

## RESEARCH ARTICLE

# An Efficient Multi-Secret Image Sharing System Based on Chinese Remainder Theorem and Its FPGA Realization

BISHOY K. SHAROBIM<sup>1</sup>, MARWAN A. FETTEHA<sup>1</sup>,  
SALWA K. ABD-EL-HAFIZ<sup>2</sup>, (Senior Member, IEEE), WAFAA S. SAYED<sup>2</sup>,  
LOBNA A. SAID<sup>1</sup>, (Senior Member, IEEE),  
AND AHMED G. RADWAN<sup>2,3</sup>, (Senior Member, IEEE)

<sup>1</sup>Nanoelectronics Integrated Systems Center (NISC), Nile University, Giza 12588, Egypt

<sup>2</sup>Engineering Mathematics Department, Faculty of Engineering, Cairo University, Giza 12613, Egypt

<sup>3</sup>School of Engineering and Applied Sciences, Nile University, Giza 12588, Egypt

Corresponding author: Wafaa S. Sayed (wafaa.s.sayed@eng.cu.edu.eg)

This work was supported by the Science, Technology, and Innovation Funding Authority (STIFA), Egypt, under Grant #45631.

**ABSTRACT** Multi-Secret Image Sharing (MSIS) is important in information security when multiple images are shared in an unintelligible form to different participants, where the images can only be recovered using the shares from participants. This paper proposes a simple and efficient  $(n, n)$ -MSIS system for colored images based on XOR and Chinese Remainder Theorem (CRT), where all the  $n$  share are required in the recovery. The system improves the security by adding dependency on the input images to be robust against differential attacks, and by using several delay units. It works with even and odd number of inputs, and has a long sensitive system key design for the CRT. Security analysis and a comparison with related literature are introduced with good results including statistical tests, differential attack measures, and key sensitivity tests as well as performance analysis tests such as time and space complexity. In addition, Field Programmable Gate Array (FPGA) realization of the proposed system is presented with throughput 530 Mbits/sec. Finally, the proposed MSIS system is validated through software and hardware with all statistical analyses and proper hardware resources with low power consumption, high throughput and high level of security.

**INDEX TERMS** Chinese remainder theorem, field programmable gate array, multi-secret image sharing, secret sharing.

## I. INTRODUCTION

The development of effective methods for information security lead to the emergence of secret sharing that was proposed by Shamir [1], and later Secret Image Sharing (SIS), which is used to share an image in the form of  $n$  shares/shadows [2]. A threshold defines how many shares out of the  $n$  shares are needed to recover the secret.  $(k, n)$ -SIS requires  $k$  or more shares to recover the secret, while  $(n, n)$ -SIS requires all the shares to recover the secret [3].

Recent literature on SIS uses different methods, where the most common methods are polynomial-based secret sharing

The associate editor coordinating the review of this manuscript and approving it for publication was Shuangqing Wei<sup>1</sup>.

and the Chinese Remainder Theorem (CRT). Gong et al. proposed  $(k, n)$ -SIS, for color images using polynomial-based secret sharing [4]. Patil and Purushothama proposed a  $(k, n)$ -SIS system for grayscale images, producing shares with a fixed size of  $23 \times 23$  [5]. Li et al. proposed another  $(k, n)$ -SIS based on the CRT for grayscale images with shares of the same size as the original image, while Chen et al. proposed  $(k, n)$ -SIS based on CRT with size of shares equal to  $1/k$  of the original image size [6]. Yan et al. also used CRT to share grayscale images with lossless recovery [7]. Others used steganography techniques to embed the shares inside cover images to make them less suspicious [8], [9]. Liu et al. proposed a multiple-level SIS, where participants have different levels and higher priority participants can

reveal more information [10]. Cheng et al. used shares in the shape of Quick Response (QR) codes, which do not raise suspicion [11]. While sharing one image is enough for some applications, other applications require multiple images sharing with increased security by building a dependency between the secret images.

Furthermore, Multi-Secret Image Sharing (MSIS) was introduced, where multiple images are shared at the same time instead of only one image. In recent  $(n, n)$ -MSIS systems, multiple methods of secret sharing are used. Sridhar and Sudha used a random grid approach to share two images as circular shape shares instead of rectangular shape [12], and Liu et al. combined it with polynomial-based SIS [13]. Another method is the XOR-based MSIS, where a mask is created from the secret images by XORing them and using a masking function, where CRT is the commonly used masking function [14]. The mask is then XORed with each of the secret images to create the shared images. In recovery, the mask is recovered by XORing the shared images, but it was restricted to an even number of input images.

Additional research on MSIS tried to increase the security and remove the restriction of an even number of inputs without changing the CRT masking function. Prasetyo et al. added a random image to the inputs to make them even, and encrypted input images using chaotic maps to increase the security of the system [15]. Prasetyo and Hesia used generalized chaotic scrambling on input images to ensure that the inputs to the MSIS module are even [16]. Prasetyo and Guo used chaotic scrambling on input images before the CRT [17]. Additionally, Guo et al. improved the security by using two masks and added beta chaotic map to perform confusion and diffusion on input images [18]. Those discussed systems only used CRT to create a mask from the modified and XORed input images. Accordingly, the masking function is a good candidate for enhancements to improve security. Sharobim et al. proposed an  $(n, n)$ -MSIS system based on CRT and S-box, where they used SHA-256 to build dependency on the secret images and added S-box after CRT [19].

Field Programmable Gate Arrays (FPGAs) are advantageous to general purpose computers because of their low power consumption, high throughput, design flexibility, low development per-unit costs, high speed, immunity to noise and a high degree of security [20], [21], [22], [23], [24], [25]. In addition, making portable, compact systems is made possible by a chip's ability to be programmed [26]. Hence, this encourages their utilization for optimized digital realizations of information security systems [25]. Specifically, few researchers implemented secret sharing systems on FPGA. In [27], the authors constructed a modified secret sharing strategy based on matrix projections and neural networks. The design used parallel hardware architecture and was tested on Virtex 6 XC6VLX760. Their implementation reduced memory requirements to store precalculated constants by 16 times through switching from a finite simple Galois field

to a complex field. In [28], the authors utilized cloud of clouds for a secret sharing system. This approach makes the system accessible over the network. The system was implemented on Xilinx Zynq-7000 AP SoC XC7Z020-CLG484. The proposed design uses Multi-Party Computation (MPC), which allows data from multiple sources to be used in secure computation. This keeps the original data protected and only displays the result, which facilitates shared use of data sets gathered by various entities.

