

A Secret Image Sharing Based on Logistic-Chebyshev Chaotic Map and Chinese Remainder Theorem

Asmaa Hilmi, Soufiane Mezroui, Ahmed El Oualkadi

Abstract

Visual secret sharing (VSS) was introduced in order to solve information security issues. It is a modern cryptographic technique. It involves breaking up a secret image into n secured components known as shares. The secret image is recovered with utmost secrecy when all of these shares are lined up and piled together. A (3, 3)-secret image sharing scheme (SIS) is provided in this paper by fusing the Chinese Remainder Theorem (CRT) and the Logistic-Chebyshev map (LC). Sharing a confidential image created with CRT has various benefits, including lossless recovery, the lack of further encryption, and minimal recovery calculation overhead. Firstly, we build a chaotic sequence using an LC map. The secret value pixel for the secret image is permuted in order to fend off differential attackers. To encrypt the scrambled image, we apply our CRT technique to create three shares. Finally, the security analysis of our (3, 3)-SIS scheme is demonstrated and confirmed by some simulation results.

Keywords: Visual Cryptography, Logistic-Chebyshev map, Chinese Remainder Theorem, share.

MSC 2010: 68R10, 68Q25, 05C35, 05C05.

1 Introduction

Visual secret sharing (VSS) consists of decoding visually a secret image without involving any complex computations by superimposing the shares. Based on Naor and Shamir's method [1], a visual cryptographic scheme (VCS) is possible to encrypt an image into n shares that are secret. k or more shares should be used to rebuild the secret image.

No information can be extracted with less than k shares. The (k, n) -threshold scheme is one type of such strategy. The shares are printed on distinct transparency [2]. When they are transmitted after applying the encrypt and decrypt cryptographic techniques and then superimposed, the secret image should become visible. In addition to the definition of contrast proposed by Noar and Shamir, other researchers suggest various other definitions to improve contrast's quality [1], [3]–[6]. Ensuring a secure transmission of secret images is a challenging task in VSS. Developing an optimal encryption and decryption algorithm to tackle this issue is the main goal of several researches done on VSS, most of these studies try to use well-known algorithms such as RSA, BLOWFISH, AES, etc. For example, in [7], the authors have generated separate color matrices R_i , G_i , and B_i from the RGB colors. Then, the basic matrices, which represent the shares of the original image, have been created by dividing the values of each pixel in R_i , G_i , and B_i by 2. Once the shares are created, Advanced Encryption Standard (AES) algorithm is used to both encrypt and decrypt them separately. The proposed method of K. Shankar and P. Eswaran is used to generate multiple shares from the extracted pixel values of RGB. The use of ordinary colors is an easy way to define the colors available in the original image. After that, blocks are created from the image's shares [8], [9]. The Elliptical Curve Cryptography (ECC) method is used to encrypt the share blocks and to decrypt the encrypted blocks. However, these traditional encryption methods have enabled to meet the current image encryption requirements. Recently, the encryption algorithm of image has been considered. The two main approaches for encrypting images are diffusion and confusion, where diffusion modifies the value of pixels and confusion modifies their position. We will include a chaotic map into our secret image sharing because of its essential properties, such as sensitivity to beginning conditions and ergodicity, which have attracted the interest of cryptographers to create new system methods. In this paper, our secret image sharing scheme based on $(3, 3)$ -threshold cryptography is proposed. We generate three shares images using the Chinese Remainder Theorem (CRT); if only we have three shares, we can reconstruct the secret image; however, with fewer than three, we are unable to collect any useful information about the secret image.

The structure of this paper is as follows: Section 2 provides an analysis of the literature on image security; Section 3 contains a brief introduction of the related method used in this paper; in Section 4, the proposed method is presented, which includes the permutation phase, sharing phase, and reconstructing phase. The performance analysis and the experimental results are discussed in Section 5. Color image encryption is described in Section 6. Section 7 presents analysis and comparison. Section 8 concludes the paper.

2 Related work

Many authors have suggested different methods for image encryption and decryption using chaotic systems or CRT. In [10], the authors have proposed a threshold secret sharing scheme for digital images; the proposed method uses the Mignote [11] and Asmuth-bloom [12] solutions that were introduced in 1983. This scheme suggested in [10] is based on the CRT and divides a secret image into k shares so that a group with k shares can recover the secret image but a group with fewer shares cannot divulge any information about the hidden image. In [13], it is suggested to use a Secret Image Sharing (SIS) system that uses diminutive shadow images and is based on the CRT. Shadow images can be made to almost $1/k$ of the size of the original secret image. Auxiliary encryption is not required for this technique because random bits are added to binary representations of the CRT's random factors. In [14], a new technique is explained how to create a collection of n shared images from a set of n hidden images. The CRT and Boolean Exclusive-OR (XOR) operation are used in this method, which also introduces symmetric and modified masking coefficients. The goal is to overcome issues induced when an odd number of secret images is used. In [15], the authors used two chaotic systems: a cat map is used firstly for image pixels permutation, and the logistic map is used secondly for image pixels diffusion. M. L. Sahari et al. [16] presented a color image encryption, the secret key is connected with the plain image, and the 3D chaotic map creates the sequence in confusion and diffusion. In [17], the authors used the Chinese remainder theorem (CRT) with arithmetic compression coding to develop a secret image-sharing system. The piecewise linear map is utilized to create the compression

