Computing and Informatics, Vol. 38, 2019, 701–727, doi: 10.31577/cai_2019_3_701

CHAOTIC ENCRYPTION AND PRIVILEGE BASED VISUAL SECRET SHARING MODEL FOR COLOR IMAGES

Aytekin Yildizhan

Computer Engineering Department
Hacettepe University
06800 Ankara, Turkey
e-mail: aytekinyildizhan@hacettepe.edu.tr

Nurettin Topaloglu

Computer Engineering Department
Gazi University
06500 Ankara, Turkey
e-mail: nurettin@gazi.edu.tr

Abstract. In the Privilege-based Visual Secret Sharing Model (PVSSM), each share has a unique privilege and a higher-privilege share contributes with more privilege to reveal the secret image. However, in PVSSM, when several shares with the higher priority are stacked, the secret image can be visibly displayed. This security problem is solved by applying a two-dimensional Logistic-Adjusted Sine Map (2D-LASM) to each share. This method is called Chaotic Encryption-based PVSSM. In this paper, we aim to present how Chaotic Encryption-based PVSSM is applied to color images. In order to assess the efficiency of this method, histogram analysis, data loss attack, salt-pepper noise attack, differential attack, chi-square analysis and correlation analysis tests were applied. The performance of this method has been evaluated according to NCPR, UACI, PSNR, SSIM and CQM. The proposed method achieved a good test values and showed better results compared to similar studies in literature.

Keywords: Cryptography, chaotic map, information security, visual secret sharing

Mathematics Subject Classification 2010: 94A60

1 INTRODUCTION

With the development of technology and the Internet network, digital images published and transmitted over the network have become extremely important. The transfer and storage of secret and private images such as military, intelligence, and medical images must be fast and secured. Thus, researchers have started to focus their attention on image security [1]. Traditional encryption algorithm such as Data Encryption Standard (DES) and Advanced Encryption Standard (AES) can be used to encrypt images.

However, image data is much greater than text data, so the traditional encryption algorithms require a lot of time to encrypt the image. In addition, the decrypted text must be equal to the original text, but decrypted image should not necessarily be equal to the original image [2]. Watermarking and steganography have been proposed instead of DES and AES for image encryption but these methods are suitable for single communication channel [3]. Therefore, Visual Secret Sharing Scheme (VSSS) methods could be one of the possible solutions.

Visual cryptography (VC), one of the VSSS methods, was first developed in 1994 by Naor and Shamir [4]. The approach of this system based fragmenting the key and distributing them to the different users. In key-based approach, if the key is lost or stolen, all secret information is inaccessible or revealed. In order to prevent crime, VC methods are used, especially cybercrime [5]. With this method, if any key is lost or stolen, other key pieces can be put together and generate the secret key. Also any user cannot get the secret information from any single key pieces.

In VC method, the secret image is divided into n images. These are called shares that do not contain any information about the secret image. If any r shares are stacked, the secret image is restored. The result of stacking shares in the VC is equivalent to that of the logical OR ($\vee$) operation. VC has the advantages that it eliminates complex algorithm to improve applicability and efficiency [6], and decryption can be done using the human visual system. However, if less than r shares are stacked, the content of the secret image remains hidden [7].

An increase in the number of shares causes more difficulties to reveal the secret image. However, if the number of the shares is too high, restoring the secret image will become difficult as well. To resolve this dilemma, Fang and Lin [8] presented a progressive VC (PVC) for binary image. While traditional VC needs all the necessary shares for the secret image to reveal, in PVC the secret image is gradually revealed as each share is added. Jin et al. [9] proposed PVC for color image. Fang's method [10] is about how to manage the shares more easily in PVC. On the other hand, with these methods, the shares have increased four times of the size of the original image and there is no order of privilege among the shares [8, 9, 10, 11].

In the process of revealing the secret image, it may be expected to be a privileged order among the shares in hierarchical systems such as military institutions, public institutions, and corporations. Therefore, the share with higher priority is distributed to people based on their positions or status. However, in most of the

studies, this situation has not been considered. In order to overcome this problem, it is necessary to use a privilege-based sharing scheme. The privilege means the capability to reveal the secret image. A group-based weighted VC is proposed in [12]. The shares are divided into different groups and given a different weight number within the group. Lin et al. [13] performed a study to determine the size of the shares according to their weights. However, when the size of any share is small, the weight of that share is small, too. Therefore, it reveals which share is small. Li et al. [14] suggested that each of the shares on the PVC scheme has a certain privilege. In their study, the shares are divided into four groups as essential, non-essential, limitedly essential and limitedly non-essential, but there is no order of importance for each group. Hou et al. [15] proposed that the importance of the shares is arranged from the lowest to the highest order. This is called the Privilege-based Visual Secret Sharing Model (PVSSM), and it has several advantages that each share size is the same as the secret image, the restored image has a better contrast than the traditional VC scheme and each share has a unique privilege level according to their order.

In PVSSM, when several shares with the higher priority are stacked, the secret image can be revealed. To solve this problem, it would be appropriate to encrypt each share. Because of the high correlation among adjacent pixels and bulk data capacity, traditional encryption algorithms such as DES, AES, RSA, are not suitable for image encryption [16]. To prevent image information leakage, chaotic systems are suitable for image encryption. Chaotic systems are used in many areas [17]. Chaotic maps are the core of a chaos-based image encryption [18]. Moreover, permutation-diffusion mechanism can be used in chaos-based image encryption [17, 19]. Chaotic maps have an excellent character such as ergodicity, flexibility, speed, unpredictability, and high sensitivity to initial state of the system and control parameter [17, 20]. As a result, chaotic-based encryption has become popular for image encryption [19].

There are many studies on chaos-based image encryption methods in protecting and transferring digital images. The level of security in chaos-based encryption depends on the performance of the chaotic maps [17]. Chaotic maps can be classified into two groups; one-dimensional and high-dimensional. The initial states and orbits of one-dimensional chaotic maps such as Logistic, Gaussian, Sinus and Tent maps, can be estimated easily [20, 21]. Arroyo et al. [20] demonstrated that the estimation of control parameters and timing attacks applied to one-dimensional chaotic maps and some weaknesses about linearity were found. Tang and Guan [22] show that control parameters were estimated in time-lagged Logistic and Mackey-Glass map by using genetic algorithm. These weaknesses have caused many security vulnerabilities in one-dimensional chaotic map [15, 19, 20]. In high-dimensional chaotic maps, because the system and control parameters are more complex, it is more unpredictable [19, 20, 21, 22, 23]. Therefore, it would be more appropriate to encrypt the shares with a high-dimensional chaotic map. However, because of the large number of parameters in the high-dimensional chaotic map, the system requirements are more expensive and the computational complexity is high [16, 17]. At the same

time, using more than one chaotic map can increase the calculation time [24]. Therefore, it is important that the high-dimensional chaotic map shows low calculation time and high degree of chaos feature [21]. A two-dimensional Logistic-adjusted Sine Map (2D-LASM) [17] is a high-dimensional chaotic map that provides these features.

In this paper, we aim to present the Chaotic Encryption-based PVSSM for color images. The secret color image is first separated into RGB channels. Then, RGB channels are transformed into binary images. PVSSM and 2D-LASM based image encryption are applied respectively to each channel. Even if the shares are captured and stacked, the secret image would not be seen. In decryption process, the shares of each channel are decrypted with 2D-LASM and stacked. Recreated RGB channels are merged. To obtain the original color image from the combined RGB channels, the pixel values of 1 are changed to 255. Finally, the secret image is revealed. Histogram analysis is applied for all R, G and B channels. In addition, for observing the proposed method's performance on different image distortions, data loss and salt-pepper noise attack are applied to the encrypted images. The results show that this method has high resistance against these attacks.

2 VISUAL CRYPTOGRAPHY

The VC was first proposed by Naor and Shamir [4], the secret image is divided into n shares. When r shares are stacked, the secret image is revealed. If $r-1$ shares stacked, the secret image cannot be visible. This is called (r, n) threshold mechanism [4, 15, 25, 26, 27, 28, 29]. In black-and-white VC scheme, black and white pixels are shared according to some rules. In $(2, 2)$ VC scheme, one pixel in the secret image is divided into four pixels in the share images in Figure 1.