This paper proposes an MSIS system, which increases the system security by adding levels of encryption to the masking function along with the CRT, without manipulating the secret images with complicated operations. The proposed system is simple, efficient, and works with different image sizes and number of shares, in addition to having a novel design of a long and sensitive system key for the CRT. The FPGA implementation provides low power consumption, high throughput, high speed, and high level of security. In addition to using the security analysis tests that are commonly used in the MSIS literature, more security and performance analysis tests are used to evaluate the proposed system. The results and comparisons demonstrate the efficiency and improved security of the system.

The remainder of this section describes the necessary background for XOR-based MSIS and CRT. The following section presents the proposed  $(n, n)$ -MSIS system, while Section III describes its hardware implementation on FPGA. Section IV gives the security analysis results, and Section V discusses the performance analysis results. Section VI presents comparisons with previous schemes, and finally, Section VII gives the conclusions and future research directions.

### A. XOR-BASED MSIS AND CRT

In the XOR-based MSIS system in [14], the generation stage works as:

$$M = CRT(I_1 \oplus I_2 \oplus \dots \oplus I_n), \quad (1a)$$

$$S_i = I_i \oplus M, \quad i = 1, 2, \dots, n, \quad (1b)$$

where  $M$  is the mask,  $I_1, I_2, \dots, I_n$  are the secret images, and  $S_1, S_2, \dots, S_n$  are the shared images. In the recovery stage, the recovered images,  $R_1, R_2, \dots, R_n$ , are recovered using:

$$M_r = CRT(S_1 \oplus S_2 \oplus \dots \oplus S_n) = M, \quad (2a)$$

$$R_i = S_i \oplus M_r, \quad i = 1, 2, \dots, n, \quad (2b)$$

where the recovery is lossless ( $M_r = M$ ) for an even value of  $n$ . The CRT encrypts color images by solving the following system of congruences for each pixel:

$$x \equiv R \pmod{k_1}, \quad (3a)$$

$$x \equiv G \pmod{k_2}, \quad (3b)$$

$$x \equiv B \pmod{k_3}, \quad (3c)$$

where  $R, G$ , and  $B$  are the pixel values for the red, green, and blue channels, respectively, and  $k_1, k_2$ , and  $k_3$  are pairwise

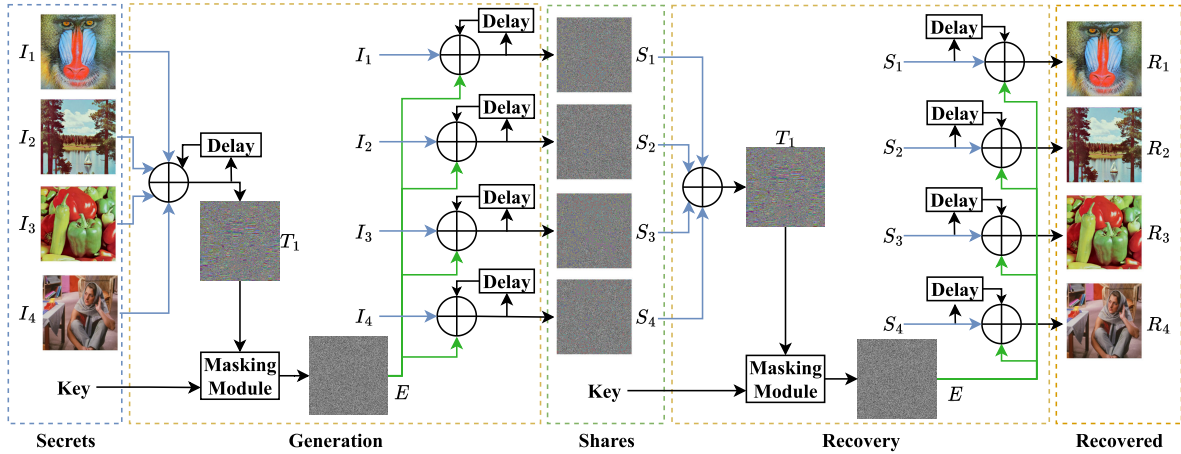


FIGURE 1. Block diagram of the proposed system for even  $n$ .

relatively prime subkeys. The steps for solving the system of congruences using CRT are [29]:

$$P = k_1 \times k_2 \times k_3, \quad (4a)$$

$$P_i = P/k_i, \quad i = 1, 2, 3, \quad (4b)$$

$$P_R = P_1(P_1^{-1} \bmod k_1), \quad (4c)$$

$$P_G = P_2(P_2^{-1} \bmod k_2), \quad (4d)$$

$$P_B = P_3(P_3^{-1} \bmod k_3), \quad (4e)$$

$$x = (R \times P_R + G \times P_G + B \times P_B) \bmod P. \quad (4f)$$

## II. PROPOSED SYSTEM

The proposed  $(n,n)$ -MSIS system uses several delay units and modifies the masking module by adding dependency on the input images to increase the security. The system includes two main generation and recovery schemes, which utilize a common masking module,  $\mathfrak{J}$ . The proposed system works for both even and odd number of input images,  $n$ . Figure 1 shows the system in case of even  $n$ , where in generation, the secret images  $\{I_1, I_2, \dots, I_n\}$  are XORed together, with delay, to get the image  $T_1$  represented as:

$$T_1(j) = I_1(j) \oplus I_2(j) \oplus \dots \oplus I_n(j) \oplus T_1(j-1), \quad (5)$$

where all equations are applied to the R, G, and B channels of each pixel,  $1 \leq j \leq HW$ , and  $H$  and  $W$  are the height and width of the images, respectively. At  $j = 0$ , the value of  $T_1$  is assumed to be 0.  $T_1$  is then used as input to the masking module  $\mathfrak{J}$ , along with the system key, to generate the mask image  $E$  as:

$$E(j) = \mathfrak{J}(T_1(j)), \quad (6)$$

The masking module,  $\mathfrak{J}$ , is shown in Fig. 2, and it includes the following three steps:

$$P_{sum} = \sum_{j=1}^{WH} T_1(j), \quad (7a)$$

$$T_2(j) = (T_1(j) + P_{sum}) \bmod 256, \quad (7b)$$

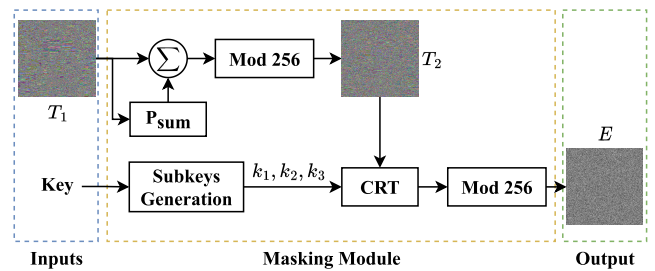


FIGURE 2. Block diagram of the proposed masking module.