coding scheme, and the CRT is used to create the compression code sharing scheme. The overview of the related work revealed that most existing (k, n) schemes face the problem of if we have any k shares, we can reconstruct the secret image. Another problem raised is the difference in weight between the participants, because this can cause a problem of confidentiality. To overcome the above stated in terms of security, the work presented in this paper proposes a scheme named $(3, 3)$ -secret image sharing scheme (SIS); in other words, to rebuild a secret image, all n shares must be present; if even one share is missing, the hidden image cannot be restored. Our scheme is based on the Logistic-Chebyshev chaotic map and CRT theorem. It is a solution to improve the level of security by using an LC chaotic map to confuse the secret image and the CRT for encrypting the confused image. It is important to note that CRT is especially used to generate shares using a pure mathematical analysis which focuses on changing pixels' values. In our case, we use chaotic map to permute the position of pixel's image. Then we apply the CRT method to encrypt the scrambled image into three shares. Our results demonstrate that we obtain a high quality reconstructed secret image when all three decrypted shares are used. However, lower quality is produced when less than three shares are decrypted. That makes our technique robust and more secure.

3 Brief introduction to the related method

The Logistic-Chebyshev map is chaotic systems that can enough to design secure crypto-systems, it is a hybrid 1-D chaos map that combines two well-known chaotic systems in order to improve the discontinuous ranges of its original ones.

3.1 Logistic-Chebyshev chaotic map

The Logistic-Chebyshev map combines the two popular 1D chaotic systems, Chebyshev and the Logistic. It can be expressed as [18]

$$LC_{i+1} = (\alpha * LC_i(1 - LC_i) + \frac{(4 - \alpha)\cos(A * \arccos(LC_i))}{4}) \bmod 1, \quad (1)$$

where $\alpha \in (0, 4)$ is the control parameter and $LC_0 \in (0, 1)$ is the original value. The Chinese Remainder Theorem has been employed

vastly in cryptography. It is an old Chinese technique for resolving a collection of linear congruences.

3.2 Chinese Remainder Theorem

The simplest version of the **Chinese Remainder Theorem** is given by [10].

Theorem 1. *Let us consider n_1, \dots, n_k being pairwise relatively prime positive integers, that is $\gcd(n_i, n_j) = 1$, when $i \neq j$. Then for all integers, there is a unique integer modulo $n = \prod_{i=1}^k n_i$, such as:*

$$x \equiv a_1(\text{mod } n_1), \dots, x \equiv a_k(\text{mod } n_k).$$

Then there exists only one solution:

$$x = a_1(\text{mod } N_1 N_1^{-1}) + \dots + a_k(\text{mod } N_k N_k^{-1})(\text{mod } N), \quad (2)$$

where $N_i = \frac{N}{n_i}$, $N_i N_i^{-1} = 1(\text{mod } n_i)$.

Based on the CRT, in ref [12], The Asmuth-Bloom system was developed by Charles Asmuth and John Bloom, and it is defined as follows.

3.3 Asmuth-Bloom's (r,n)-threshold secret sharing scheme

Definition 1. [12] *Let a group of integers be $m_0, m_1, m_2, \dots, m_n$. These integers should satisfy the following conditions:*

- (i) $(m_i, m_j) = 1$ for $i \neq j$;
- (ii) $m_0 \prod_{i=0}^{r-2} m_{n-i} < \prod_{i=1}^r m_i$.

As before, n here stands for the number of shares. The scheme works as follows:

- *The secret S is chosen as a random integer.*
- *Let A be a random integer such that $(S + Am_0) < m_1, \dots, m_r$. Shares are determined by $y_i = (S + Am_0) \text{mod}(m_i)$ for all $1 \leq i \leq n$. During the decoding procedure, the following system of congruences is considered for any r shares $y_i, 1 \leq i \leq r$ out of n shares:*

$$x \equiv y_i \text{mod}(m_i). \quad (3)$$

x can easily be calculated by using the CRT since m_i values are pairwise co-prime.

4 Our proposed method

4.1 Permutation phase

As we already know, image information differs from text information in a number of ways, including significant levels of redundancy and a strong correlation between neighboring pixels. As stated in the previous section, we construct our permutation phase according to the steps below:

- 1- Let us consider a $m \times n$ gray-scale image.
- 2- We convert our $m \times n$ gray-scale image in one vector $[1, m \times n]$.
- 3- A chaotic vector $X = X_0, X_1, \dots, X_{m \times n - 1}$ is generated from Logistic-Chebyshev map taking $m \times n$ iterations from 0 to $(m \times n - 1)$
- 4- The sequence obtained is sorted in descending order based on the index of the sequence X to create a new index j .
- 5- Our image vector $[1, m \times n]$ is permuted according to the new index j .

Figure 1 describes the steps detailed above for an example of a (3,3) gray-scale image.