In Figure 1, if the pixel is black, one of six blocks is randomly selected for the first share. According to the first share's block, the other block is selected for the second share. If the pixel is white, the same rule is applied. Then the shares are stacked. Black pixel is logical 1 and white pixel is logical 0. Therefore, black pixels in the secret image are obtained full black and white pixels in the secret image are obtained half-black-and-white. The stacked image is four times as big as the original image, but aspect ratio remains the same. Although the contrast of the secret image is degraded by 50 %, human visual system can still detect the content of the secret image.

In Figure 2, a black and white secret image with the words of "123456" is decomposed into two shares and the stacked image is shown.

In some studies, the privilege of the shares is limited or does not exist [4, 7, 9, 13, 28]. If the shares have a privilege order, it will be better for hierarchical systems. This means that if a person in hierarchical systems has higher privilege such as the manager of the company, etc., then his/her share must be also a higher privilege. Thus, more privileged shares are stacked, more information will be reached or revealed.

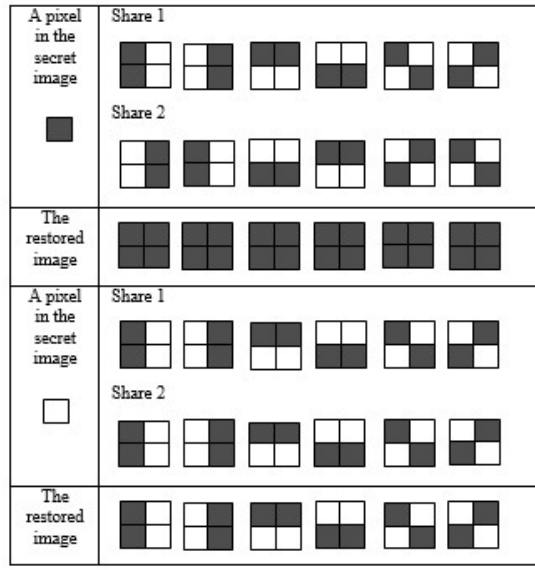
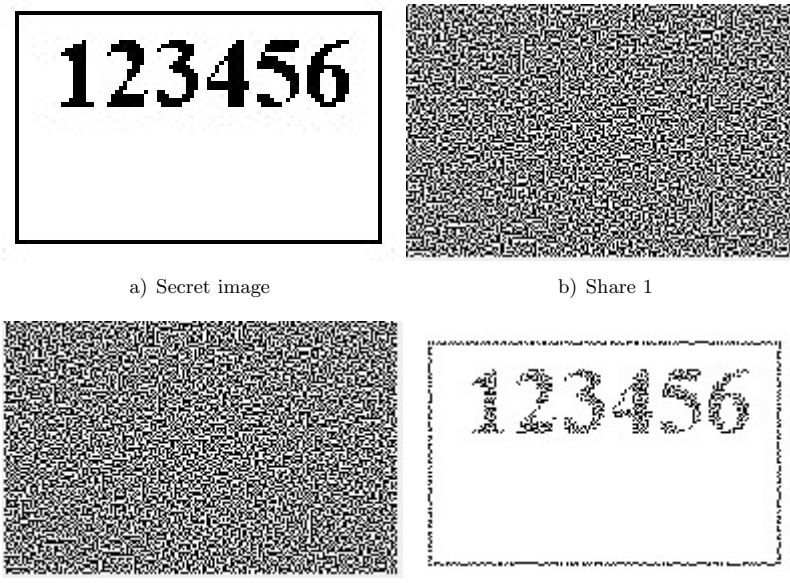


Figure 1. $(2, 2)$ VC scheme



a) Secret image b) Share 1

c) Share 2 d) Stacked image

Figure 2. Visual cryptography

Fang and Lin [8] first described a progressive VC on binary images. In their work, each pixel in the secret image was magnified to 2×2 blocks. If the black pixels are encrypted, 2×2 blocks are full black. If the white pixels are encrypted, one of randomly selected two pixels is white in 2×2 blocks. However, due to pixel enlargement, more memory and processing time are required.

Hou and Quan [29] reported that Fang and Lin's work [8] had pixel enlargement, unnecessary storage space and more transfer time, and also it had a low visual quality of the stacked images. Hou and Quan stated that they eliminated these disadvantages.

Fang [10] proposed a new progressive VC that stego images and shares are used together. The aim of this work is a more simplified management of shares. However, in Fang's method, the share has been increased in size by four times more than the secret image.

Hou [7] proposed a privileged-based approach. In Hou's study, to create the shares of color images, he uses three color shares (Cyan-Magenta-Yellow) and mask share. Thus, four shares are produced. The masks are randomly created to cover unwanted colors in the stacked image, while the three main colors represent the color share images. Although there is no privilege among the color shares, according to the mask, the stacked image is changed. In this case, the mask image is more privileged than the color share images. However, in this method, the size of the stacked image size has increased to four times as large as the original image and the encryption process is limited to only four shares.

Li et al. [14] posed the method that emphasizes the importance of the shares among themselves. The shares on the progressive VC scheme are classified into two groups: necessarily with higher importance and non-necessarily with lower importance. Later on, intermediate shares are also added with important and non-important shares, but it is difficult to manage the shares in this study. In addition, the size of non-important shares is larger than the size of the important ones. Because of the different size, the importance of shares is revealed.

PVSSM is proposed in [15]. With this work, each share has a unique level of privilege. The privilege level of the shares is set by the proportion of the black pixel in the secret image. This means the blacker pixels in the secret image, the higher the order of importance.

3 PRIVILEGED-BASED VISUAL SECRET SHARING MODEL

In this section, PVSSM is explained. The flow diagram of PVSSM is given in Figure 3.

The design of sharing matrices C^0 and C^1 is defined below. All rows and columns start from 1 and n is defined as the number of shares.

C^0 consists of two parts, the left-C^0 and the right-C^0. The column of left-C^0 is calculated as $m_1 = n(n-1)/2$. The size of left-C^1 is set to $n \times m_1$. In left-C^0, all 0s are placed to different columns. The number of 0s in i^{th} row is

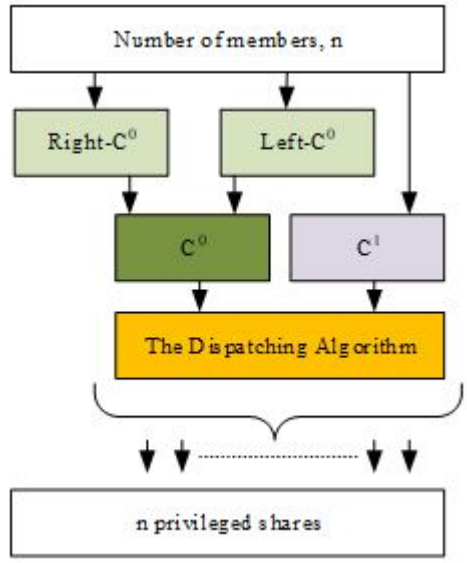


Figure 3. PVSSM flow diagram

equal to $n - i$. The remaining locations are filled with 1s. Right-C^0 and left-C^0 have the same number of rows. The column of right-C^0 is equal to $m_2 = n(n-1)(n-2)/2$. The size of right-C^0 is set to $n \times m_2$. All locations of right-C^0 are filled with 0s. After this design, right-C^0 and left-C^0 concatenate and the design of C^0 is completed.

The column of C^1 is calculated as $m = n(n-1)(n-1)/2$. Moreover, Equation (1) is satisfied:

$$m = m_1 + m_2. \tag{1}$$

The size of C^1 is set to $n \times m$. In C^1, all 1s are placed to different columns. The number of 1s in i^{th} row is calculated as $(n^2 - 3n + 2i)/2$. The remaining locations are filled with 0s. Therefore, the design of C^1 is completed.

After the design of the C^0 and C^1 sharing matrices, the dispatching algorithm is implemented to generate the shares in Figure 4.