$$E(j) = \text{CRT}(T_2(j)) \bmod 256. \quad (7c)$$

An addition  $\bmod 256$  is used to preserve the 8 bits for each channel and  $P_{sum}$  is used to create sensitivity where any small change in  $T_1$  leads to a totally different  $T_2$ . Finally, the CRT, which is described in Eqs. (3) and (4), is used to encrypt  $T_2$  and get the mask  $E$ .

Since the CRT requires that the subkeys  $k_1$ ,  $k_2$ , and  $k_3$  be pairwise relatively prime integers, the following method is designed to generate them from a single integer  $K$ . First, a unity bit is concatenated to the right of the input key  $K$ , which can be of any length, leading to the first odd subkey,  $k_1$ . Next,  $k_2$  and  $k_3$  are generated such that  $k_2 = k_1 + 1$  and  $k_3 = k_1 + 2$ . Using the Euclidean algorithm, it can be easily proven that the three subkeys generated in this manner are pairwise relatively prime [29]. Having one key for the system is more secure, sensitive, and user-friendly than having multiple keys. Since  $P_R$ ,  $P_G$ ,  $P_B$  and  $P$  in Eq. (4f) are calculated from  $k_1$ ,  $k_2$ , and  $k_3$  and are the same for all the image pixels, they are calculated once in the system, which make the system faster and more efficient.

After finding  $x$  using the CRT, its value is reduced  $\bmod 256$  and saved in the three channels of the corresponding pixel in the mask image  $E$ . Finally,  $E$  is XORed with each of the secret images, with delay, to generate the shared images

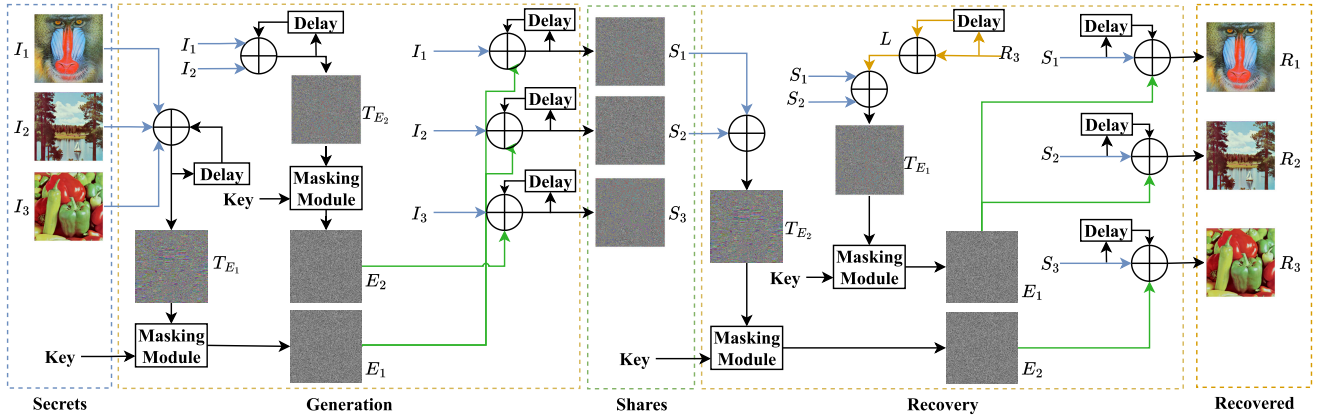


FIGURE 3. Block diagram of the proposed system for odd  $n$ .

$\{S_1, S_2, \dots, S_n\}$  as:

$$S_i(j) = I_i(j) \oplus E(j) \oplus S_i(j-1), \quad i = 1, 2, \dots, n, \quad (8)$$

where the value of  $S_i$  is assumed to be 0 at  $j = 0$ . The delay is added to improve the system security because every pixel from the input secret images affects all upcoming pixels of  $T_1$  [30]. Moreover, every input and masking pixel affects all upcoming pixels of the shares.

In the recovery scheme for even  $n$ , the shares are XORed together to get the image  $T_1$  that is used as input to the masking module, along with the system key, to recover the mask image  $E$ . Finally,  $E$  is XORed with each of the shared images, with delay on  $S_i$ , to get the recovered secret images  $\{R_1, R_2, \dots, R_n\}$  using:

$$R_i(j) = S_i(j) \oplus E(j) \oplus S_i(j-1), \quad i = 1, 2, \dots, n. \quad (9a)$$

The system for odd number of images  $n$  is shown in Fig. 3, where two masks  $\{E_1, E_2\}$  are used by adapting the method proposed in [17] to incorporate the effect of delay as follows. In the generation scheme:

$$T_{E_1}(j) = I_1(j) \oplus I_2(j) \oplus \dots \oplus I_n(j) \oplus T_{E_1}(j-1), \quad (10a)$$

$$E_1(j) = \mathfrak{J}(T_{E_1}(j)), \quad (10b)$$

$$T_{E_2}(j) = I_1(j) \oplus I_2(j) \oplus \dots \oplus I_{n-1}(j) \oplus T_{E_2}(j-1), \quad (10c)$$

$$E_2(j) = \mathfrak{J}(T_{E_2}(j)), \quad (10d)$$

$$S_i(j) = I_i(j) \oplus E_1(j) \oplus S_i(j-1), \quad i = 1, 2, \dots, n-1, \quad (10e)$$

$$S_n(j) = I_n(j) \oplus E_2(j) \oplus S_n(j-1). \quad (10f)$$

In the recovery scheme:

$$T_{E_2}(j) = S_1(j) \oplus S_2(j) \oplus \dots \oplus S_{n-1}(j), \quad (11a)$$

$$E_2(j) = \mathfrak{J}(T_{E_2}(j)), \quad (11b)$$

$$R_n(j) = S_n(j) \oplus E_2(j) \oplus S_n(j-1), \quad (11c)$$

$$L(j) = L(j-1) \oplus R_n(j), \quad (11d)$$

$$T_{E_1}(j) = S_1(j) \oplus S_2(j) \oplus \dots \oplus S_{n-1}(j) \oplus L(j), \quad (11e)$$

$$E_1(j) = \mathfrak{J}(T_{E_1}(j)), \quad (11f)$$

$$R_i(j) = S_i(j) \oplus E_1(j) \oplus S_i(j-1), \quad i = 1, 2, \dots, n-1. \quad (11g)$$