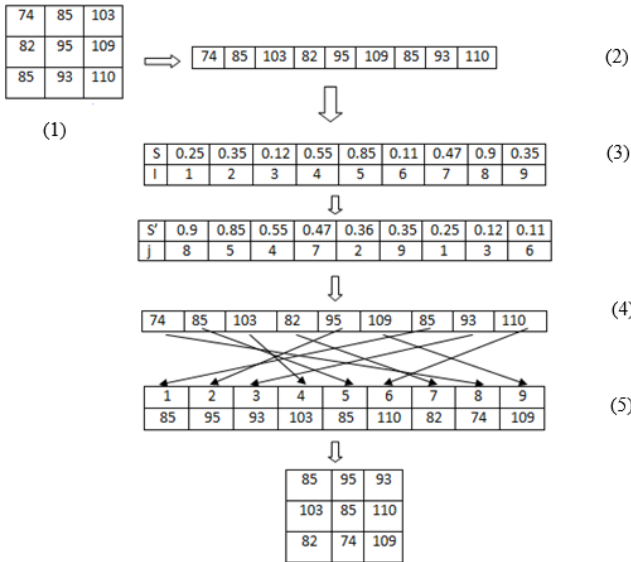


Figure 1. Permutation phase for gray-scale image

4.2 Sharing phase

In the following, we use the CRT theorem to encrypt the confused image; we consider a pixel X which is an integer value between 0 and 255. Since the decomposition of 255 in primary numbers is given by $255 = 17 \times 5 \times 3$, we obtain:

$$\begin{aligned} share_1 &\equiv X \pmod{17} \oplus K_m \\ share_2 &\equiv X \pmod{5} \oplus K_m \\ share_3 &\equiv X \pmod{3} \oplus K_m \end{aligned} \tag{4}$$

with K_m is a matrix random key whose size is the same as that of the secret image. Figure 2 shows an example of obtained share1, 2, and 3 from image of size (3,3) before applying the eXclusive-OR with the K_m .

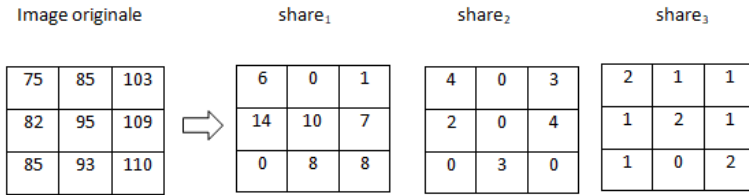


Figure 2. Example of creation shares with our proposed method

4.3 Reconstructing phase

The inverse of the sharing phase is the reconstruction phase. It is to note that we decrypt the encrypted images using the inverse of CRT Eq(2). Then, to obtain the original image, the reconfused image is permuted by using the inverse of the permutation phase as follows:

- 1- Let us consider the reconfused image after decrypting all shares.
- 2- We convert it in one vector.
- 3- We generate the same chaotic vector X from the Logistic-Chebyshev map obtained in permutation phase; cited by $(S; I)$.
- 4- The sequence obtained X is sorted in descending order based on their index I , to create a new index J ; cited by (S', J) .
- 5- We reconstruct the secret image as follows: the X pixel in J^{th} position of the reconfused image vector is placed in I^{th} position as shown

in Figure 3.

6- The reconstructed image (m, n) .

Figure 3 describes the reconstructed steps of the reconfused image detailed above.

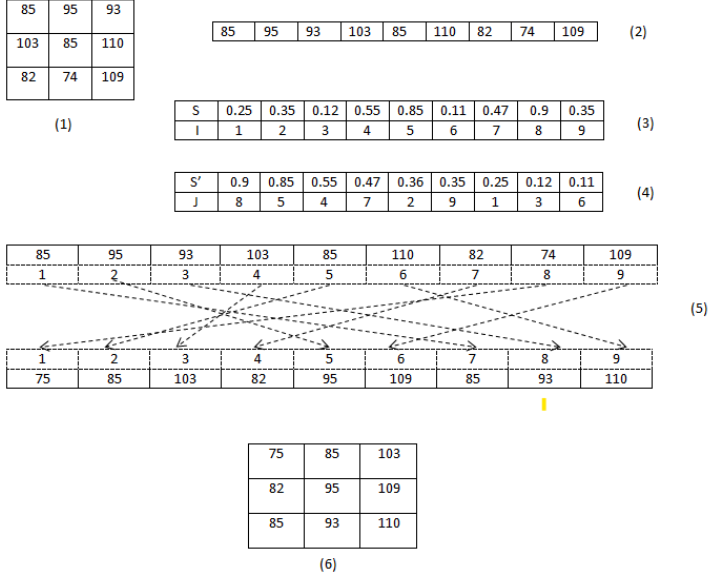


Figure 3. Reconstructed steps of reconfused image

5 Experimental results and analysis

In this paper, the feasibility and applicability of the suggested solution are presented, and the secret images of three sizes (a) 220×220 px, (b) 174×290 , and (c) 642×640 are encrypted. As shown in Figure 4, in our solution, all three shares can restore the original secret images without distortion. We demonstrate that with two parameters, $psnr$ and $ssim$.

5.1 The PSNR

PSNR is defined as the difference between the highest achievable power of the signal and the power of the corrupted noise [20] and given by



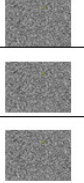



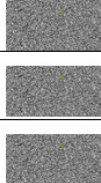



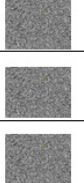

Secret image	Confused image	Encrypted shares	Decrypted image
 (a)			
 (b)			
 (c)			

Figure 4. Encryption and decryption of gray image

$$PSNR(dB) = 20 \log_{10} \left(\frac{max_i}{\sqrt{MSE}} \right), \quad (5)$$

where the image's maximum potential pixel value is max_i , it is equal to 255. The MSE stands for Mean Squared Error and represents the average square of the error between the original and the reconstructed image. The pixels are represented using 8 bits per sample. Theoretically, PSNR can be infinite if MSE equals 0; in this instance, the original and the reconstructed images are identical, i.e., the corresponding pixels of both images have similar values. The PSNR can also be calculated for color image by

$$PSNR(dB) = \frac{1}{n} \times (PSNR(Red) + PSNR(Green) + PSNR(Blue)), \quad (6)$$

where n is the number of all RGB color components.