Firstly, a random number "t", between 1 and m, is selected. If the pixel in the secret image is white (0), t^{th} column of C^0 is selected. The first element of this t^{th} column is distributed to the first share, the second element is distributed to the second share, the third element is distributed to the third share, etc. If the pixel in the secret image is black (1), t^{th} column of C^1 is selected. The first element of this t^{th} column is distributed to the first share, the second element is distributed to the second share, the third element is distributed to the third share, etc. The densities of the black pixels in the shares determine the level of its privilege in PVSSM because the human vision system more focuses on the black pixels in binary image. Output of

The Dispatching Algorithm:
Input: a halftone secret image SI, size of (i x j)
n, number of members
C^0 and C^1,sharing matrices
Output: n privileged shares, PS_k, k=1, 2, 3,…,n
Process:

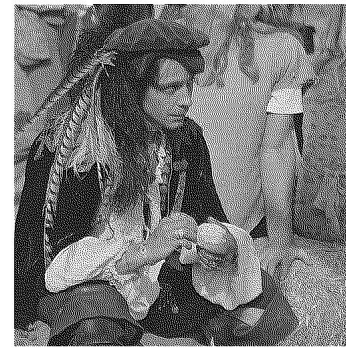
```
for a ← 1:i
    for b ← 1:j
        t ← Random Number (1 ≤ t ≤ m)
          if SI (a, b) is black
                for z ← 1:n
                  PSk(a, b) = C1z,t
          else
                for z ← 1:n
                  PSk(a, b) = C0z,t
```

Figure 4. The dispatching algorithm

this algorithm are privileged shares with increasing order and each share is a unique privilege [14].

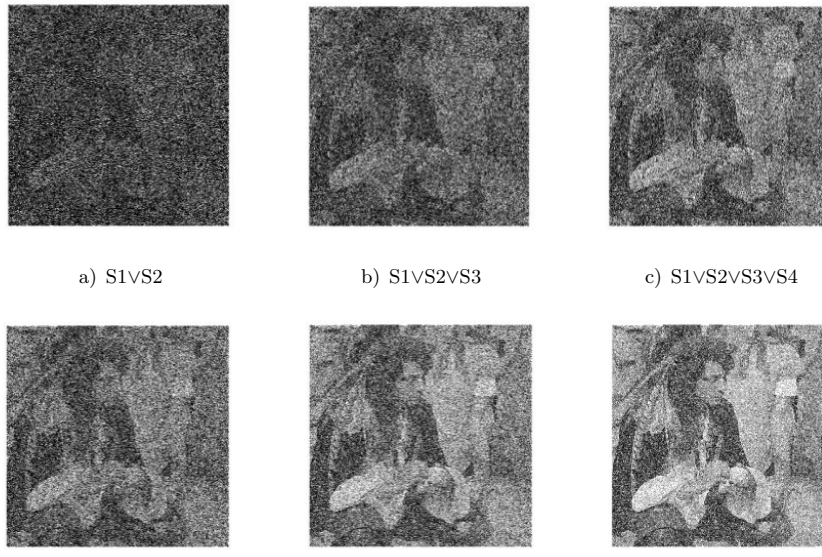
The grayscale test image size of 256 × 256 pixels is used and it has produced 6 shares in PVSSM as an example (S1, S2, S3, S4, S5, S6). The grayscale test image is first converted with the Jarvis algorithm [30] into binary image in Figure 5 and it is shared by PVSSM.

a) Grayscale image



b) Binary image

Figure 5. Test image



a) S1∨S2 b) S1∨S2∨S3 c) S1∨S2∨S3∨S4

d) S1∨S2∨S4∨S5 e) S1∨S2∨S3∨S4∨S5 f) S1∨S2∨S3∨S4∨S5∨S6

Figure 6. The secret image gradually appears

As seen in Figure 6, the secret image becomes apparent while the shares are stacked one by one. The human vision system can detect the secret. Therefore, all the shares are not needed to restore the secret image. Table 1 shows the similarity ratio of the images in Figure 6 using PSNR (peak to noise signal ratio) and SSIM (structural similarity index). They have been seen to be similar both visually and mathematically.

Images	**a)**	**b)**	**c)**	**d)**	**e)**	**f)**
PSNR	52.3784	53.3662	54.5234	54.3006	55.9546	57.7802
SSIM	0.9868	0.9915	0.9944	0.9940	0.9958	0.9961

Table 1. PSNR and SSIM values

4 THE PROPOSED METHOD

Although PVSSM determines the order of importance among the shares, when the shares with the higher priority are stacked, the secret image appears visually in Figure 6. It also proves the similarities by using PSNR and SSIM in Table 1. In order to overcome this problem of PVSSM, PVSSM and 2D-LASM based image encryption are used together. The proposed method is called Chaotic Encryption-

based PVSSM and we have explained how this method is applied to color images.

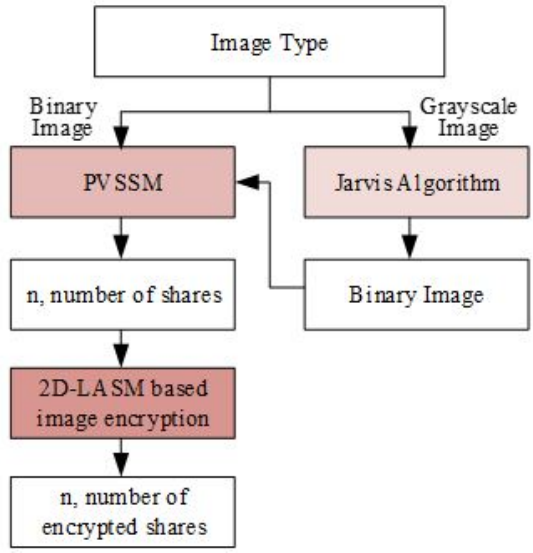


Figure 7. Chaotic Encryption-based PVSSM flow diagram for grayscale images

Firstly, the diagram of the Chaotic Encryption-based PVSSM for grayscale images is shown in Figure 7. In Figure 7, if the secret image is binary, PVSMM is applied to the secret image. n shares are obtained. Then, these n shares are encrypted by 2D-LASM based image encryption. If the secret image is grayscale, it is transformed into binary image by Jarvis algorithm. After that, this binary image is shared by PVSSM. Finally, n shares are encrypted by 2D-LASM based image encryption. Therefore, even if n encrypted shares are captured and stacked, no information about the secret image can be revealed.

In decryption process, firstly n encrypted shares are decrypted by 2D-LASM based image encryption. Then n shares are stacked and the secret image is restored.

The diagram of the Chaotic Encryption-based PVSSM for color images is shown in Figure 8. In Chaotic Encryption-based PVSSM for color images, the color secret image is first separated into RGB channels. After, RGB channels are transformed into binary images by the Jarvis algorithm. Then PVSSM is applied to binary images of RGB channel. n shares of R channel, n shares of G channel and n shares of B channel are obtained. After that, 2D-LASM based image encryption is applied to each channel shares. Finally, $3n$ encrypted shares are obtained. Therefore, no information is revealed from the shares.

