Received: February 13, 2022. Revised: March 15, 2022.

INASS

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Effective Secret Image Sharing using Enhanced Chinese Remainder Theorem

Arvind Singh Choudhary[1]* **Manoj Kumar[2]** **Sudhir Keshari[1]**

[1]*Government Engineering College Bharatpur, Bharatpur, India*
[2]*GLA University, India*
* Corresponding author's Email: arvindbecs@gmail.com

Abstract: In recent decades, the Secret Image Sharing (SIS) technique is used for encrypting a secret image into "n" number of specious shadow images, where it is hard to reveal the data on a secret image, even if one shadow image is not achieved. In this manuscript, a new SIS model is proposed based on the Chinese Remainder Theorem (CRT), where the proposed model utilizes polynomial f(x) over F_2 (x) for partitioning the secret image. Further, the least significant bit substitution technique is applied for hiding the shadow images and generating stego images. The proposed enhanced CRT (ECRT) model guarantees loss-less cover and secret image reconstruction. The proposed ECRT is more secure compared to the traditional CRT model, because the shadow images are noise-less and the secret images are meaningful. The experimental outcomes show that the proposed ECRT model achieved superior SIS performance even under the conditions of crop attack, noise attacks, and histogram equalization using seven different performance measures. By inspecting the experimental outcomes, the proposed ECRT model almost showed 20% to 25% improvement in peak signal to noise ratio value related to the comparative models.

Keywords: Chinese remainder theorem, Least significant bit substitution, Polynomial ring, Secret image sharing, security.

1. Introduction

In recent decades, the internet and technology improvement offers more possibilities to transmit and store images on cloud storage, mobiles, and computers [1, 2]. However, the online platforms are not 100% secure, so it is essential to protect the images from being destroyed or robbed by hackers, particularly in the research field of defense and industrial sectors [3-5]. To overcome these issues, the researchers developed many protection techniques like steganography, cryptography, SIS, etc. [6-8]. Among the available image protection techniques, the SIS is one of the primitives for protecting important images [9]. The SIS technique develops shadow images from a secret image and then transmits them to the respective participants. In recent periods, the SIS technique is applied in numerous applications, which includes the distributed storage of digital images in the cloud. Where, the present digital images are highly important in the computer vision and medical fields [10]. In a few cases, the secret image is a gray-scale image, and the participants have dissimilar rights. Therefore, it is essential to allocate the shares with secret information to the participants with maximum weights [11]. The transmission quality of the communication channels is different while transmitting the shares [12]. In this manuscript, a new ECRT model is proposed for secure image sharing. The major contributions of this manuscript are listed as follows:

- A new CRT based SIS model over $F_2(x)$ is implemented for partitioning a secret image to generate n number of shadow images. In addition, the Least Significant Bit (LSB) substitution technique is employed for embedding the shadow images into the cover images to create useful stego images.
- In the proposed ECRT model, the LSB pixels in the cover images are stored in $f(x)$ such

that the cover images are reconstructed after extracting the secret images.

- The simulation results confirmed that the proposed ECRT model obtained shadow images with better quality.
- The efficiency of the ECRT model is validated by utilizing seven performance measures like Mean Absolute Error (MAE), entropy value, Mean Square Error (MSE), Peak Signal-to Noise ratio (PSNR), Similarity index (SSIM), Normalized Cross-Correlation (NCC) and Unified Averaged Changed Intensity (UACI).

This manuscript is structured as follows: a few articles on the research area "SIS" are surveyed in Section 2. The mathematical derivations and the experimental examination of the ECRT model are detailed in Sections 3 and 4. The conclusion of the manuscript is represented in Section 5.

2. Related works

Sardar and Adhikari, [13] developed a polynomial-based SIS approach that converts the secret color images into shadow images, which were smaller related to the original secret images. The transformation of shadow image precisely reconstructs the original secret image without any distortions. The comparison and experimental outcomes demonstrated that the presented approach obtained significant performance compared to the existing approaches. However, the shadow size reduction needs to be improved without compromising security. Shankar [14] presented a new wavelet-based SIS approach based on optimal homomorphic encryption technique. Initially, the Discrete Wavelet Transform (DWT) technique was employed on the secret images to generate sub-bands that create multiple shadows. Further, every shadow was encrypted and decrypted using homomorphic encryption technique and oppositional-based harmony search method that enhances the shadow security by generating the optimal key. The experimental examination showed that the presented wavelet-based SIS approach obtained better security related to other existing approaches. Still, the developed wavelet based SIS approach includes two problems like controlling the image quality and recovering secret images losslessly.