Table 1. The PSNR value

Images	PSNR(dB)
(a)	infinite
(b)	infinite
(c)	infinite

From Table 1, the image revealed by three share images represents a PSNR infinite which means they have similar values to the original image. We will demonstrate later that fewer than three share images cannot give any information about the original secret image, but all share images can be used to reconstruct the original secret image without distortion.

5.2 The SSIM

A quality evaluation index is the SSIM Index. The computation of three parameters: the luminance, the contrast, and the structural parameters forms the basis of this method. According to [23], the overall index is given by

$$SSIM(x, y) = [l(x, y)]^\alpha \cdot [c(x, y)]^\beta \cdot [s(x, y)]^\gamma \quad (7)$$

and

$$\begin{cases} l(x, y) = \frac{2\mu_x\mu_y + C_1}{\mu_x^2 + \mu_y^2 + C_1} \\ c(x, y) = \frac{2\sigma_x\sigma_y + C_2}{\sigma_x^2 + \sigma_y^2 + C_2} \\ s(x, y) = \frac{\sigma_{xy} + C_3}{\mu_x^2 + \mu_y^2 + C_3} \end{cases}, \quad (8)$$

where, x and y represent two input images; μ_x, μ_y are the local means; σ_x, σ_y , are the standard deviations; and s is a cross-covariance for images x, y . α, β , and γ are factors used to modify the relative importance of the luminance, contrast, and structure; C_1, C_2 , and C_3 are constants used to avoid instability [23]. In the case when $\alpha = \beta = \gamma = 1$ and

$C_3 = \frac{C_2}{2}$, Eq.(7) can be expressed by

$$SSIM(x, y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)}. \quad (9)$$

Table 2 shows the values of SSIM. The obtained SSIM index is a decimal value between -1 and 1. An integer between -1 and 1 represents the obtained SSIM index. Only in the situation of two identical images x and y , the SSIM is a value equal to 1, signifying perfect structural similarity. It is necessary to note that, in our case, x is the original image and y is the reconstructed image.

Table 2. The SSIM value

Images	SSIM
(a)	1
(b)	1
(c)	1

By analyzing the results presented in Tables 1 and 2, we conclude that the proposed method is lossless. Furthermore, to rebuild the hidden image using this approach, all shares must be present and be the same size as the original image. The comparison of the proposed schemes with other references is shown in Table 3.

6 Security analysis

We examine the scheme's security in this section. We shall examine its resistance to the most significant attacks in particular. The security of the (3, 3)-SIS scheme relates to that we encrypt our image in three shares, and all three shares should be presented to restore the secret image. We demonstrate that with fewer than three shares, we rebuild the original image, but the quality is quite poor.

6.1 Statistical analysis

The statistical test seeks to ascertain the proposed scheme's confusion and diffusion features. A correlation test of the nearby pixels in the

Table 3. The comparison of the schemes presented in [17], [22], [25], [26] and the scheme proposed in this paper

	Scheme in [17]	Scheme in [22]	Scheme in [25]	Scheme in [26]	Our proposed
Encryption and decryption	CRT	CRT	CRT	CRT	CRT
The same size	Different size	the same size	the same size	Different size	the same size
Additional Information	Compression code	-	Confusion using chaotic map	-	Confusion using chaotic map
Is lossless	Yes	Yes	Yes	Yes	Yes
Threshold	(n, n)	(k, n)	(k, n)	(k, n)	(3, 3)

original image and their share, the entropy of Shannon, and histogram analysis are presented in this section.

6.1.1 Correlation coefficient factor

Correlation coefficient factor is a crucial element for evaluating an encryption algorithm's quality (CC). This analysis helps to explain how closely the original image and encrypted images resemble one another. According to Eqs(10)(11)(12)(13), the CC factor of the adjacent pixel [21] can be stated.

$$r_{xy} = \frac{cov(x, y)}{\sqrt{D(x)}\sqrt{D(y)}} \quad (10)$$

$$cov(x, y) = \frac{1}{N} \sum_{i=1}^N (x_i - E(x))(y_i - E(y)) \quad (11)$$

$$D(x) = \frac{1}{N} \sum_{i=1}^N (x_i - E(x))^2 \quad (12)$$

$$D(x) = \frac{1}{N} \sum_{i=1}^N x_i \quad (13)$$

where x and y represent the values of two neighboring pixels in the original or encrypted images, $E(x)$ is the mean value of x , $D(x)$ is the variance with respect to mean, $cov(x, y)$ represents the estimation of the covariance between neighboring pixels x and y , and r_{xy} represents the correlation coefficient between x and y . For better encrypted image, correlation coefficient should be close to zero or very low. Table 4 lists the computed correlation coefficients of original and share images. It is clear from Table 4 that the two neighboring pixels in the original images are strongly correlated to each other, while the correlation coefficients for the encrypted images are so close to zero.