In decryption process for color image, the shares are first decrypted with 2D-LASM based image encryption. Then the shares are stacked for each color channel,

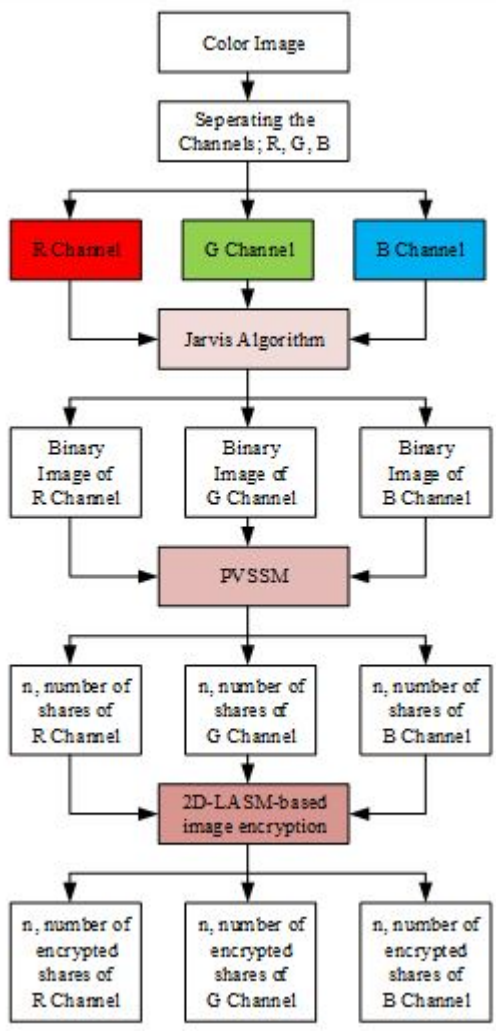


Figure 8. Chaotic encryption-based PVSSM flow diagram for color images

and the RGB channels are merged. Finally, the pixel values of 1 are changed into 255 to obtain the original color image in Table 2. In this way, 8 colors are obtained. The secret color image is restored.

This work is implemented with the MATLAB 2014b program on the AMD A10-4600M 2.30 GHz 8 GB computer. This method is applied to color Lena image size of 256×256. The color Lena image is divided into RGB channels in Figure 9. Then Jarvis algorithm is used and the RGB channels are converted into binary images in Figure 10.

The Resulting Pixel Values	**New Pixel Values of Color Images**	**The Obtained Color**
$(0,0,0)$	$(0,0,0)$	Black
$(0,0,1)$	$(0,0,255)$	Blue
$(0,1,0)$	$(0,255,0)$	Green
$(0,1,1)$	$(0,255,255)$	Cyan
$(1,0,0)$	$(255,0,0)$	Red
$(1,0,1)$	$(255,0,255)$	Magenta
$(1,1,0)$	$(255,255,0)$	Yellow
$(1,1,1)$	$(255,255,255)$	White

Table 2. Restored color

a) Secret image b) R channel c) G channel d) B channel

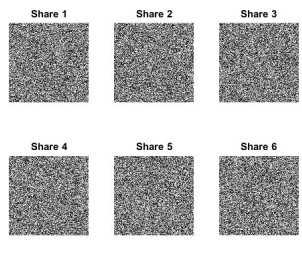
Figure 9. Color Lena image

PVSSM and 2D-LASM based image encryption is applied to the binary RGB channels respectively. 6 shares are produced as example. Figure 11 shows each of the encrypted shares and their histograms. In Figure 11, Chaotic Encryption-based PVSSM for color images is successfully applied. The encrypted shares of the histograms show a balanced distribution. Figures 11 a), c), and e) show the chaotic encrypted PVSSM implementation for all R, G and B channels, respectively. Figures 11 b), d), and f) represent histograms of the encrypted images for all R, G and B channels, respectively. The x-axis of these histograms shows the pixel values (0–255), and the y-axis shows the number of pixels. Thus, it will be difficult to obtain information with statistical methods [16]. The restored images are shown

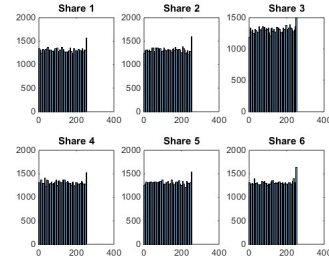
a) R channel b) G channel c) B channel

Figure 10. Binary channels

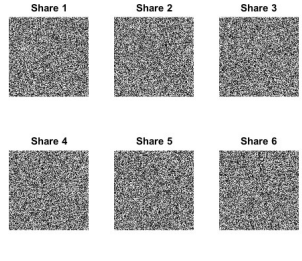
in Figure 12. Also PSNR and SSIM values of R, G, and B channels of color Lena image are shown in Table 3.



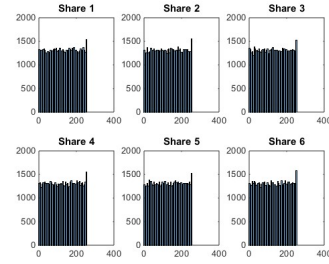
a) Encrypted R channel



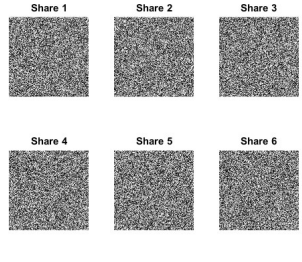
b) Histograms of Figure a)



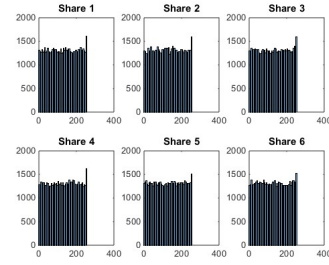
c) Encrypted G channel



d) Histograms of Figure c)



e) Encrypted B channel

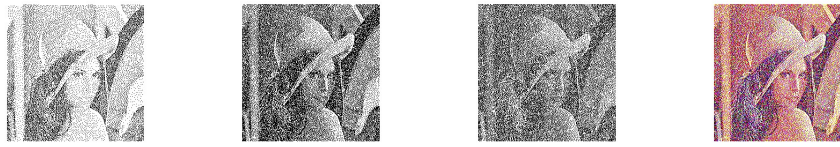


f) Histograms of Figure e)

Figure 11. Chaotic Encryption-based PVSSM

5 EXPERIMENTAL RESULTS

In this section, we analyze the proposed method with some tests including histogram analysis, data loss attack, salt-pepper noise attack, differential attack, chi-square analysis and correlation analysis. NCPR, UACI, PSNR, SSIM and CQM



a) R channel b) G channel c) B channel d) Secret image

Figure 12. Restored images

	R Channel	G Channel	B Channel	Average
PSNR	60.5639	57.3671	57.5363	58.4891
SSIM	0.9983	0.9955	0.9958	0.9965

Table 3. PSNR and SSIM values of channels of color Lena image

are used for measurement. Experimental images are used from the USC-SIPI image database.

5.1 Histogram Analysis

The histograms of the encrypted shares are shown in Figures 11 b), d), and f). These histograms show a balanced distribution, so it is difficult to get information from the shares [16]. In addition, showing a balanced distribution, this will reduce the possibility of statistic attacks.

5.2 Data Loss Attack

Data loss attack means that some parts of the share lose their real value by adding noise to them. In this section, grayscale Lena image and color Lena image are used. Both images are encrypted with Chaotic Encryption-based PVSSM with 6 shares. Then data loss attacks of various types take place. Each encrypted share is attacked on the same region and the same noise ratio. Finally, the encrypted shares are decrypted.

The grayscale secret image and restored image is shown in Figure 13. Data loss attack is implemented to all shares. Only first share is shown for grayscale image in Figure 14 and only R channel share is shown for color image in Figure 15.

5.3 Salt-Pepper Noise Attack

In this section, grayscale Lena image and color Lena image are encrypted and then salt-pepper noise with different ratio is added to all shares. Finally, the encrypted shares are decrypted. Simulation results are shown in Figure 16.

a) Lena image b) Binary image of Figure a) c) Restored image

Figure 13. Grayscale test image

5.4 Differential Attack

NPCR (Number of pixels change rate) and UACI (Unified average changing intensity) metrics can measure the number of pixel changing rate with respect to differential attacks [31]. For secret image, randomly change one bit of a pixel and obtaining another secret image. NPCR and UACI are represented as Equations (2), (3) and (4), respectively [21]:

$$NPCR(C_1, C_2) = \sum_{i=1}^{M} \sum_{j=1}^{N} \frac{D(i,j)}{L} \times 100\,\%, \tag{2}$$

$$UACI(C_1, C_2) = \sum_{i=1}^{M} \sum_{j=1}^{N} \left(\frac{|(C_1(i,j) - (C_2(i,j)|}{T \times L} \right) \times 100\,\%, \tag{3}$$

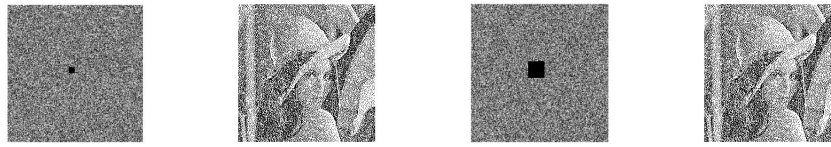
$$D(i,j) = \begin{cases} 0, & \text{if } (C_1(i,j) = (C_2(i,j), \\ 1, & \text{if } (C_1(i,j) \neq (C_2(i,j) \end{cases} \tag{4}$$

where C_1 and C_2 are encrypted images, M and N denote the size of images, i and j denote the pixels, T is the total number of pixels in the encrypted image, L is the largest allowed pixel value in the images and D is the bipolar array.