### III. HARDWARE IMPLEMENTATION

This section illustrates the hardware architecture for the generation and the recovery schemes, where the input images are stored in 4 block RAMs  $I_1, I_2, I_3$  and  $I_4$  in case of the generation and  $S_1, S_2, S_3$  and  $S_4$  in case of the recovery. Each block RAM has 24 bits data width and 65536 memory depth to store a  $256 \times 256$  RGB image.

#### A. GENERATION SCHEME

The generation scheme, shown in Fig. 4(a), consists of 3 stages. The first stage involves bit-wise XORING the four images as well as the previous  $T_1$ . The total of each channel of  $T_1$  is accumulated in the 8-bit register  $P_{sum}$  until the block RAM's end is reached. Then  $P_{sum}$  is added to each of the channels of  $T_1$  after it has been regenerated.

The subkeys  $k_1, k_2$  and  $k_3$  in Eq. (4a) are used to calculate the 390-bit registers  $P_R, P_G, P_B$  and  $P$ . Then, the CRT in Eq. (4f) is applied and the result's least significant byte is saved in the  $8 \times 65536$  block RAM  $E$ .

In stage 2,  $I_1, I_2, I_3$ , and  $I_4$  are XORed with  $S_1, S_2, S_3$  and  $S_4$ , respectively and with the corresponding location in  $E$ . In stage 3, each of  $S_1, S_2, S_3$  and  $S_4$  are buffered and sent to the PC using Universal Asynchronous Receiver-Transmitter (UART).

#### B. RECOVERY SCHEME

The recovery scheme is show in Fig. 4(b), where in stage 1, the register Delay does not exist. As for stage 2, the register Delay holds the value of the inputs, i.e., secret shares, and there are no changes in stage 3.

#### C. EXPERIMENTAL VALIDATION

Each scheme is realized in Verilog hardware description language and implemented on Genesys2 XC7K325TFFG900-2 FPGA [31]. The schemes operates at a maximum frequency of 22.09 MHz with a throughput of 530 Mbit/s. The generated



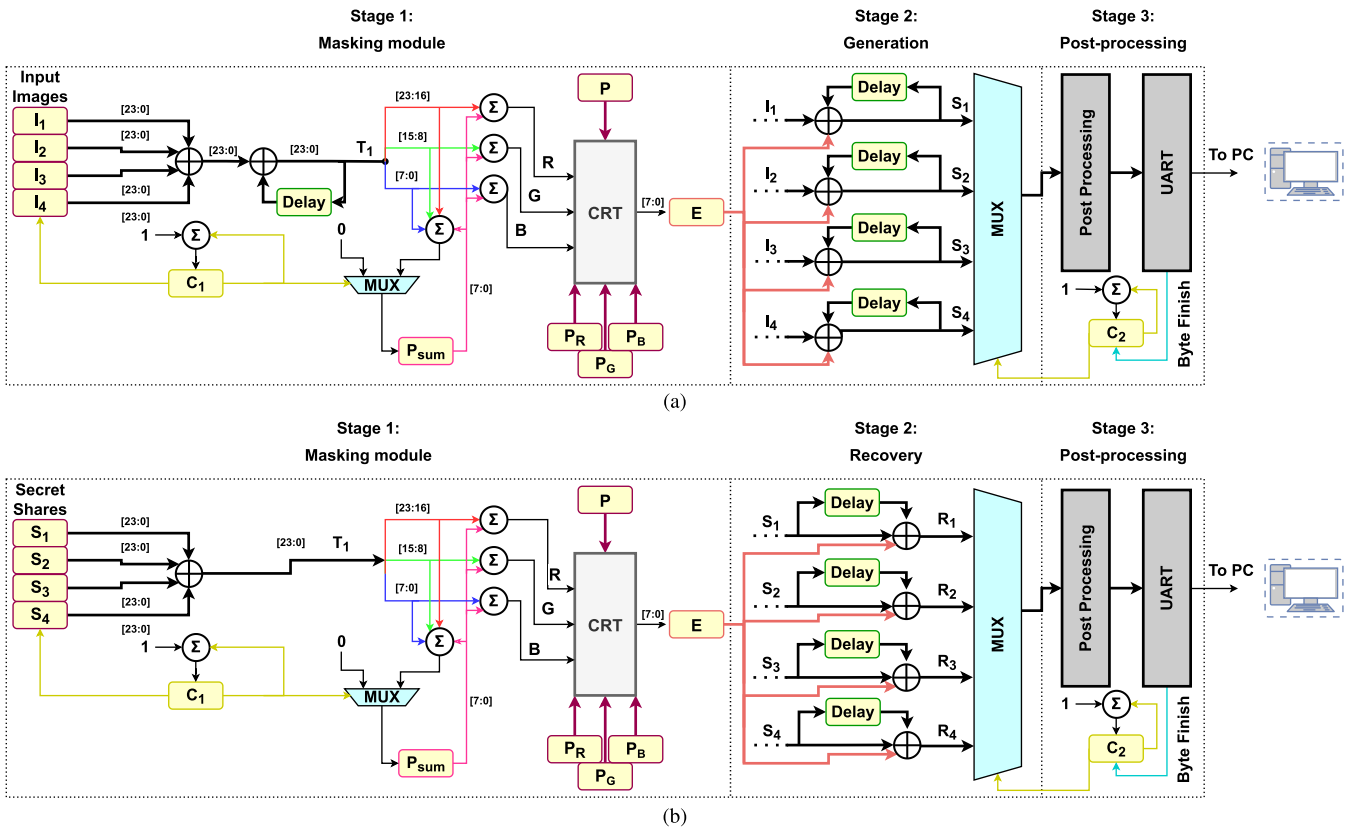


FIGURE 4. Hardware architecture of (a) generation and (b) recovery schemes.

