit," *Iraqi Journal of Science*, vol. 63, no. 2, pp. 556-570, 2022.

[26] Z. T. M. Al-Ta'i and S. M. Sadoon, "Securing Privacy: Encrypted Image Retrieval with CNNs and Chaos-Based Visual Cryptography on Cloud Computing," *International Journal of Intelligent Engineering & Systems*, vol. 16, no. 6, 2023.

[27] C. Li, K. Tan, B. Feng, and J. Lü, "The graph structure of the generalized discrete arnold's cat map," *IEEE Transactions on Computers*, vol. 71, no. 2, pp. 364-377, 2021.

[28] Mursi, Khalid T., et al. "A fast deep learning method for security vulnerability study of XOR PUFs." Electronics 9.10 (2020): 1715.

[29] Kiran, S., et al. "Development of cryptographic algorithm using bit shifting and Matrix XOR operations." (2022).