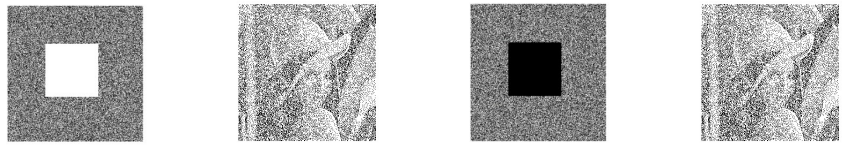
Experimental Image	**NCPR**	**UACI**
Lena Image	0.9963	0.3347
Barbara Image	0.9963	0.3346
Boat Image	0.9961	0.3346
Cameraman Image	0.9962	0.3342
Elanie Image	0.9961	0.3347
Peppers Image	0.9960	0.3344

Table 4. NCPR and UACI values

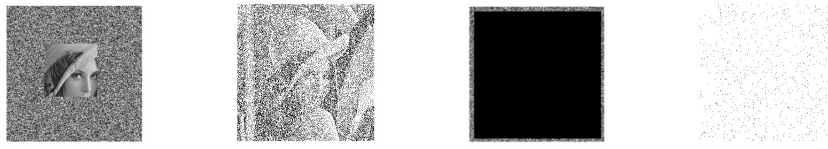
Table 4 shows NPCR and UACI values with respect to same secret key. When NPCR is equal to 0, it implies that all pixels remain the same between images.



a) 10 × 10 black square attack b) 10 × 10 black square result c) 30 × 30 black square attack d) 30 × 30 black square result



e) 100 × 100 white square attack f) 100×100 white square result g) 100×100 black square attack h) 100×100 black square result



i) 100 × 100 part of image attack j) 100×100 part of image attack result k) 90 % data loss attack l) 90 % data loss result

Figure 14. Data loss attack results for grayscale image

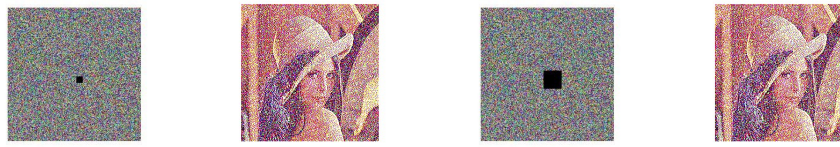
When NPCR is equal to 1, it implies that all pixel values are changed [31]. The ideal value of NCPR is 0.9961 and the ideal value of UACI is 0.3346 [32]. Table 4 shows that NPCR and UACI values are over 0.9960 and 0.3342, respectively, so the proposed method has good ability to resist differential attacks.

5.5 Chi-Square Analysis

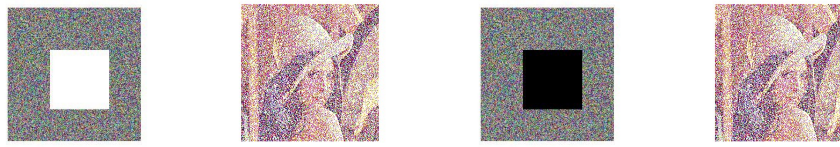
The chi-square parameter X^2 is defined as Equation (5):

$$X^2 = \sum_{i=1}^{256} \frac{(O_i - E_i)^2}{E_i} \tag{5}$$

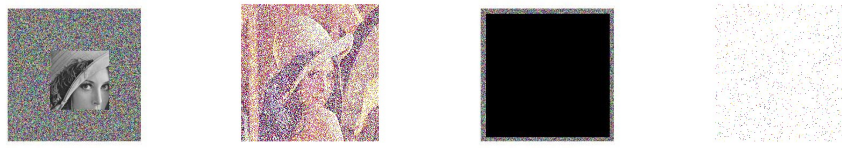
where i is the number of gray values, O_i and E_i are observed and expected occurrence of each gray value (0 to 255), respectively. In this experiment, we obtained 6 encrypted shares as an example, so it is obtained chi-square analysis between test image and its encrypted shares one by one. Then, the average is calculated. The



a) 10 × 10 black square attack b) 10 × 10 black square result c) 30×30 black square attack d) 30 × 30 black square result



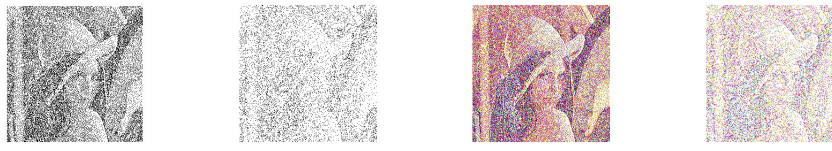
e) 100 × 100 white square attack f) 100 × 100 white square result g) 100 × 100 black square attack h) 100 × 100 black square result



i) 100 × 100 part of image attack j) 100 × 100 part of image attack result k) 90 % data loss attack l) 90 % data loss result

Figure 15. Data loss attack results for color image

values of chi-square for images under study are listed in Table 5. Table 5 shows that the histograms of the encrypted images are uniform.



a) 1 % salt-pepper noise for grayscale image b) 5 % salt-pepper noise for grayscale image c) 1 % salt-pepper noise for color image d) 5 % salt-pepper noise for color image

Figure 16. Salt-pepper noise attack result

Experimental Image	Chi-Square Value
Lena Image	255
Barbara Image	255
Boat Image	128
Cameraman Image	255
Elanie Image	255
Peppers Image	255

Table 5. Chi-square values

5.6 Correlation Analysis

The correlation coefficient $R_{x,y}$ between two grayscale adjacent pixels x and y are defined as Equation (6):

$$R_{x,y} = \frac{cov(x,y)}{\sqrt{D(x)D(y)}} \tag{6}$$

where $cov(x,y) = \frac{1}{T}\sum_{i=1}^{T}(x_i - E(x))(y_i - E(y))$, $E(x) = \frac{1}{T}\sum_{i=1}^{T} x_i$, $D(x) = \frac{1}{T}\sum_{i=1}^{T}(x_i - E(x))^2$ and T is the total number of pixels selected from the encrypted image.

In this experiment, the grayscale Lena image is used and 6 encrypted shares are obtained. 2 000 pairs of adjacent pixels are randomly selected. The horizontal, vertical and diagonal correlation coefficients of Lena image and original Lena image are shown in Table 6.

	1	2	3	4	5	6	Avg.	Lena
Horizontal	0.1356	0.1303	0.0821	0.0846	0.1210	0.1312	0.1141	0.9269
Vertical	0.1101	0.1007	0.1008	0.1317	0.0923	0.0775	0.1021	0.9699
Diagonal	0.1068	0.1089	0.1078	0.0815	0.1340	0.1013	0.1067	0.9129

Table 6. Correlation coefficients of encrypted shares of Lena image

As can be seen in Table 6, a small coefficient value means a weak correlation between two adjacent pairs [17]. There are no detectable correlations between the encypted share images and Lena image. Thus, the proposed method has good ability to resist statistical attacks.

5.7 Test Results

PSNR is a metric that measures the similarity between two images. PSNR can represent the image noise removal effects [33]. PSNR is represented as Equation (7):

$$PSNR = 10\log_{10}\frac{255^2}{\frac{1}{n\times m}\sum_{i=0}^{n-1}\sum_{j=0}^{m-1}(x_{ij} - x'_{ij})^2} \tag{7}$$

where $n \times m$ denotes the size of the secret image, x_{ij} and (x'_{ij}) denote the pixel of secret image and restored image, respectively.