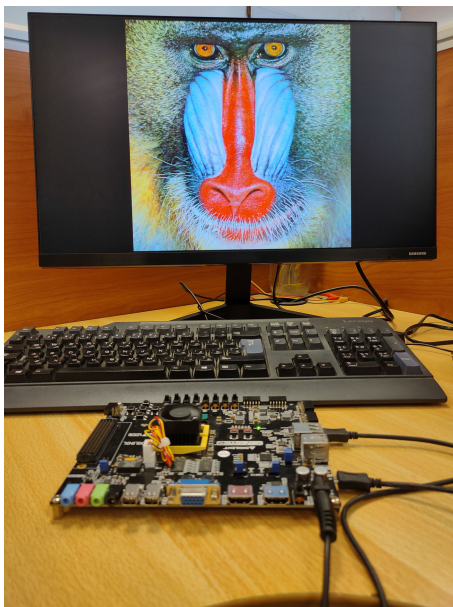


FIGURE 5. FPGA setup.

bit-stream is sent over a UART channel so that each output image from the generation and recovery schemes is compared to the output of the corresponding software according to the setup in Fig. 5.

TABLE 1. Generation and recovery schemes hardware resources utilization.

Resources	Generation		Recovery	
	Util.	Util. %	Util.	Util. %
Lookup Tables (LUTs)	5864	2.88	5830	2.86
Flip Flops (FFs)	413	0.1013	389	0.0954
Block RAMs (BRAMs)	192	43.15	192	43.15
Digital Signal Processors (DSPs)	69	8.21	69	8.21

The hardware resources utilization of the generation and recovery schemes are given in Table 1, which shows that both schemes have almost the same utilization.






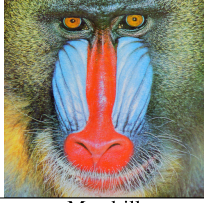



#### IV. SECURITY ANALYSIS

This section discusses the security analysis results of the proposed system using secret images of sizes  $256 \times 256$ ,  $512 \times 512$ , and  $1024 \times 1024$  as shown in Table 2 [32], and the 128-bit key

$$(A0\ 80\ B6\ 74\ 68\ 09\ AA\ 70\ 85\ E7\ AF\ B9\ E5\ 5F\ 74\ B8)_{16}.$$

The system was tested on (2,2), (3,3), and (4,4) thresholds, where the images  $\{b, e\}$ ,  $\{a, c, e\}$ ,  $\{a, b, c, d\}$  are used for each threshold, respectively. In the case of (4,4)-threshold for  $512 \times 512$  images, the used four secret images are shown in Fig. 6(a)–(d), and the secret shares generated are shown in Fig. 6(e)–(h).

TABLE 2. Used images from the USC-SIPI database [32].

Code	<i>a</i>	<i>b</i>	<i>c</i>	<i>d</i>	<i>e</i>
Images of size 256×256					
Description	Female 1	Female 2	House	Tree	Jelly beans
Images of size 512×512					
Description	Mandrill	Lake	Peppers	Barbara	Splash
Images of size 1024×1024					
Description	San Diego 1	San Diego 2	San Francisco 1	San Francisco 2	Oakland

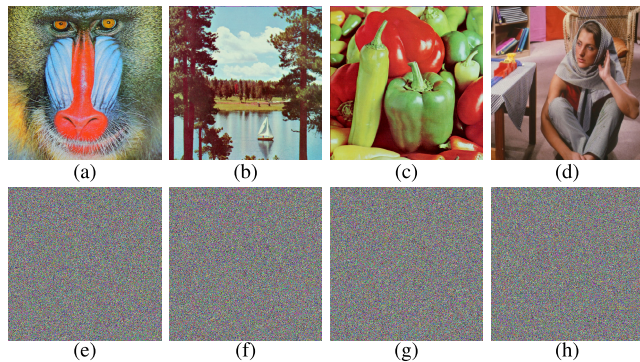


FIGURE 6. (a-d) Secret images ( $I_1, I_2, I_3, I_4$ ), and (e-h) shared images ( $S_1, S_2, S_3, S_4$ ) for  $512 \times 512$  images.

In the following subsections, the results of several statistical tests, such as histograms, entropy, Root Mean Square Error (RMSE), correlation coefficients, and adjacent pixels correlation are analyzed, where some of these tests are not commonly performed in the MSIS literature. Moreover, resistance to differential attacks and key sensitivity results are discussed.

A. STATISTICAL ANALYSIS RESULTS

The histogram of an image shows the distribution of pixel values across the whole image. In the case of (4,4)-threshold for  $512 \times 512$  images, the histograms of a plain image are non-uniform as shown in Fig. 7(a)-(c) for the three channels of the secret image,  $I_1$ . For a strong encryption system, the

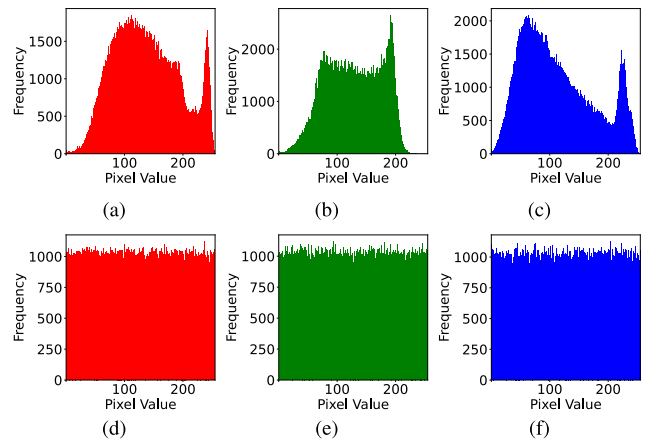


FIGURE 7. (a-c) Histograms of the image  $I_1$ , and (d-f) histograms of the share  $S_1$  of (4,4)-threshold for  $512 \times 512$  images.

histograms of encrypted images must be uniform [33]. The histograms of the three channels of the share  $S_1$  are shown in Fig. 7(d)-(f), where all the other shares show similar uniform histograms.

Entropy measures the randomness of image pixels and is measured using:

$$Entropy = - \sum_{i=0}^{255} P(i) \log_2 P(i), \tag{12}$$

where  $P(i)$  is the probability of the pixel value  $i$ . The encrypted images of a good encryption system should have entropy values close to 8 to eliminate the predictability [34].