Nag [15] presented a new multi SIS approach based on XOR operation. The presented approach was lossless and computationally light-weighted, due to XOR operation, which does not involve any pixel expansion. The simulation result showed that the presented multi SIS approach attained better results with a low correlation coefficient between secret and share images. However, the developed multi-SIS approach includes the problem of single-point failure. Wu [16] presented a novel modular arithmetic approach to improving the quality of recovery images based on the polynomial based SIS approach. The presented approach outperformed the traditional approaches in light of recovered image quality. Still, the developed modular arithmetic approach needed to be included in the image-sharing application to further enhance the visual performance. Tan [17] introduced a Chinese Remainder Theorem (CRT) for securely sharing the gray-scale images. However, the average light transmission was different and needs to be enhanced in future work.

Meng [18] developed a new SIS approach based on CRT, which utilizes polynomials for dividing the secret images. In addition, the least significant bit technique was applied to generate stego images and to hide the shadow images. In the resulting section, the developed SIS approach achieved better lossless reconstruction on both cover and secret images. Yan [19] used CRT with three decoding options like visual previewing ability, grayscale stacking recovery, and lossless recovery for SIS. The grayscale secret image was decoded losslessly by solving the linear congruence equation with the modular operation. The theoretical and experimental evaluation showed the effectiveness of the developed SIS approach. However, the major issue of this literature was to handle the dishonest participants. Ding [20] implemented a matrix theory based on polynomial based SIS approach. The obtained experimental and theoretical results showed the efficiency of the presented approach. The developed matrix theory model includes pixel expansion problem that decreases the number of shares and reduces the resolution and security of the secret image. For highlighting the aforementioned issues, a new model: ECRT is proposed in this article.

3. Methodology

The proposed ECRT model initially partitions a secret image S into 'n' number of shadow images SH_i, and then a cover image C is used for generating 'n' number of stego images $ST_i, i = 1,2 \ldots\ldots n$. The cover and secret images are losslessly recovered by pooling t or more stego images together. Two types of images (secret and cover images) are used for experimental investigation in the SIS application. Generally, the cover image is utilized to embed a secret image, which should be a noise-less and appropriate image. In this manuscript, the multimedia images like Lena, Baboon, Pepper, etc. are utilized as

a secret and cover image. The ECRT model needs to satisfy two conditions such as correctness and security, which are mathematically mentioned in the Eqs. (1) and (2).

$$H\left(S\middle|\left(ST_{i_1},\ldots..,ST_{i_t}\right)\right)=0$$
$$H\left(C\middle|\left(ST_{i_1},\ldots..,ST_{i_t}\right)\right)=0 \quad (1)$$

$$I\left(S;\left(ST_{i_1},\ldots,ST_{i_{t-1}}\right)\right)=0 \quad (2)$$

Where, $I(X;Y)$ is mutual information that includes the information of X, which is obtained from the knowledge of Y, $H(X)$ is entropy that represents X uncertainty, and $H(X/Y)$ is a conditional entropy that denotes the uncertainties of X and Y. The threshold t is 2 and a total number of shadow images SH is 3. The ECRT model includes 3 algorithms such as sharing, recovery, and hiding.

3.1 Sharing algorithm

Step 1: Initially, the dealer D selects the secret images S with the size of $W_s \times H_s$, and the cover images C with the size of $W_c \times H_c$, is mathematically represented in Eq. (3).

$$4(W_s \times H_s) = (t-1)(W_c \times H_c) \quad (3)$$

Step 2: Then, $m_0(x) = x^8$ is defined. The dealer D chooses co-prime polynomials $m_i(x)\,\epsilon\,F_2[x]$, where, $i = 1,2,..,n$, such that $deg\left(m_1(x)\right) = \cdots = deg\left(m_n(x)\right) = 8$, and $\forall i\epsilon\{1,2,\ldots,n\}$, where $m_i(x)$ and $m_0(x)$ are co-prime. The dealer D make all the polynomials public: $m_i(x)$ and $m_0(x)$, and $m_i(x)$ is related to shareholder U_i.

Step 3: The cover image C is partitioned into $\frac{W_c \times H_c}{4}$ blocks, where every block comprises four pixels. In addition, the secret image S is partitioned into $\frac{W_s \times H_s}{t-1}$ blocks, where each block has $t-1$ pixels.