SSIM is the other metric of the similarity. If SSIM is equal to 1, two images are the same [34]. SSIM is of the following form [35]:

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + C1) + (2\sigma_{xy} + C2)}{(\mu_x^2 + \mu_y^2 + C1) + (\sigma_x^2 + \sigma_y^2 + C2)} \tag{8}$$

where x and y are the secret image and the restored image, μ_x and μ_y denote the mean values, σ_{xy} denotes the covariance, σ_x and σ_y denote the variance of the secret image and restored image, respectively. $C1$ and $C2$ are the constants that inhibits division by 0.

CQM is the measurement of color image similarity [36]. In this method, first RGB channels are transformed to YUV channels:

$$Y = 0.257R + 0.504G + 0.098B + 16, \tag{9}$$

$$U = -0.148R - 0.291G + 0.439B + 128, \tag{10}$$

$$V = 0.439R - 0.368G - 0.071B + 128. \tag{11}$$

Then, C_W and R_W are calculated as $C_W = 0.0551$ and $R_W = 0.9449$. C_W is the weight on the human perception of the cones and R_W is the weight on the human perception of the rods.

Finally, CQM is calculated as Equation (12):

$$CQM = (PSNR_Y \times R_W) + \left(\frac{PSNR_U + PSNR_V}{2}\right) \times C_W. \tag{12}$$

Some test images are encrypted and their PSNR, SSIM and CQM values are calculated and shown in Table 7.

Experimental Image	**PSNR**	**SSIM**	**Experimental Image**	**CQM**
Binary Lena Image	58.3701	0.9958	Color Pepper Image	20.6227
Grayscale Lena Image	58.1951	0.9966	Color Lena Image	22.1913
Grayscale Barbara Image	57.8817	0.9962	Color House Image	22.4517
R Channel of Pepper Image	58.9144	0.9973	Color Jet plane Image	25.8311
G Channel of Pepper Image	57.7796	0.9958	Color Baboon Image	20.5208
B Channel of Pepper Image	56.5663	0.9941	–	–
Grayscale Building Image	59.8442	0.9978	–	–

Table 7. Test results of Chaotic Encryption-based PVSSM

As can be seen in Table 7, PSNR, SSIM and CQM values show that there is a similarity between the original secret image and the restored images which are both grayscale and color images. In addition, SSIM values are close to 1. Also the

proposed method has not only worked with square image but also rectangular image because a building image with size of (232 × 311) is a rectangular.

Grayscale	PSNR	SSIM	Color	CQM
(10 × 10) black square	75.7988	1.000	(10 x 10) black square	25.4017
(30 × 30) black square	67.4142	0.9997	(30 x 30) black square	25.3883
(100 × 100) white square	57.6786	0.9959	(100 x 100) white square	25.3587
(100 × 100) black square	57.6786	0.9959	(100 x 100) black square	25.3587
(100 × 100) part of image	57.6762	0.9959	(100 x 100) part of image	25.3543
90 % data loss	52.0986	0.9728	90 % data loss	24.9894
1 % salt-pepper noise	58.7118	0.9971	1 % salt-pepper noise	25.1583
5 % salt-pepper noise	53.5124	0.9834	5 % salt-pepper noise	25.0015

Table 8. Attack type results

As can be seen in Table 8, when the same attack type rate increases, PSNR, SSIM and CQM values decrease. It is understood that the similarity ratio decreases as the attack rate increases. According to PSNR, SSIM and CQM values, the similarity ratio of the images is still high despite these attacks. SSIM values are also close to 1. In only 90 % data loss, the image is visually lost in Figures 14 and 15. As a result, it has been seen that the system is resistant to most attacks.

6 DISCUSSION

When experimental PSNR and SSIM values are investigated, high PSNR values represent the success of the proposed method. SSIM shows the proposed method's quality measure of one of the images being compared with original images. Tables 9 and 10 compare the proposed method with other methods.

Method	Image Type	PSNR
Wang et al. proposed method 1 [11]	Grayscale	51.13
Thien and Lin [37]	Grayscale	37.37
Yang et al. scheme 1 [38]	Grayscale	50.53
Yang et al. scheme 2 [38]	Grayscale	48.88
Pandey et al. [39]	Grayscale	57.6337
Goswami et al. [40]	Grayscale	37.24
Proposed Method	Grayscale	58.1951

Table 9. Encryption comparisons 1

In Table 9, Wang et al. [11] get PSNR value of 51.13 (proposed method 1), Thien and Lin [37] get PSNR value of 37.37, Yang et al. [38] get PSNR values of 50.53 and 48.88, Pandey et al. [39] get PSNR value of 57.6337 and Goswami et al. [40] get PSNR value of 37.24. A higher rate of PSNR value (58.1951) is obtained in the proposed method.

As can be seen in Table 10, Goswami et al. [40] get SSIM value of 0.9960 and, Weir et al. [41] get SSIM value of 0.9147. A higher rate of SSIM value of 0.9966 is obtained with the proposed method. SaiCandana and Anuradha [42] get SSIM values of 0.98 and 0.99 (color) and Huang et al. [43] get SSIM values of 0.9879 and 0.9925 (color). A higher rate of SSIM value (0.9965 – color) is obtained in the proposed method.

Method	**Image Type**	**SSIM**
Goswami et al. [40]	Grayscale	0.9960
Weir et al. [41]	Grayscale	0.9147
SaiCandana et al. [42] example 1	Color	0.98
SaiCandana et al. [42] example 2	Color	0.99
Huang et al. [43] example 1	Color	0.9879
Huang et al. [43] example 2	Color	0.9925
Proposed Method	Grayscale	0.9966
Proposed Method	Color	0.9965

Table 10. Encryption comparisons 2

Gorji et al. [44] get PSNR values of 53.6654 (1 % salt-pepper), 47.8638 (5 % salt-pepper) and 56.6781 ((10×10) data loss). A higher rate of PSNR values 58.7118 (1 % salt-pepper), 53.5124 (5 % salt-pepper) and 75.7988 6781 ((10×10) data loss) are obtained in the proposed method (see Table 11).

Method	**Attack Type**	**Image Type**	**SSIM**
Gorji et al. [44]	1 % salt-pepper	Grayscale	53.6654
Proposed method	1 % salt-pepper	Grayscale	58.7118
Gorji et al. [44]	5 % salt-pepper	Grayscale	47.8638
Proposed method	5 % salt-pepper	Grayscale	53.5124
Gorji et al. [44]	(10×10) data loss	Grayscale	56.6781
Proposed method	(10×10) data loss	Grayscale	75.7988

Table 11. Attack comparisons 1

In Lena image, Xu et al. [45] and Ye et al. [19] get NCPR values of 0.9962 and 0.9955, respectively. A higher rate of NCPR value 0.9963 is obtained in the proposed method. Xu et al. [45] and Ye et al. [19] get UACI values of 0.3351 and 0.3339, respectively. In the proposed method, UACI value 0.3347 is obtained.

In Boat image, Hua et al. [17] and Ye et al. [19] get NCPR values of 0.9963 and 0.9962, respectively. A lower rate of NCPR value 0.9961 is obtained in the proposed method. Hua et al. [17] and Ye et al. [19] get UACI values of 0.3353 and 0.3347, respectively. A lower rate of UACI value 0.3346 is obtained in the proposed method.

In Elanie image, Hua et al. [17] and Hua et al. [21] get NCPR values of 0.9962 and 0.9961, respectively. In the proposed method, UACI value 0.9961 is obtained. Hua et al. [17] and Hua et al. [21] get UACI values of 0.3342 and 0.3355, respectively. In the proposed method, UACI value 0.3347 is obtained.