Table 4. The correlation coefficient of images (a), (b), and (c) and their corresponding Share images

Images	Horizontal	Vertical	Diagonal
(a)	0.9207	0.9582	0.8909
Share1	-0.0083	-0.0031	0.0026
Share2	-0.0085	-0.0038	0.0043
Share3	-0.0081	-0.0043	0.0043
(b)	0.9759	0.9710	0.9573
Share1	0.0074	0.0017	0.0011
Share2	-0.0079	-0.0020	-0.0017
Share3	-0.0079	0.0015	0.0016
(c)	0.9308	0.9131	0.8812
Share1	-0.0010	-0.0011	-0.0005
Share2	-0.0009	-0.0008	0.0009
Share3	-0.0009	-0.0008	0.0006

6.1.2 Entropy of Shannon

The Shannon entropy over the ciphertext is a standard metric for evaluating the effectiveness of image encryption. It was first proposed by Claude Shannon in 1948, [24] and defined by Eq (14).

$$H(X) = - \sum_{i=1}^n Pr(x_i) \log_2 Pr(x_i). \quad (14)$$

X denotes the test random variable, x_i denotes the i_{th} possible value of X , and $Pr(x_i)$ is the probability of $X = x_i$. An ideally encrypted image is completely random if an encrypted image is very random-like. It is believed that information entropy is very close to theoretical maximum; therefore, the pixel values are uniformly distributed within a random encrypted image. Table 5 shows the entropy of encrypted images, which is very close to 8, the theoretical upper bound of entropy for an 8-bit image. Since the image entropy is a quantitative measurement, it is an equivalent test to the histogram analysis, which plots the distribution of Pr and is commonly used for security analysis in the image encryption literature.

Table 5. The entropy value

Images	secret image	im-share 1	share 2	share 3
(a)	7.4721	7.9964	7.9956	7.9947
(b)	7.6451	7.9959	7.9459	7.9958
(c)	7.3405	7.9994	7.9990	7.9986

6.1.3 Histogram of analysis

The statistical properties of images are shown by the histograms. The histograms of the secret and reconstructed images are displayed in Fig. 5, where it can be seen that for images (a), (b), and (c), the histogram following the decryption process is identical to that of the secret image; whereas, before decryption, the encrypted images' histograms are uniformly distributed and significantly different from those of the original images.

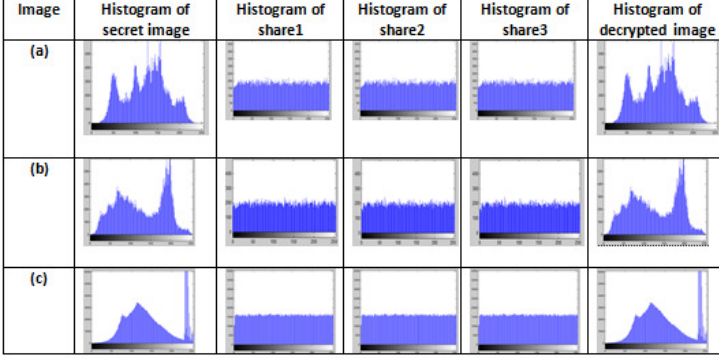


Figure 5. The histogram analysis of secret, encrypted, and decrypted images

6.2 Security of the sharing scheme

The logistic-Chebyshev map and CRT serve as the foundation for the sharing scheme's security. The threshold in this method is three, and any shadow images with two or less cannot obtain enough data to reconstruct the hidden image. From Section 4, in our case $r = n$, then $\min(r) = \prod_{i=1}^r m_i$ and $\max(r - 1) = \prod_{i=1}^{n-r+2} m_i$ we choose an arbitrary secret value $S = 127$, which is a positive integer and $\max(r - 1) < S < \min(r)$. Let a_i denote the remainder of S modulo m_i . In our scheme, we have three prime integers $m_1 = 17, m_2 = 5$, and $m_3 = 3$, which $3 < 5 < 17$, and $a_1 = 8, a_2 = 2$, and $a_3 = 1$. The S can be restored by all three sharing values. We compute $y = CRT[(a_1, a_2, a_3), (m_1, m_2, m_3)] = 127$. If we choose $w = CRT[(a_1, a_2), (m_1, m_2)] = 25 \neq 127$ or $w = CRT[(a_2, a_3), (m_2, m_3)] = 187 \neq 127$ or $w = CRT[(a_1, a_3), (m_1, m_3)] = 170 \neq 127$.

In Figure 6, (a), (b), and (c) are the secret images; however, (a-1), (b-1), and (c-1) are the images revealed by 2 shares. Moreover, (a-2), (b-2), and (c-2) are the images revealed by 1 share. According to the experimental results, two or one share images cannot divulge any information about the original secret image, but the three share images can be used to accurately reconstruct the original secret image.

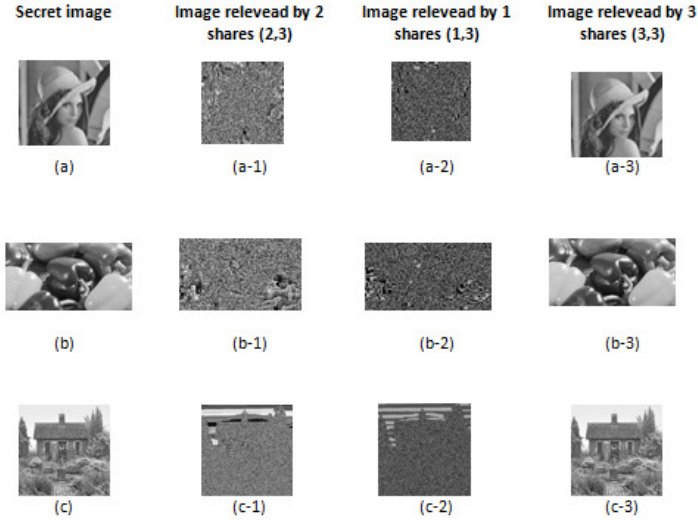


Figure 6. The experimental results of (1,3), (2,3), and (3,3) secret image sharing based on Chinese remainder theorem

To better clarify the experimental results, the PSNR values of images (a-1), (a-2), (a-3), (b-1), (b-2), (b-3), (c-1), (c-2), and (c-3) are presented in Table 6. According to Table 6, the PSNR values of the images revealed by one or two share images are very low ($< 10dB$).