Step 4: Then, the dealer D selects one block that includes four pixels in the cover image C such as $p_{c,1}, p_{c,2}, p_{c,3}, and\ p_{c,4}$. Further, the D uses LSBs in the four pixels for constructing the polynomial of degree seven that is mathematically stated in Eq. (4). The LSB is utilized as the bit position of the integer values. By employing seven bit LSB, the pixel value of secret and cover images are transformed.

$$A(x) = \sum_{i=1}^{4}(a_{i,1}x^{2i-2} + a_{i,2}x^{2i-1}) \quad (4)$$

Where, $a_{i,j}$ represents j^{th} LSB of pixel $p_{c,i}$.

Step 5: The dealer D selects one block that includes $t-1$ pixels $p_{s,1}, \ldots, p_{s,t-1}$ in the secret image S for constructing a polynomial of degree eight: $8(t-1)-1$, as mathematically stated in Eq. (5).

$$B(x) = \sum_{i=1}^{t-1}\sum_{j=1}^{8} b_{i,j}x^{8(i-1)+(j-1)} \quad (5)$$

Where, $b_{i,j}$ indicates j^{th} LSB of pixel $p_{s,i}$.

Step 6: The dealer D utilizes $A(x), B(x)\ and\ m_0(x)$ for obtaining the sharing polynomial $f(x)$, which is mathematically represented in Eq. (6).

$$f(x) = A(x) + B(x) \times m_0(x) \quad (6)$$

Step 7: Further, the dealer D calculates a share polynomial $s_{sh,i}(x)$ for a shareholder U_i, which is mathematically depicted in Eq. (7).

$$s_{sh,i}(x) = f(x)\ mod\ m_i(x) \quad (7)$$

The $s_{sh,i}(x)$ a degree is not more than eight, because $deg\left(m_i(x)\right) = 8$, so share polynomial $s_{sh,i}(x)$ is re-written as stated in Eq. (8). Further, the shadow image pixel $p_{sh,i}$ is determined as $p_{sh,i} = s_{sh,i}$.

$$s_{sh,i}(x) = c_0 + c_1x + \cdots + c_7x^7 \quad (8)$$

Step 8: Repeat steps 4 to 7, until the secret images are completely shared. Finally, the dealer D obtains the shadow images with the size of $\frac{W_c \times H_c}{4}$.

3.2 Hiding algorithm

In this scenario, the dealer D uses the 2-LSB technique for embedding the shadow images SH_i in the cover images C for generating the stego images ST_i.

Step 1: The dealer D selects a pixel $p_{sh,i}$ in the shadow image SH_i, where one block contains four pixels such as $p_{c,1}, p_{c,2}, p_{c,3}, and\ p_{c,4}$ in the cover image C. The dealer D need to hide $p_{sh,i}$ in the four pixels of the cover image C for generating four pixels $p_{st,1}, p_{st,2}, p_{st,3}, and\ p_{st,4}$ of the stego image ST_i.

Step 2: The pixel $p_{sh,i}$ is calculated as $p_{sh,i} = s_{sh,i}$, where c_i of $s_{sh,i}(x)$ is $i+1^{th}$ bit of $p_{sh,i}$. The four pixels in the stego image are calculated based on the 2-LSB technique, which are mathematically denoted in the Eqs. (9) to (12).

$$p_{st,1} = p_{c,1} - (p_{c,1} \; mod \; 4) + c_0 + (c_1) \times 2 \quad (9)$$

$$p_{st,2} = p_{c,2} - (p_{c,2} \; mod \; 4) + c_2 + (c_3) \times 2 \; (10)$$

$$p_{st,3} = p_{c,3} - (p_{c,3} \; mod \; 4) + c_4 + (c_5) \times 2 \; (11)$$

$$p_{st,4} = p_{c,4} - (p_{c,4} \; mod \; 4) + c_6 + (c_7) \times 2 \; (12)$$

Step 3: Repeat the steps 1 and 2, until SH_i is completely embedded into C. Finally, the dealer D generates the stego image ST_i with the size of $W_c \times H_c$.

Step 4: The dealer D distributes ST_i to the respective shareholder U_i after all the stego images are generated $ST_i, i = 1,2,3, \dots, n$.

3.3 Recovery algorithm

Step 1: The shareholders $U_1, U_2, \dots U_k$ are collaborated for recovering the cover image C and secret image S. Further, every shareholder obtains k stego images $ST_i, i = 1,2, \dots, k$.