Method	Image	NCPR	UACI
Xu et al. [45]	Lena	0.9962	0.3351
Ye et al. [19]	Lena	0.9955	0.3339
Proposed method	Lena	0.9963	0.3347
Hua et al. [17]	Boat	0.9962	0.3347
Ye et al. [19]	Boat	0.9963	0.3353
Proposed method	Boat	0.9961	0.3346
Hua et al. [17]	Elanie	0.9962	0.3342
Hua et al. [21]	Elanie	0.9961	0.3355
Proposed method	Elanie	0.9961	0.3347
Ye et al. [19]	Cameraman	0.9960	0.3353
Proposed method	Cameraman	0.9962	0.3342

Table 12. Attack comparisons 2

In Cameraman image, Ye et al. [19] get NCPR value of 0.9960 and UACI value of 0.3353. In the proposed method, NCPR value 0.9962 and UACI value 0.3342 are obtained (see Table 12).

The encrypted shares are tested by using many methods of histogram analysis, data loss attack and salt-pepper noise attack. These tests are applied to both grayscale and color images. The histograms of the encrypted shares are balanced and unbiased causing the statistical methods to fail in information extraction. The measurement results of data loss and salt-pepper noise attacks are obtained with PSNR and SSIM for binary and grayscale images whereas CQM is used for color images. When image resolutions are examined, the worst result is obtained with 90 % loss compared to (10×10), (30×30) and (100×100) data losses attacks. A better image resolution is obtained in 1 % salt-pepper noise attacks compared to 5 % salt-pepper noise attacks.

Moreover, the measurement results of differential attacks are obtained with NCPR and UACI. There is no big difference between these comparisons in Table 12. Chi-square analysis is also applied. The low values of chi-square confirm that the proposed method offers fairly high encryption effect [46].

Finally, all comparisons show that the proposed method has better PSNR, SSIM values and a good NPCR and UACI values. Thus it provides a better security.

7 CONCLUSION

In PVSSM, when the higher privileged shares are superimposed, the secret image is restored. Therefore, there is no need for all share images to reveal the secret image.

In this work, we have presented a solution to the security problem of PVSSM. We combined PVSSM with 2D-LASM based image encryption. This method was called Chaotic Encryption-based PVSSM. There are some advantages and novelty of the proposed method:

1. One of the VC and chaotic encryption methods are employed together.
2. Unlike traditional VC, this method has no pixel expansion.
3. When grayscale and color images are encrypted, Jarvis algorithm is applied.
4. Chaotic Encryption-based PVSSM is suitable for binary, grayscale, and color images.
5. For color images, CQM metric is used.

Finally, according to the test results, the proposed method is resistant against various attacks. Moreover, a better image quality has been obtained with the proposed method.

Since PVSSM is a lossy-method, certain loss may be possible while decrypting the encrypted image. Future works may ensure better image quality and compare CQM values for color images.

REFERENCES

[1] Hua, Z.—Zhou, Y.—Pun, C.-M.—Chen, C. L. P.: Image Encryption Using 2D Logistic-Sine Chaotic Map. IEEE International Conference on Systems, Man and Cybernetics, 2014, pp. 3229–3234, doi: 10.1109/smc.2014.6974425.

[2] Kapoor, D.—Keshari, S.—Gaur, S. K.: An Overview of Visual Cryptography. International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 4, 2014, No. 2, pp. 103–110.

[3] Thien, C.-C.—Lin, J.-C.: Secret Image Sharing. Computers and Graphics, Vol. 26, 2002, No. 5, pp. 765–770, doi: 10.1016/s0097-8493(02)00131-0.

[4] Naor, M.—Shamir, A.: Visual Cryptography. In: De Santis, A. (Ed.): Advances in Cryptology – EUROCRYPT '94. Springer, Berlin, Heidelberg, Lecture Notes in Computer Science, Vol. 950, 1995, pp. 1–12, doi: 10.1007/bfb0053419.

[5] Pandey, A.—Som, S.: Applications and Usage of Visual Cryptography: A Review. 5th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), 2016, pp. 375–381, doi: 10.1109/icrito.2016.7784984.

[6] Wei, K.-J.—Lee, J.-S.—Chen, S.-J.: Enhancing the Security of Credit Card Transaction Based on Visual DSC. KSII Transactions on Internet and Information Systems, Vol. 9, 2015, No. 3, pp. 1231–1245, doi: 10.3837/tiis.2015.03.022.

[7] Hou, Y.-C.: Visual Cryptography for Color Images. Pattern Recogniton, Vol. 36, 2015, No. 7, pp. 1619–1629, doi: 10.1016/s0031-3203(02)00258-3.

[8] Fang, W.-P.—Lin, J.-C.: Progressive Viewing and Sharing of Sensitive Images. Pattern Recognition and Image Analysis, Vol. 16, 2006, No. 4, pp. 632–636, doi: 10.1134/s1054661806040080.

[9] Jin, D.—Yan, W.-Q.—Kankanhalli, M. S.: Progressive Color Visual Cryptography. Journal of Electronic Imaging, Vol. 14, 2005, No. 3, Art. No. 033019, doi: 10.1117/1.1993625.

[10] Fang, W.-P.: Friendly Progressive Visual Secret Sharing. Pattern Recognition, Vol. 41, 2008, No. 4, pp. 1410–1414, doi: 10.1016/j.patcog.2007.09.004.

[11] Wang, R.-Z.—Chien, Y.-F.—Lin, Y.-Y.: Scalable User-Friendly Image Sharing. Journal of Visual Communication and Image Representation, Vol. 21, 2010, No. 7, pp. 751–761, doi: 10.1016/j.jvcir.2010.06.001.

[12] Chen, C.-C.—Chen, C.-C.—Lin, Y.-C.: Weighted Modulated Secret Image Sharing Method. Journal of Electronic Imaging, Vol. 18, 2009, No. 4, Art. No. 043011, doi: 10.1117/1.3268362.

[13] Lin, S.-J.—Chen, L. S.-T.—Lin, J.-C.: Fast-Weighted Secret Image Sharing. Optical Engineering, Vol. 48, 2009, No. 7, Art. No. 077008, doi: 10.1117/1.3168644.

[14] Li, P.—Yang, C.-N.—Wu, C.-C.—Kong, Q.—Ma, Y.: Essential Secret Image Sharing Scheme with Different Importance of Shadows. Journal of Visual Communication and Image Representation, Vol. 24, 2013, No. 7, pp. 1106–1114, doi: 10.1016/j.jvcir.2013.07.005.

[15] Hou, Y.-C.—Quan, Z.-Y.—Tsai, C.-F.: A Privilege-Based Visual Secret Sharing Model. Journal of Visual Communication and Image Representation, Vol. 33, 2015, pp. 358–367, doi: 10.1016/j.jvcir.2015.10.005.

[16] Mao, Y.—Chen, G.: Chaos-Based Image Encryption. Chapter 8. In: Bayro Corrochano, E. (Ed.): Handbook of Geometric Computing. Springer, 2005, pp. 231–265.

[17] Hua, Z.—Zhou, Y.: Image Encryption Using 2D Logistic-Adjusted-Sine Map. Information Sciences, Vol. 339, 2016, pp. 237–253, doi: 10.1016/j.ins.2016.01.017.

[18] Alvarez, G.—Li, S.: Cryptanalyzing a Nonlinear Chaotic Algorithm (NCA) for Image Encryption. Communications in Nonlinear Science and Numerical Simulations, Vol. 14, 2009, No. 11, pp. 3734–3749, doi: 10.1016/j.cnsns.2009.02.033.

[19] Ye, G.—Zhao, H.—Chai, H.: Chaotic Image Encryption Algorithm Using Wave-Line Permutation and Block Diffusion. Nonlinear Dynamics, Vol. 83, 2016, No. 4, pp. 2067–2077, doi: 10.1007/s11071-015-2465-7.

[20] Arroyo, D.—Rhouma, R.—Alvarez, G.—Li, S.—Fernandez, V.: On the Security of a New Image Encryption Scheme Based on Chaotic Map Lattices. Chaos: An Interdisciplinary Journal of Nonlinear Science, Vol. 18, 2008, No. 3, Art. No. 033112, doi: 10.1063/1.2959102.

[21] Hua, Z.—Zhou, Y.—Pun, C. M.—Chen, C. L. P.: 2D Sine Logistic Modulation Map for Image Encryption. Information Sciences, Vol. 297, 2015, pp. 80–94, doi: 10.1016/j.ins.2014.11.018.