Table 6. The PSNR value

Images	PSNR(dB)
(a-1)	9.314
(a-2)	9.181
(b-1)	9.257
(b-2)	9.187
(c-1)	8.278
(c-2)	9.102

7 Color image

Now, the scheme is extended to apply to the encryption of color image. After testing, the effect is good. The scheme can also be used for color image.

7.1 Simulation results

The simulation is realized for the "Lena" color image. We first extracted the original image in three components, R, G, and B (Red, Green, and Blue); then we used the Logistic-Chebyshev map to scramble each component; after that we have (3, 3)-scheme based on CRT to encrypt each component in three shares as shown in Figures 7 and 8.



Figure 7. The color secret image and the confused images for each component image

7.2 Security analysis

This section shows directly the PSNR value of the reconstructed images when less than n shares are decrypted. For information, please refer to Section 5.1.

As shown in Figures 9, 10, and 11, the images reconstructed by less than nine shares (three shares for each components) present bad-quality of images. This is demonstrated by the PSNR values of the SIS schemes (8,9), (7,9), and (6,9) which do not exceed 11.99 dB.

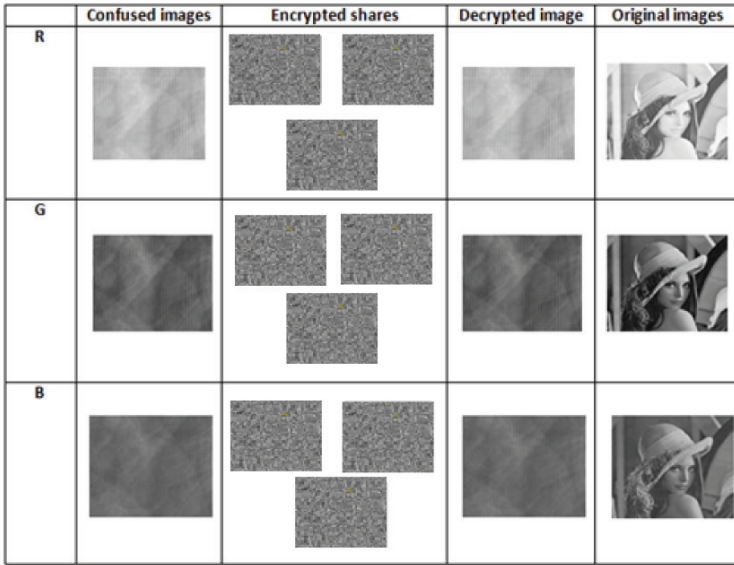


Figure 8. The confused images, encrypted shares, decrypted shares, and reconstructed images

7.2.1 Correlation coefficient factor

For details of correlation, see Section 6.1.1. This section directly shows the correlation coefficients of the R, G, and B components of the "Lena" color image. As shown in Table 7, our scheme can resist statistical analysis.

8 Analysis and comparison

This section analyzes the experimental findings of the (3, 3) secret sharing scheme based on the Chinese remainder theorem and compares it to the secret image sharing schemes provided in Reference [25].

8.1 Analysis

The (3, 3)-SIS scheme based on the Chinese remainder theorem is examined in this section in view of the experimental findings in Section


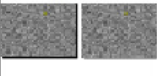


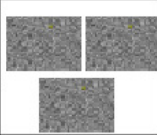

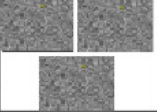

	Input image	Encrypted shares	Decrypted images	Output image
	R			<i>PSNR = 11.99 dB</i> 
	G			
	B			

Figure 9. The reconstructed image using (8, 9)-SIS schemes with PSNR value


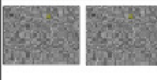

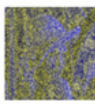
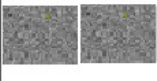

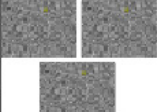

	Input image	encrypted shares	Decrypted images	Output image
	R			<i>PSNR = 9.88 dB</i> 
	G			
	B			