Step 2: The U_i need to extract the shadow image SH_i from the stego image ST_i. Further, the stego image is partitioned into $\frac{W_c \times H_c}{4}$ blocks. Next, U_i selects one block that consists of four pixels such as $p_{st,1}, p_{st,2}, p_{st,3}, and \; p_{st,4}$, and then one pixel $p_{sh,i}$ of shadow image SH_i is determined using Eq. (13). The U_i used the shadow image for recovering both cover and secret image after all k shadow images are recovered.

$$p_{sh,i} = \sum_{j=1}^{4} (p_{st,j} \; mod \; 4)^{4^{j-1}} \quad (13)$$

Step 3: The U_i selects one pixel $p_{sh,i}$ from SH_i and then recovers $s_{sh,i}(x)$ from $p_{sh,i}$. Further, the congruent equations are obtained, as shown in Eq. (14).

$$\begin{Bmatrix} f(x) \equiv s_{sh,1}(x) \; mod \; m_1(x); \\ f(x) \equiv s_{sh,2}(x) \; mod \; m_2(x); \\ \vdots \\ \vdots \\ f(x) \equiv s_{sh,k}(x) \; mod \; m_k(x). \end{Bmatrix} \quad (14)$$

Additionally, $f(x)$ is evaluated based on $deg(f(x)) < \sum_{i=1}^{k} deg(m_i(x))$, as mentioned in Eq. (15).

$$f(x) = (\sum_{i=1}^{k} s_{sh,i}(x) r_i(x) M_i(x)) \; mod \; M(x) \; (15)$$

Where, $r_i(x) \equiv M_i^{-1}(x) \; mod \; m_i(x)$, $M(x) = \prod_{i=1}^{k} m_i(x)$ and $M_i(x) = M(x)/m_i(x)$. Further, U_i evaluates $A(x)$ and $B(x)$, which are mathematically depicted in the Eqs. (16) and (17).

$$A(x) = f(x) \; mod \; m_0(x) \quad (16)$$

$$B(x) = \frac{f(x) - A(x)}{m_0(x)} \quad (17)$$

Step 4: The terms $A(x)$ and $B(x)$ are already computed as shown in Eqs. (18) and (19).

$$A(x) = \sum_{i=1}^{4} (a_{i,1} x^{2i-2} + a_{i,2} x^{2i-1}) \quad (18)$$

$$B(x) = \sum_{i=1}^{t-1} \sum_{j=1}^{8} b_{i,j} x^{8(i-1)+(j-1)} \quad (19)$$

Where, $p_{s,i}$ indicates pixel value of secret image, $p_{c,i}$ represents pixel value of cover image, $b_{i,j}$ is j^{th} LSB of pixel $p_{s,i}$, $a_{i,j}$ is j^{th} LSB of pixel $p_{c,i}$, and U_i recovers $t-1$ pixels of the secret image from $B(x)$. Further, four pixels $p_{c,1}, p_{c,2}, p_{c,3}, and \; p_{c,4}$ of cover image is recovered from $A(x)$ and four pixels $p_{st,1}, p_{st,2}, p_{st,3}, and \; p_{st,4}$ of a stego image is mathematically depicted in Eqs. (20) to (23).

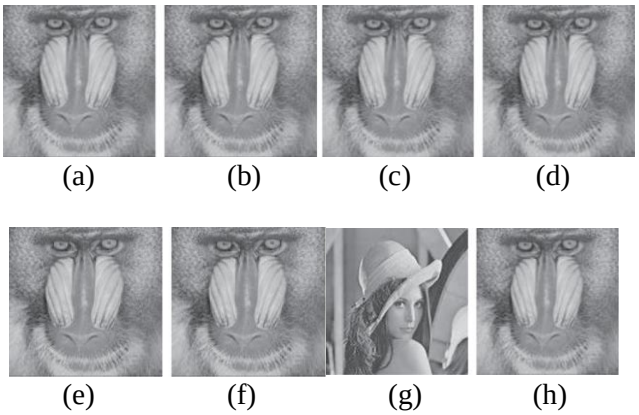
$$p_{c,1} = p_{st,1} - (p_{st,1} \; mod \; 4) + a_{1,1} + (a_{1,2}) \times 2; \; (20)$$

$$p_{c,2} = p_{st,2} - (p_{st,2} \; mod \; 4) + a_{2,1} + (a_{2,2}) \times 2; \; (21)$$

$$p_{c,3} = p_{st,3} - (p_{st,3} \; mod \; 4) + a_{3,1} + (a_{3,2}) \times 2; \; (22)$$

$$p_{c,4} = p_{st,4} - (p_{st,4} \; mod \; 4) + a_{4,1} + (a_{4,2}) \times 2. \; (23)$$

Step 5: Finally, repeat steps 3 to 5, until both cover and secret image are completely recovered, which is graphically depicted in Fig. 1.