[22] Tang, Y.—Guan, X.: Parameter Estimation of Chaotic System with Time-Delay: A Differential Evolution Approach. Chaos, Solitons and Fractals, Vol. 42, 2009, No. 5, pp. 3132–3139, doi: 10.1016/j.chaos.2009.04.045.

[23] Wu, Y.—Noonan, J. P.—Yang, G.—Jin, H.: Image Encryption Using the Two-Dimensional Logistic Chaotic Map. Journal of Electronic Imaging, Vol. 21, 2012, No. 1, Art. No. 013014, doi: 10.1117/1.jei.21.1.013014.

[24] Ye, G.: Image Scrambling Encryption Algorithm of Pixel Bit Based on Chaos Map. Pattern Recognition Letters, Vol. 31, 2010, No. 5, pp. 347–354, doi: 10.1016/j.patrec.2009.11.008.

[25] Liu, F.—Wu, C.: Embedded Extended Visual Cryptography Schemes. IEEE Transactions on Information Forensics and Security, Vol. 6, 2011, No. 2, pp. 307–322, doi: 10.1109/tifs.2011.2116782.

[26] Chang, C.-C.—Hsieh, Y.-P.—Liao, C.-C.: A Visual Secret Sharing Scheme for Progressively Restoring Secrets. Journal of Electronic Science and Technology, Vol. 9, 2011, No. 4, pp. 325–331.

[27] Soman, N.— Baby, S.: XOR-Based Visual Cryptography. International Journal on Cybernetics and Informatics (IJCI), Vol. 5, 2016, No. 2, pp. 253–264, doi: 10.5121/ijci.2016.5228.

[28] Padhmavathi B.—Kumar, P. N.: A Novel Mathematical Model for (t, n)-Threshold Visual Cryptography Scheme. International Journal of Computer Trends and Technology (IJCTT), Vol. 12, 2014, No. 3, pp. 126–129, doi: 10.14445/22312803/ijctt-v12p125.

[29] Hou, Y.-C.—Quan, Z.-Y.: Progressive Visual Cryptography with Unexpanded Shares. IEEE Transactions on Circuits and Systems for Video Technology, Vol. 21, 2011, No. 11, pp. 1760–1764, doi: 10.1109/tcsvt.2011.2106291.

[30] Nikate, P. M.—Mujawar, I. I.: Performance Evaluation of Floyd Steinberg Halftoning and Jarvis Halftoning Algorithms in Visual Cryptography. International Journal of Innovations in Engineering and Technology, Vol. 5, 2015, No. 1, pp. 336–342.

[31] Wu, Y.—Noonan, J. P.—Agaian, S.: NPCR and UACI Randomness Tests for Image Encryption. Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT), April Edition, 2011, pp. 31–38.

[32] Borujeni, S. E.—Eshghi, M.: Chaotic Image Encryption Design Using Tompkins-Paige Algorithm. Mathematical Problems in Engineering, Vol. 2009, 2009, Art. No. 762652, 22 pp., doi: 10.1155/2009/762652.

[33] Yu, J.—Tan, L.—Zhou, S.—Wang, L.—Wang, C.: Image Denoising Based on Adaptive Fractional Order Anisotropic Diffusion. KSII Transactions on Internet and Information Systems, Vol. 11, 2017, No. 1, pp. 436–450, doi: 10.3837/tiis.2017.01.023.

[34] Kocak, C.: CLSM: Couple Layered Security Model A High-Capacity Data Hiding Scheme Using with Steganography. Image Analysis and Stereology, Vol. 36, 2017, No. 1, pp. 15–23, doi: 10.5566/ias.1482.

[35] Wang, Z.—Bovik, A. C.—Sheikh, H. R.—Simoncelli, E. P.: Image Quality Assessment: From Error Visibility to Structural Similarity. IEEE Transactions on Image Processing, Vol. 13, 2004, No. 4, pp. 600–612, doi: 10.1109/tip.2003.819861.

[36] Yalman, Y.—Ertürk, İ.: A New Color Image Quality Measure Based on YUV Transformation and PSNR for Human Vision System. Turkish Journal of Electrical Engineering and Computer Sciences, Vol. 21, 2013, No. 2, pp. 603–612, doi: 10.3906/elk-1111-11.

[37] Thien, C.-C.—Lin, J.-C.: An Image Sharing Method with User-Friendly Shadow Images. IEEE Transactions on Circuits and Systems for Video Technology, Vol. 13, 2003, No. 12, pp. 1161–1169, doi: 10.1109/tcsvt.2003.819176.

[38] Yang, C.-N.—Yu, K.-H.—Lukac, R.: User-Friendly Image Sharing Using Polynomials with Different Primes. International Journal of Imaging Systems and Technology, Vol. 17, 2007, No. 1, pp. 40–47, doi: 10.1002/ima.20096.

[39] Pandey, D.—Rawat, U. S.—Kumar, A.: Robust Progressive Block Based Visual Cryptography with Chaotic Map. Journal of Discrete Mathematical Sciences and Cryptography, Vol. 19, 2016, No. 5–6, pp. 1025–1040, doi: 10.1080/09720529.2015.1132040.

[40] Goswami, A.—Mukherjee, R.—Ghoshal, N.: Chaotic Visual Cryptography Based Digitized Document Authentication. Wireless Personal Communications, Vol. 96, 2017, No. 3, pp. 3585–3605, doi: 10.1007/s11277-017-4088-4.

[41] Weir, J.—Yan, W.—Kankanhalli, M. S.: Image Hatching for Visual Cryptography. ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM) – Special Issue on Multimedia Security, Vol. 8, 2012, No. 2S, Art. No. 32, 15 pp., doi: 10.1145/2344436.2344438.

[42] SaiChandana, B.—Anuradha, S.: A New Visual Cryptography Scheme for Color Images. International Journal of Engineering Science and Technology, Vol. 2, 2010, No. 6, pp. 1997–2000.

[43] Huang, H.-C.—Lu, Y.-Y.—Liu, J.: Ownership Protection for Progressive Image Transmission with Reversible Data Hiding and Visual Secret Sharing. Optik, Vol. 127, 2016, No. 15, pp. 5950–5960, doi: 10.1016/j.ijleo.2016.04.011.

[44] Gorji, R. B.—Shirvani, M. H.—Mooziraji, F. R.: A New Image Encryption Method Using Chaotic Map. Journal of Multidisciplinary Engineering Science and Technology (JMEST), Vol. 2, 2015, No. 2, pp. 251–256.

[45] Xu, L.—Li, Z.—Li, J.—Hua, W.: A Novel Bit-Level Image Encryption Algorithm Based on Chaotic Maps. Optics and Lasers in Engineering, Vol. 78, 2016, pp. 17–25, doi: 10.1016/j.optlaseng.2015.09.007.

[46] Ahmad, M.—Alsharari, H. D.—Nizam, M.: Security Improvement of an Image Encryption Based on mPixel-Chaotic-Shuffle and Pixel-Chaotic-Diffusion. European Journal of Scientific Research, Vol. 98, 2013, No. 3, 14 pp.

Aytekin Yildizhan received his B.Sc. degree in computer engineering from the Izmir Institute of Technology, Izmir, Turkey in 2008. He received his M.Sc. degree in computer engineering from Gazi University, Ankara, Turkey in 2013. He is a Ph.D. candidate in computer engineering at Hacettepe University, Ankara, Turkey. He currently works as an engineer first lieutenant in Turkish Armed Forces. He does research in cognitive science, visual secret sharing and visual cryptography.

Nurettin Topaloglu is Professor of the Computer Engineering Department at the Technology Faculty of Gazi University in Turkey. He received his B.Sc. in electronics, M.Sc. in electronics and computer education and Ph.D. in electric education. His research interests are computer architecture and organization, informatics technologies and information security. He has been involved in research areas in deep and machine learning. He developed the educational software Visual 6502 microprocessor simulator for teaching computer architecture. He is a writer of microprocessors and assembly language, and x86 microprocessor architecture and assembly language in Turkish.