Figure 10. The reconstructed image using (7, 9)-SIS schemes with PSNR value

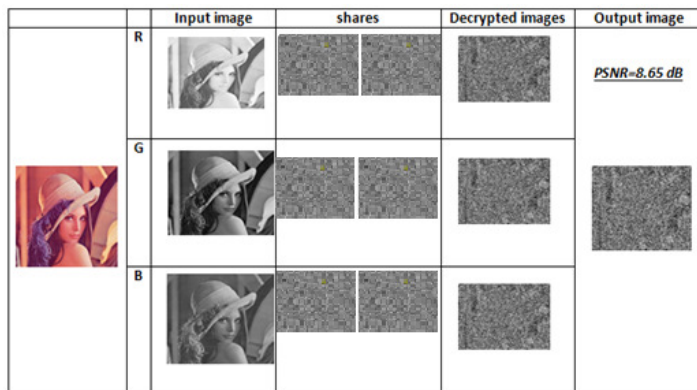


Figure 11. The reconstructed image using (6, 9)-SIS schemes with PSNR value

Table 7. The correlation coefficient of Lena and its corresponding share images

Images	Horizontal	Vertical	Diagonal
R	0.9433	0.9716	0.9150
Share1	0.0114	0.0128	0.0138
Share2	0.0041	-0.0037	-0.0114
Share3	0.0043	0.0058	-0.0006
G	0.9257	0.9618	0.8980
Share1	-0.0044	0.00938	0.0060
Share2	0.0061	0.0074	0.0018
Share3	0.0026	-0.0097	-0.0030
B	0.9100	0.9435	0.8783
Share1	-0.0040	-0.0066	0.0052
Share2	0.0030	0.0022	-0.0031
Share3	0.0017	-0.0068	-0.0017

5, and the following conclusions are drawn:

- a) Each and every one of the shared images is just random noise, revealing nothing about the original secret image.
- b) A recovery process cannot represent any information from the original secret image with fewer than three sharing images.
- c) To recreate the original secret image without distortion, three sharing images are used.
- d) Since there is no pixel expansion in the suggested approach, each share image is the same size as the original image.
- e) The approach can get rid of pixel correlations from the original secret image.
- f) Our proposed scheme is very suitable for color images.

8.2 Comparison

In the reference [25], a secret digital image is split into n pieces and then disseminated among the n participants, and only by using the cooperation of arbitrary r parties can the hidden digital image be rebuilt. But in our scheme, we choose three prime numbers that satisfy the CRT, and all these three parties are totally indispensable and should be present, just with $r \leq 2$ we can not rebuild the hidden image. The second point is about the permutation phase. In [25], the transformation is done via an equation. In our case, the permutation is totally different. The permutation phase is done according to the new index j as detailed in Section 4.1.

9 Conclusion

This paper proposes a lossless secret image sharing for grayscale and color image based on (3, 3) threshold cryptography, i.e., (3, 3)-SIS scheme. In order to strengthen our solution and make it more resistant against differential attack, we use a chaotic map to scramble the secret image before constructing three share images using our CRT technique. For the (3, 3)-SIS scheme, all three participants should be existed to restore the secret value. From the experiment, we can see that our (3, 3)-SIS scheme using CRT is reliable and effective; more-

over, we demonstrate that when the number of participants is less than three, the relevant information is very bad, which increases the level of security.

References

- [1] M. Naor and A. Shamir, “Visual cryptography,” in *EUROCRYPT: Workshop on the Theory and Application of Cryptographic Techniques*, (Italy), Springer, 1994.
- [2] W. Q. Yan, D. Jin, and M. S. Kankanhalli, “Visual cryptography for print and scan applications,” in *IEEE International Symposium on Circuits and Systems*, (Vancouver), 2004.
- [3] F. Liu, C. Wu, and X. Lin, “Step Construction of Visual Cryptography Schemes,” *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 1, pp. 27–38, 2009.
- [4] E. Verheul and H. V. Tilborg, “Constructions and properties of k out of n visual secret sharing schemes,” *Des. Codes Cryptogr.*, vol.11, pp. 179–196, 1997.
- [5] P. A. Eisen and D. R. Stinson, “Threshold visual cryptography schemes with specified whiteness levels of reconstructed pixels,” *Des. Codes Cryptogr.*, vol. 25, pp. 15–61, 2002.
- [6] F.Liu, C.Wu, and X.Lin, “A new definition of the contrast of visual cryptography scheme,” *Information Processing Letters*, vol. 110, no. 7, pp. 241–246, 2009.
- [7] K. Shankar and P. Eswaran, “Sharing a Secret Image with Encapsulated Shares in Visual Cryptography,” *Procedia Computer Science*, vol. 70, pp. 462–468, 2015.
- [8] K. Shankar and P. Eswaran, “RGB-Based Secure Share Creation in Visual Cryptography Using Optimal Elliptic Curve Cryptography Technique,” *Journal of Circuits, Systems, and Computers*, vol. 25, pp. 1–23, 2016.