(a) (b) (c) (d)

(e) (f) (g) (h)

Figure. 1 (a) to (f) Stego images, (g) Recovered secret image, and (h) Recovered cover image

4. Experimental results

The proposed ECRT model's effectiveness is validated using MATLAB 2020a software tool on a system configuration with 16GB random access memory, 4TB hard-disk, Intel core i9 processor, and Linux operating system. In this manuscript, the proposed ECRT model result is compared with the existing works on some standard images like Pepper, Barbara, Baboon, Lena, etc. Additionally, the proposed ECRT model's efficiency is analyzed using the performance measures like PSNR, NCC, SSIM, UACI, MSE, entropy, and MAE. The mathematical representations of entropy value, PSNR and MSE are defined in the Eqs. (24) to (26).

$$E(m) = \sum_{x=0}^{m-1} p(m_x) log_2 \frac{1}{p(m_x)} \quad (24)$$

Where, m represents the total number of symbols $m_x \epsilon m$, and $p(m_x)$ indicates a probability of symbol occurrence m_x.

$$PSNR = 10\ log_{10}(\frac{255^2}{MSE}) \quad (25)$$

$$MSE = 1/pq \sum_{x=0}^{p-1} \sum_{y=0}^{q-1} [I(x,y) - k(x,y)]^2 \quad (26)$$

Where, $I(x,y)$ indicate original input image, $k(x,y)$ represents a reconstructed image, and $p\ and\ q$ states row and column of the image. The mathematical representations of SSIM, UACI, and NCC are defined in the Eqs. (27) to (29).

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)} \quad (27)$$

$$\frac{1}{pq} \sum_{x=1}^{p} \sum_{y=1}^{q} \frac{|E_1(x,y) - E_2(x,y)|}{255} \times 100 \quad (28)$$

$$NCC = \left[\frac{\sum_{x=1}^{p} \sum_{y=1}^{q} [I(x,y) k(x,y)]}{\sum_{x=1}^{p} \sum_{y=1}^{q} [I(x,y)]^2} \right] \quad (29)$$

Where, $E_1\ and\ E_2$ indicates encrypted image, $c_1\ and\ c_2$ denotes constants, $\mu\ and\ \sigma$ denotes mean and standard deviation of x and y, and $x\ and\ y$ states windows of the original image and reconstructed image. The MAE is applied to estimate the average error magnitude between the original input image and the reconstructed image, which is mathematically stated in Eq. (30). Additionally, the tested images are graphically shown in Fig. 2.

(a) (b) (c) (d)

(e) (f) (g) (h)

Figure. 2 Tested images, (a) Airplane, (b) Barbara, (c) Cameraman, (d) Elaine, (e) Lake, (f) Peppers, (g) Lena, and (h) Baboon

$$MAE = 1/pq \sum_{x=0}^{p-1} \sum_{y=0}^{q-1} [I(x,y) - k(x,y)] \quad (30)$$

4.1 Quantitative analysis

In this scenario, the proposed ECRT model's efficiency is validated on the standard images like Peppers, Lake, Lena, Elaine, Cameraman, Barbara, Baboon and airplane. As mentioned in table 1, the stego images were tested in dissimilar cover images and validated by means of MAE, MSE, entropy value, PSNR, NCC, SSIM, and UACI. By examining table 1, the proposed ECRT model achieved average MAE value of 0.235, MSE value of 0.19, Entropy value of 7.92, PSNR of 65.12 dB, UACI of 35.62%, NCC value of 0.996, and SSIM value of 0.996. The proposed ECRT model uses $f(x)$ to partition the secret images and to generate the shadow images. The obtained experimental results confirmed that the shadow images achieved satisfactory image quality with better security.