**TABLE 3. Entropy of the secret images and shares of (4,4)-threshold for 512 × 512 images.**

Image	$I_1$	$I_2$	$I_3$	$I_4$	$S_1$	$S_2$	$S_3$	$S_4$
Entropy	7.7624	7.7622	7.6698	7.6385	7.9998			

Table 3 shows the entropy of the secret images and the shares, where the entropy of the shares approach the expected value of 8.

RMSE is used to measure the difference between two images  $x$  and  $y$  using:

$$RMSE = \sqrt{\frac{1}{W \times H} \sum_{i=1}^H \sum_{j=1}^W (x(i, j) - y(i, j))^2}, \quad (13)$$

where  $W$  and  $H$  are the width and height of the images, respectively, and zero RMSE means identical images [34].

Correlation is used to measure the degree of similarity between two vector variables  $x$  and  $y$  and it is calculated using:

$$Cov(x, y) = \frac{1}{n} \sum_{i=1}^n (x_i - \frac{1}{n} \sum_{i=j}^n x_j)(y_i - \frac{1}{n} \sum_{i=j}^n y_j), \quad (14a)$$

$$D(x) = \frac{1}{n} \sum_{i=1}^n (x_i - \frac{1}{n} \sum_{i=j}^n x_j)^2, \quad (14b)$$

$$\rho = \frac{Cov(x, y)}{\sqrt{D(x)}\sqrt{D(y)}}, \quad (14c)$$

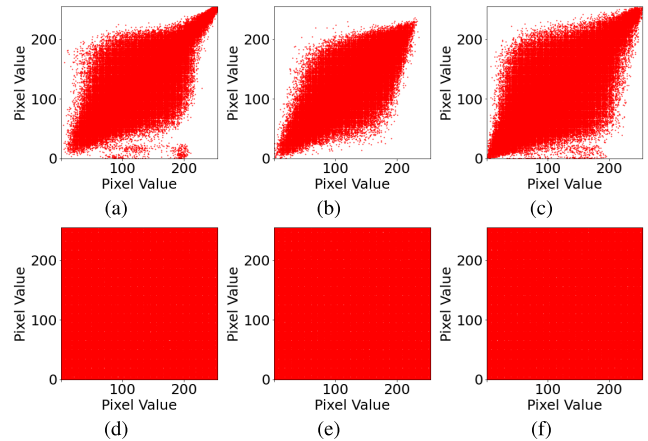
where  $n$  is the length of the two vectors,  $Cov$  is the covariance and  $\rho$  is the correlation coefficient. The range of correlation coefficient is  $[-1, 1]$ , where 0 means no correlation, and it is the desired value for a strong encryption system [34].

Table 4 shows the average results for different number of shares and image sizes. The entropy is near 8 which is the desired value, correlation tends to zero, and RMSE is high, which is an indication of good system security.

Correlation is also measured between adjacent pixels in horizontal, vertical, and diagonal directions [33]. Table 5 shows high correlations between pixel pairs in each direction and channel of the secret images, and the corresponding values for the secret shares approach zero. Figure 8 shows the scatter diagrams of the red channel in secret image  $I_1$  and share  $S_1$  across the three directions in the case of (4,4)-threshold with size of  $512 \times 512$ , whereas the other secret images and shares have similar diagrams in different directions and channels. The correlation results demonstrate the achieved weak correlation between adjacent pixels of the shares in all directions.

**B. RESISTANCE TO DIFFERENTIAL ATTACKS**

Differential attacks rely on observing the change in the encrypted image when a change is made in the original image. For a strong encryption system, a change of a bit in the original image must lead to a complete change in the encrypted image. The Number of Pixel Change Rate (NPCR) is used to



**FIGURE 8. Scatter diagrams of adjacent pixels correlation in vertical, horizontal, and diagonal directions of the red channel in (a)-(c) secret image  $I_1$ , and (d)-(f) shared image  $S_1$  of (4,4)-threshold for 512 × 512 images.**

measure the percentage of change between two images  $E_1$  and  $E_2$  and is calculated by:

$$D(i, j) = \begin{cases} 0 & \text{if } (E_1(i, j) = E_2(i, j)), \\ 1 & \text{if } (E_1(i, j) \neq E_2(i, j)) \end{cases} \quad (15a)$$

$$NPCR = \frac{1}{H \times W} \sum_{i=1}^H \sum_{j=1}^W D(i, j) \times 100\%, \quad (15b)$$

where  $W, H$  are the width and height of images, respectively, and  $E_1(i, j)$  is the pixel value at location  $(i, j)$  and a good encryption system must give values close to 99.61% [35]. Another metric is the Unified Average Changing Intensity (UACI) which measures the average difference of intensities between two images  $E_1$  and  $E_2$  and is calculated by:

$$UACI = \frac{1}{H \times W} \sum_{i=1}^H \sum_{j=1}^W \frac{|E_1(i, j) - E_2(i, j)|}{255}, \quad (16)$$

where a good encryption system must have values close to 33.46% [35].

The differential attack tests were performed by changing the Least Significant Bit (LSB) of a random pixel in a random channel of a random secret image. Then, NPCR and UACI are measured between shares generated from the original secret images and the shares  $MS_i$  generated from the modified secret images. The experiment was performed 200 times with randomly changed locations and the average values of NPCR and UACI are as required as shown in Table 6 for the case of (4,4)-threshold for  $512 \times 512$  images. It should be pointed out that UACI and NPCR were measured by the previous schemes as statistical measures between secret images and secret shares, which is conceptually similar to the information provided by the correlation and RMSE measures.

**C. KEY SPACE AND SENSITIVITY**

Any key size can be used in the proposed system, but a key size of 128 bits or more is required to resist brute-force



TABLE 4. Average statistical analysis results for different number of shares and image sizes.