- [9] K. Shankar and P. Eswaran, “RGB Based multiple Share Creation in Visual Cryptography with Aid of Elliptic Curve Cryptography,” *China Communications*, vol. 14, pp. 118–130, 2017.
- [10] S. J. Shyu and Y. -R. Chen, “Threshold Secret Image Sharing by Chinese Remainder Theorem,” in *2008 IEEE Asia-Pacific Services Computing Conference*, (Yilan, Taiwan), 2008, pp. 1332–1337. DOI: 10.1109/APSCC.2008.223.
- [11] M. Mignote, “How to share a secret,” in *Cryptography. EURO-CRYPT 1982* (Lecture Notes in Computer Science, vol 149), T. Beth, Ed. Berlin, Heidelberg: Springer, 1983, pp. 371–375. DOI: https://doi.org/10.1007/3-540-39466-4_27.
- [12] C. Asmuth and J. Bloom, “A Modular Approach to Key Safeguarding,” *IEEE Transactions on information theory*, vol. 29, pp. 208–210, 1983.
- [13] Jinrui Chen, Kesheng Liu, Xuehu Yan, Lintao Liu, Xuan Zhou, and Longdan Tan, “Chinese Remainder Theorem-Based Secret Image Sharing with Small-Sized Shadow Images,” *Symmetry*, vol. 10, no. 8, Article No. 340, 2018. DOI: <https://doi.org/10.3390/sym10080340>.
- [14] P. Heri and M.G. Jing, “A Note on Multiple Secret Sharing Using Chinese Remainder Theorem and Exclusive-OR,” *IEEE Access*, vol. 7, pp. 37473–37497, 2019.
- [15] Guanrong Chen, Yaobin Mao, and Charles K. Chui, “A symmetric image encryption scheme based on 3D chaotic cat maps,” *Chaos, Solitons and Fractals*, vol. 21, no. 3, pp. 749–761, 2004. DOI: <https://doi.org/10.1016/j.chaos.2003.12.022>.
- [16] M. L. Sahari and I. Boukemara, “A pseudo-random numbers generator based on a novel 3D chaotic map with an application to color image encryption,” *Nonlinear Dynamics*, vol. 94, pp. 723–744, 2018. DOI: <https://doi.org/10.1007/s11071-018-4390-z>.

- [17] Wei Hua and Xiaofeng Liao, “A secret image sharing scheme based on piecewise linear chaotic map and Chinese remainder theorem,” *Multimedia Tools and Applications*, vol. 76, no. 5, pp. 1–17, 2016. DOI: 10.1007/s11042-016-3364-8.
- [18] A. Alanezi, B. Abd-El-Atty, H. Kolivand, A. A. Abd El-Latif, B. Abd El-Rahiem, S. Sankar, and H. S. Khalifa, “Securing Digital Images through Simple Permutation-Substitution Mechanism in Cloud-Based Smart City Environment,” *Security and Communication Networks*, Volume 2021, Article ID 6615512, 2021. DOI: <https://doi.org/10.1155/2021/6615512>.
- [19] S. Iftene and I.C. Boureanu, “Weighted threshold secret sharing based on the Chinese remainder theorem,” *Scientific Annals of Cuza University*, vol. 15, pp. 161–172, 2005.
- [20] A. T. Nasrabadi, M. A. Shirsavar, A. Ebrahimi, and M. Ghanbari, “Investigating the PSNR calculation methods for video sequences with source and channel distortions,” in *IEEE International Symposium on Broadband Multimedia Systems and Broadcasting*, (Beijing, China), 2014, pp. 1–4. DOI: 10.1109/BMSB.2014.6873482.
- [21] Sura F. Yousif, “Grayscale Image Confusion and Diffusion Based on Multiple Chaotic Maps,” in *1st International Scientific Conference of Engineering Sciences - 3rd Scientific Conference of Engineering Science (ISCES)*, pp. 114–119, 2018.
- [22] S. Zhang and F. Miao, “Secret Image Sharing Based on Chinese Remainder Theorem over a Polynomial Ring,” in *Machine Learning for Cyber Security. ML4CS 2020* (Lecture Notes in Computer Science, vol 12486), X. Chen, H. Yan, Q. Yan, X. Zhang, Eds. Springer, Cham., 2020, pp. 634–643.
- [23] W. Zhou, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, “Image Quality Assessment: From Error Visibility to Structural Similarity,” *IEEE Transactions on Image Processing*, vol. 13, pp. 600–612, 2004.

- [24] C.E. Shannon, "A mathematical theory of communication," *Bell System Technical Journal*, vol. 27, pp. 379–423 and 623–656, 1948.
- [25] C. Hu, X. Liao, and D. Xiao, "Secret Image Sharing Based on Chaotic Map and Chinese Remainder Theorem," *International Journal of Wavelets, Multiresolution and Information Processing*, vol. 10, no. 3, 2012.
- [26] S. J. Shyu and Y. R. Chen, "Threshold secret image sharing by Chinese Remainder theorem," in *Asia-Pacific Services Computing Conference, 2008. APSCC'08. IEEE*, pp. 1332–1337, 2008.

Asmaa Hilmi, Soufiane Mezroui,
Ahmed El Oualkadi

Received October 16, 2021
Revised 1 – October 24, 2022
Revised 2 – February 09, 2023
Accepted February 16, 2023

Asmaa Hilmi

ORCID: <https://orcid.org/0000-0002-4665-7177>

Abdelmalek Essaadi University National School

of applied sciences of Tangier (ENSAT)

Laboratory of Information and Communication Technologies (LabTIC)

ENSA Tanger, Route Ziaten, BP 1818, Tanger principale, Morocco.

E-mail: asmaa00hilmi@gmail.com

Soufiane Mezroui

ORCID: <https://orcid.org/0000-0003-2705-9806>

Abdelmalek Essaadi University National School

of applied sciences of Tangier (ENSAT)

Mathematics and Intelligent Systems Team (MASI) ENSA Tanger,

Route Ziaten, BP 1818, Tanger principale, Morocco.

E-mail: mezroui.soufiane@yahoo.fr

Ahmed El Oualkadi

ORCID: <https://orcid.org/0000-0002-4953-1000>

Abdelmalek Essaadi University National School

of applied sciences of Tetuan (ENSATe)

Laboratory of Information and Communication Technologies (LabTIC)

ENSA Tetouan, Avenue Palestine B.P 2222, M'hannech II-Tetouan, Morocco.

E-mail: eloualkadi@gmail.com