Table 1. Stego-images evaluated in dissimilar cover images

Images	MAE	MSE	Entropy value	PSNR (dB)	UACI (%)	NCC	SSIM
Peppers	0.34	0.11	7.98	60.98	36.12	0.996	0.999
Lake	0.25	0.12	7.88	63.90	34.60	0.995	0.996
Lena	0.12	0.24	7.87	62.80	35.66	0.996	0.995
Elaine	0.23	0.33	7.90	64.64	35.25	0.997	0.995
Cameraman	0.26	0.23	7.92	60.92	35.40	0.999	0.997
Barbara	0.35	0.22	7.94	67.93	36.58	0.997	0.998
Baboon	0.20	0.17	7.95	68.94	36.48	0.997	0.997
Airplane	0.13	0.14	7.96	70.90	34.90	0.996	0.997
Average	0.23	0.19	7.92	65.12	35.62	0.996	0.996

Table 2. Stego-images evaluated in dissimilar secret images

Images	MAE	MSE	Entropy value	PSNR (dB)	UACI (%)	NCC	SSIM
Peppers	0.32	0.15	7.91	62.90	35.40	0.997	0.998
Lake	0.24	0.16	7.89	64.96	36.64	0.998	0.998
Lena	0.14	0.22	7.89	65.94	34.48	0.998	0.999
Elaine	0.26	0.38	7.92	65.17	34.45	0.999	0.997
Cameraman	0.27	0.24	7.94	62.94	34.49	0.998	0.997
Barbara	0.32	0.26	7.97	64.90	34.56	0.998	0.999
Baboon	0.27	0.18	7.98	68.12	35.45	0.999	0.996
Airplane	0.14	0.17	7.98	67.92	35.58	0.999	0.998
Average	0.24	0.22	7.93	65.35	35.13	0.998	0.997

Table 3. Experimental results of ECRT model under different attacks

Images	Performance measures	Normal	Histogram equalization	Crop attacks		Noise attacks	
						SP noise	Gaussian
				20%	30%	10%	10%
Lake as cover image	PSNR (dB)	63.90	58.16	59.10	57.30	54.06	53.26
	SSIM	0.996	0.995	0.995	0.995	0.995	0.995
	NCC	0.995	0.995	0.995	0.995	0.995	0.995
	Entropy	7.88	6.50	6.53	6.23	5.59	5.59
	UACI (%)	34.60	33.48	33.43	33.43	33.43	33.42
	MSE	0.12	0.24	0.32	0.34	0.28	0.29
	MAE	0.25	0.32	0.38	0.36	0.34	0.34
Lake as secret image	PSNR (dB)	64.96	63.47	58.04	51.10	56.06	56.07
	SSIM	0.998	0.989	0.980	0.954	0.988	0.988
	NCC	0.998	0.998	0.993	0.988	0.997	0.998
	Entropy	7.89	7.88	7.52	7.48	7.45	7.48
	UACI (%)	36.64	34.45	33.48	33.48	33.47	33.47
	MSE	0.16	0.34	0.44	0.32	0.30	0.28
	MAE	0.24	0.28	0.29	0.30	0.29	0.28

Correspondingly, in Table 2, the stego images tested in dissimilar secret images, and the results are evaluated using MAE, MSE, entropy value, PSNR, NCC, SSIM, and UACI. By viewing Table 2, the proposed ECRT model has achieved average MAE value of 0.24, MSE value of 0.22, Entropy value of 7.93, PSNR of 65.35 dB, UACI of 35.13%, NCC value of 0.998, and SSIM value of 0.997. The proposed ECRT model utilizes the LSB substitution approach for embedding the shadow images into the cover images that generate useful stego images. In this article, the LSBs of cover image are stored in $f(x)$ such that the cover image is recovered losslessly after extraction of the secret image.

In addition, Table 3 describes the experimental results of the proposed ECRT model for both secret and cover images. In this scenario, the performance investigation is carried out in four different conditions such as histogram equalization, normal scenario, with noise attacks (10% salt and pepper noise and 10% Gaussian noise), and crop attacks (20% and 30%). By inspecting table 3, the proposed ECRT model achieved effective experimental results even under the conditions of crop attacks, noise attacks and histogram equalization in light of PSNR, NCC, SSIM, UACI, MSE, entropy, and MAE (particularly Lake as cover and secret image).

4.1. Comparative analysis

The comparative investigation between the ECRT model and the state-of-the-art models is stated in Table 4 to 6. Shankar [14] utilized an optimal homomorphic encryption model for an effective SIS. At first, the DWT technique was applied to a secret image for generating sub-bands that create multiple shadow images. Then, the oppositional-based harmony search approach and homomorphic encryption technique were employed for encrypting and decrypting the shadow images that improve the security by generating the optimal keys. The experimental results showed that the ECRT model obtained effective performance compared to the existing model on a few standard multimedia images by means of PSNR, NCC, MSE, entropy and MAE, especially on stego images as secret images, as detailed in Table 4.