Image Size	256×256			512×512			1024×1024			
	<i>n</i>	2	3	4	2	3	4	2	3	4
Entropy avg. ( $S_i$ ), $1 \leq i \leq n$		7.9990	7.9991	7.9991	7.9998	7.9998	7.9998	7.9999	7.9999	7.9999
RMSE avg. ( $I_i, S_i$ ), $1 \leq i \leq n$		93.47	98.75	98.31	103.25	99.83	96.57	91.09	92.64	88.17
RMSE avg. ( $S_i, S_j$ ), $1 \leq i, j \leq n, i \neq j$		104.61	104.68	104.47	104.58	104.45	104.48	104.48	104.45	105.79
Correlation avg. ( $I_i, S_i$ ), $1 \leq i \leq n$		0.00310	0.00264	0.00121	-0.00006	-0.00093	-0.00002	0.00003	-0.00022	-0.00010
Correlation avg. ( $S_i, S_j$ ), $1 \leq i, j \leq n, i \neq j$		-0.00060	-0.00202	-0.00011	-0.00096	0.00120	0.00020	0.00079	0.00081	-0.02514




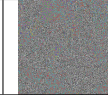
TABLE 5. Correlation of adjacent pixels in secret images and shares of (4,4)-threshold for 512 × 512 images.

Direction	Channel	Correlation							
		$I_1$	$I_2$	$I_3$	$I_4$	$S_1$	$S_2$	$S_3$	$S_4$
Vertical	Red	0.86607	0.96633	0.96633	0.96633	0.00174	-0.00133	0.00004	-0.00036
	Green	0.76522	0.98176	0.98176	0.98176	0.00011	0.00181	0.00173	-0.00112
	Blue	0.88095	0.96641	0.96641	0.96641	-0.00139	-0.00117	-0.00504	0.00169
Horizontal	Red	0.92227	0.96351	0.96351	0.96351	-0.00057	0.00074	0.00006	0.00170
	Green	0.86386	0.98110	0.98110	0.98110	0.00023	0.00138	0.00459	-0.00265
	Blue	0.90684	0.96648	0.96648	0.96648	0.00307	0.00042	-0.00030	0.00113
Diagonal	Red	0.85434	0.95638	0.95638	0.95638	0.00082	-0.00089	-0.00186	-0.00224
	Green	0.73480	0.96866	0.96866	0.96866	0.00446	0.00035	0.00199	0.00206
	Blue	0.83986	0.94779	0.94779	0.94779	0.00025	0.00185	-0.00217	-0.00023

TABLE 6. Measures for differential attacks in the case of (4,4)-threshold for 512 × 512 images.

Images	$S_1, MS_1$	$S_2, MS_2$	$S_3, MS_3$	$S_4, MS_4$
UACI %	33.45	33.46	33.47	33.46
NPCR %	99.49	99.49	99.51	99.49

TABLE 7. Key sensitivity results in the case of (4,4)-threshold for 512 × 512 images.

Image name	$MR_1$	$MR_2$	$MR_3$	$MR_4$
Image				
MSE	8640.48	10122.53	10124.52	8506.30

attacks [36]. The key space has a size of  $2^k$  where  $k$  is the number of bits of the used key. Key sensitivity is tested by changing the LSB of the key and measuring the Mean Squared Error (MSE) between the images recovered by the original key,  $R_i$ , and the images recovered by the modified key,  $MR_i$  [33]. The MSE is calculated using the square of Eq. (13). The key is sensitive as demonstrated by Table 7 giving the large MSE results and the images recovered by the modified key in the case of (4,4)-threshold for 512 × 512 images.

V. PERFORMANCE ANALYSIS

The time complexity of the proposed scheme depends on the dimensions of the secret images  $H \times W$ , where  $H$  and  $W$  are the height and the width of the images, respectively. The time complexity is  $\mathcal{O}(H \times W)$  because the proposed system only scans the images and performs constant-time operations on separate pixels. The space complexity also depends on the dimensions of secret images and, hence, it is  $\mathcal{O}(H \times W)$ . Table 8 shows average runtimes of 20 runs for

TABLE 8. Sample runtimes for different image sizes and numbers.

No. of images	Size	Gen. (S)	Rec. (S)	Total (S)
Even	2, 256 × 256	0.230	0.043	0.273
	4, 256 × 256	0.356	0.044	0.400
	2, 512 × 512	0.949	0.182	1.131
	4, 512 × 512	1.467	0.185	1.652
	2, 1024 × 1024	3.829	0.742	4.571
Odd	4, 1024 × 1024	5.936	0.753	6.689
	3, 256 × 256	0.396	0.163	0.559
	3, 512 × 512	1.639	0.685	2.324
	3, 1024 × 1024	6.666	2.792	9.458

different input numbers and dimensions using the system specifications (Windows 11, Intel Core i7-10750H CPU @ 2.60GHz, 15.8 GB RAM, Python programming language, and JupyterLab IDE). When the number of secret images is even,  $2n$ , the runtime is not significantly affected by increasing  $n$ . However, when the number of secret images is odd,  $2n + 1$ , the total runtime of generation and recovery is about double that of the  $2n$  case because the masking is performed twice. It should also be noted that the recovery time is less than the generation time because the direct XOR on the shares requires less computational power.

VI. COMPARISON

To compare the proposed system, the same images used in previous MSIS systems are used in the case of (4,4)-threshold. The previous systems only presented the results for (4,4)-threshold and size of 512 × 512. The comparison is with the previous schemes presented in [14], [15], [17], and [18], where some references presented several schemes, and the results of the last scheme in each reference is used in comparison.

Table 9 shows the RMSE between the secret images and the shares, and between the shares, where the proposed system



**TABLE 9.** RMSE between secret images and shares, and between shares compared to previous schemes.

Images		RMSE				
		Prop.	[14]	[15]	[17]	[18]
$I_i, S_i$	$I_1, S_1$	92.84	10.77	92.81	<b>92.85</b>	92.72
	$I_2, S_2$	<b>100.58</b>	10.58	100.04	100.04	100.04
	$I_3, S_3$	<b>100.56</b>	9.95	100.40	100.28	100.37
	$I_4, S_4$	92.30	9.45	92.36	92.21	<b>92.40</b>
$S_i, S_j$	$S_1, S_2$	<b>104.49</b>	10.61	101.90	103.87	101.81
	$S_1, S_3$	<b>104.25</b>	10.60	102.22	101.17	102.07
	$S_1, S_4$	<b>104.71</b>	10.54	100.54	102.90	100.46
	$S_2, S_3$	<b>104.61</b>	10.71	102.24	101.15	102.22
	$S_2, S_4$	<b>104.38</b>	10.49	102.09	102.93	102.12
	$S_3, S_4$	<b>104.44</b>	10.65	100.55	102.97	100.54