Table 4. Comparative result between the proposed and the existing model in terms of PSNR, NCC, MSE, entropy and MAE

Images	Models	PSNR (dB)	NCC	MSE	Entropy	MAE
Lena	DWT- Harmony search [14]	52.21	0.990	0.28	7.69	0.36
	ECRT	65.94	0.998	0.22	7.89	0.14
Baboon	DWT- Harmony search [14]	51.20	0.850	0.21	7.05	0.30
	ECRT	68.12	0.999	0.18	7.98	0.27
Barbara	DWT- Harmony search [14]	52.20	0.930	0.25	7.68	0.42
	ECRT	64.90	0.998	0.26	7.97	0.32
Peppers	DWT- Harmony search [14]	51.89	0.970	0.25	7.55	0.45
	ECRT	62.90	0.997	0.15	7.91	0.32

Table 5. Comparative result between the proposed and the existing model in terms of PSNR

Images	PSNR (dB) (cover)		PSNR (dB) (secret)	
	CRT [18]	ECRT	CRT [18]	ECRT
Peppers	44.16	60.98	44.16	62.90
Lake	44.13	63.90	44.15	64.96
Elaine	44.13	64.64	44.18	65.17
Cameraman	44.13	60.92	44.14	62.94
Barbara	44.13	67.93	44.16	64.90
Airplane	44.14	70.90	44.15	67.92

Table 6. Comparative result between the proposed and the existing model in terms of entropy

Images	Entropy values	
	Polynomial-based SIS [13]	ECRT
Lena	7.59	7.89
Baboon	7.46	7.98
Bird	7.53	7.90

Meng [18] introduced a novel SIS model based on CRT that utilizes polynomials to partition the secret image and then LSB technique was used to generate stego images and to hide the shadow images. The extensive experiments showed that the ECRT model achieved significant SIS performance compared to the conventional CRT model by means of PSNR. In this literature, the experimental investigations were accomplished on the stego images and it is tested in dissimilar cover and secret images, as stated in Table 5. M.K. Sardar and A. Adhikari, [13] presented a new polynomial-based SIS approach which transforms the secret color images into shadow images that precisely reconstructs the original secret image without any distortions. Compared to this existing approach, the proposed ECRT model achieved better performance in terms of information entropy, as mentioned in table 6.

The obtained experimental results showed that the ECRT model attained superior SIS performance and significantly highlighted the concerns mentioned in the related works section such as better visual performance and image quality, and recovers the secret images losslessly.

5. Conclusion

In this manuscript, a new ECRT model is proposed for an effective SIS, where the proposed ECRT model utilizes the LSB pixels in secret and cover images for constructing $f(x)$ over $F_2(x)$. The sharing polynomial $f(x)$ partition the secret images and creates the shadow images. Further, the LSB substitution technique is applied for embedding the shadow images into the cover images for generating useful stego images. Generally, the conventional data hiding methods work based on LSB substitution techniques, which are irreversible, so the LSB pixels in the cover images are lost. To highlight this issue, in the ECRT model, the LSB pixels in the cover image are stored in a sharing polynomial $f(x)$. In addition, the lossless stego images t are utilized for reconstructing $f(x)$ by an ECRT model, where LSB pixels in secret and cover images are extracted from a sharing polynomial $f(x)$. Finally, both cover and secret images are recovered losslessly, and the ECRT model's performance is validated in terms of PSNR, NCC, SSIM, UACI, MSE, entropy, and MAE. The experimental outcome showed that the proposed ECRT model obtained effective performance in SIS related to the existing models even under the conditions of crop attacks, noise attacks, and histogram equalization. As seen in the resulting section, the proposed ECRT model almost showed 20 to 25% improvement in PSNR value related to the comparative models: CRT, Polynomial-based SIS, and DWT- Harmony search. As a future extension, a new innovative swarm optimization algorithm can be developed to further improve the security level of medical and identity images.

Conflicts of Interest

The authors declare no conflict of interest.

Author Contributions

The paper background work, conceptualization, methodology, dataset collection, implementation, result analysis and comparison, preparing and editing draft, visualization have been done by first and second author. The supervision, review of work and project administration, have been done by third author.

References

[1] J. Yuan and L. Li, "A fully dynamic secret sharing scheme", *Information Sciences*, Vol. 496, pp. 42-52, 2019.

[2] X. Yan, Q. Gong, L. Li, G. Yang, Y. Lu, and J. Liu, "Secret image sharing with separate shadow authentication ability", *Signal Processing: Image Communication*, Vol. 82, p. 115721, 2020.

[3] Z. Wu, Y. Liu, and X. Jia, "A novel hierarchical secret image sharing scheme with multi-group joint management", *Mathematics*, Vol. 8, No. 3, p. 448, 2020.

[4] P. Li, Z. Liu, and C. N. Yang, "A construction method of (t, k, n)-essential secret image sharing scheme", *Signal Processing: Image Communication*, Vol. 65, pp. 210-220, 2018.

[5] Y. X. Liu, C. N. Yang, S. Y. Wu, and Y. S. Chou, "Progressive (k, n) secret image sharing schemes based on Boolean operations and covering codes", *Signal Processing: Image Communication*, Vol. 66, pp. 77-86, 2018.

[6] L. Xiong, X. Zhong, and C. N. Yang, "DWT-SISA: a secure and effective discrete wavelet transform-based secret image sharing with authentication", *Signal Processing*, Vol. 173, p. 107571, 2020.

[7] S. Kabirirad and Z. Eslami, "Improvement of (n, n)-multi-secret image sharing schemes based on Boolean operations", *Journal of Information Security and Applications*, Vol. 47, pp. 16-27, 2019.

[8] S. Kabirirad and Z. Eslami, "A (t, n)-multi secret image sharing scheme based on Boolean operations", *Journal of Visual Communication and Image Representation*, Vol. 57, pp. 39-47, 2018.

[9] Y. X. Liu, C. N. Yang, Y. S. Chou, S. Y. Wu, and Q. D. Sun, "Progressive (k, n) secret image sharing scheme with meaningful shadow images by GEMD and RGEMD", *Journal of Visual Communication and Image Representation*, Vol. 55, pp. 766-777, 2018.

[10] X. Yan, Y. Lu, L. Liu, and S. Wang, "Partial secret image sharing for (k, n) threshold based on image inpainting", *Journal of Visual Communication and Image Representation*, Vol. 50, pp. 135-144, 2018.

[11] A. M. Ahmadian and M. Amirmazlaghani, "A novel secret image sharing with steganography scheme utilizing optimal asymmetric encryption padding and information dispersal algorithms", *Signal Processing: Image Communication*, Vol. 74, pp. 78-88, 2019.

[12] P. Li, C. N. Yang, and Q. Kong, "A novel two-in-one image secret sharing scheme based on perfect black visual cryptography", *Journal of Real-Time Image Processing*, Vol. 14, pp. 41-50, 2018.

[13] M. K. Sardar and A. Adhikari, "A new lossless secret color image sharing scheme with small shadow size", *Journal of Visual Communication and Image Representation*, Vol. 68, p. 102768, 2020.

[14] K. Shankar, M. Elhoseny, R. S. Kumar, S. K. Lakshmanaprabu, and X. Yuan, "Secret image sharing scheme with encrypted shadow images using optimal homomorphic encryption technique", *Journal of Ambient Intelligence and Humanized Computing*, Vol. 11, No. 5, pp. 1821-1833, 2020.

[15] A. Nag, J. P. Singh, and A. K. Singh, "An efficient Boolean based multi-secret image sharing scheme", *Multimedia Tools and Applications*, Vol. 79, No. 23, pp. 16219-16243, 2020.

[16] X. Wu, C. N. Yang, Y. T. Zhuang, and S. C. Hsu, "Improving recovered image quality in secret image sharing by simple modular arithmetic", *Signal Processing: Image Communication*, Vol. 66, pp. 42-49, 2018.

[17] L. Tan, Y. Lu, X. Yan, L. Liu, and L. Li, "Weighted Secret Image Sharing for a (k, n) Threshold Based on the Chinese Remainder Theorem", *IEEE Access*, Vol. 7, pp. 59278-59286, 2019.

[18] K. Meng, F. Miao, Y. Xiong, and C. C. Chang, "A reversible extended secret image sharing scheme based on Chinese remainder theorem", *Signal Processing: Image Communication*, Vol. 95, p. 116221, 2021.

[19] X. Yan, Y. Lu, L. Liu, J. Liu, and G. Yang, "Chinese remainder theorem-based two-in-one image secret sharing with three decoding options", *Digital Signal Processing*, Vol. 82, pp. 80-90, 2018.

[20] W. Ding, K. Liu, X. Yan, H. Wang, L. Liu, and Q. Gong, "An image secret sharing method based on matrix theory", *Symmetry*, Vol. 10, p. 530, 2018.