**TABLE 10.** Correlation between secret images and shares, and between shares compared to previous schemes.

Images		Correlation				
		Prop. 4 DP	[14] 4 DP	[15] 3 DP	[17] 2 DP	[18] 3 DP
$I_i, S_i$	$I_1, S_1$	-0.0006	-0.0023	<b>0.000</b>	0.00	0.001
	$I_2, S_2$	-0.0012	-0.0014	<b>0.000</b>	0.00	<b>0.000</b>
	$I_3, S_3$	0.0016	-0.0017	<b>-0.001</b>	0.00	<b>0.001</b>
	$I_4, S_4$	<b>0.0001</b>	-0.0004	-0.002	0.00	0.002
$S_i, S_j$	$S_1, S_2$	<b>-0.0004</b>	0.0276	0.050	0.01	0.051
	$S_1, S_3$	<b>0.0049</b>	0.0350	0.044	0.06	0.046
	$S_1, S_4$	<b>-0.0047</b>	0.0092	0.076	0.03	0.076
	$S_2, S_3$	<b>-0.0017</b>	-0.0123	0.043	0.06	0.044
	$S_2, S_4$	<b>0.0017</b>	0.1634	0.047	0.03	0.046
	$S_3, S_4$	<b>0.0014</b>	0.0416	0.075	0.03	0.076

results are comparable to or better than the previous schemes. Table 10 shows the correlation between the secret images and the shares, and between the shares, where the table demonstrates the good results of the proposed system compared to the previous schemes. It should be noted that some previous schemes only reported 2 or 3 Decimal Points (DP), which is insufficient as the results reported were 0.00 and 0.000.

## VII. CONCLUSION

This paper introduced a simple, secure and efficient (n,n)-MSIS system of colored images, by adding several delay units and input dependency to the commonly used CRT masking function. The system works with even and odd number of inputs, and a secure and sensitive key for the CRT was designed. The system was implemented on Genesys2 (XC7K325TFFG900-2) FPGA and operates at a maximum frequency of 22.09 MHz. The output bit stream of the FPGA implementation was verified against the software simulation.

The system successfully passed all security analysis tests that are used in previous literature, and also passed additional security and performance analysis tests. The FPGA implementation provides low power consumption, high throughput, high speed, and high level of security. In future work, further improvements can be made in which the number of output shares can be different from the number of secret images or other thresholds can be used.

## CONFLICT OF INTEREST

None of the authors have a conflict of interest to disclose.

## REFERENCES

- [1] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612–613, Nov. 1979.
- [2] C.-C. Thien and J.-C. Lin, "Secret image sharing," *Comput. Graph.*, vol. 26, no. 5, pp. 765–770, Oct. 2002.
- [3] D. R. Ibrahim, J. S. Teh, and R. Abdullah, "An overview of visual cryptography techniques," *Multimedia Tools Appl.*, vol. 80, nos. 21–23, pp. 31927–31952, Sep. 2021.
- [4] Q. Gong, Y. Wang, X. Yan, and L. Liu, "Efficient and lossless polynomial-based secret image sharing for color images," *IEEE Access*, vol. 7, pp. 113216–113222, 2019.
- [5] S. M. Patil and B. R. Purushothama, "Pixel co-ordinate-based secret image sharing scheme with constant size shadow images," *Comput. Electr. Eng.*, vol. 89, Jan. 2021, Art. no. 106937.
- [6] J. Chen, K. Liu, X. Yan, L. Liu, X. Zhou, and L. Tan, "Chinese remainder theorem-based secret image sharing with small-sized shadow images," *Symmetry*, vol. 10, no. 8, p. 340, Aug. 2018.
- [7] X. Yan, Y. Lu, L. Liu, and X. Song, "Reversible image secret sharing," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 3848–3858, 2020.
- [8] L. Xiong, X. Zhong, C.-N. Yang, and X. Han, "Transform domain-based invertible and lossless secret image sharing with authentication," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 2912–2925, 2021.
- [9] K. Gao, J.-H. Horng, and C.-C. Chang, "An authenticatable (2, 3) secret sharing scheme using meaningful share images based on hybrid fractal matrix," *IEEE Access*, vol. 9, pp. 50112–50125, 2021.
- [10] Y.-N. Liu, Q. Zhong, M. Xie, and Z.-B. Chen, "A novel multiple-level secret image sharing scheme," *Multimedia Tools Appl.*, vol. 77, no. 5, pp. 6017–6031, Mar. 2018.
- [11] Y. Cheng, Z. Fu, and B. Yu, "Improved visual secret sharing scheme for QR code applications," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 9, pp. 2393–2403, Sep. 2018.
- [12] S. Sridhar and G. F. Sudha, "Circular meaningful shares based (k, n) two in one image secret sharing scheme for multiple secret images," *Multimedia Tools Appl.*, vol. 77, no. 21, pp. 28601–28632, Nov. 2018.
- [13] L. Liu, Y. Lu, and X. Yan, "A novel (k1, k2, n)-threshold two-in-one secret image sharing scheme for multiple secrets," *J. Vis. Commun. Image Represent.*, vol. 74, Jan. 2021, Art. no. 102971.
- [14] M. Deshmukh, N. Nain, and M. Ahmed, "A novel approach for sharing multiple color images by employing Chinese remainder theorem," *J. Vis. Commun. Image Represent.*, vol. 49, pp. 291–302, 2017.
- [15] H. Prasetyo, C.-H. Hsia, and J.-Y. Deng, "Multiple secret sharing with simple image encryption," *J. Internet Technol.*, vol. 21, pp. 323–342, Jan. 2020.
- [16] H. Prasetyo and C.-H. Hsia, "Improved multiple secret sharing using generalized chaotic image scrambling," *Multimedia Tools Appl.*, vol. 78, no. 20, pp. 29089–29120, Aug. 2018.
- [17] H. Prasetyo and J.-M. Guo, "A note on multiple secret sharing using Chinese remainder theorem and exclusive-OR," *IEEE Access*, vol. 7, pp. 37473–37497, 2019.
- [18] J.-M. Guo, D. Riyono, and H. Prasetyo, "Improved beta chaotic image encryption for multiple secret sharing," *IEEE Access*, vol. 6, pp. 46297–46321, 2018.
- [19] B. K. Sharobim, S. K. Abd-El-Hafiz, W. S. Sayed, L. A. Said, and A. G. Radwan, "A unified system for encryption and multi-secret image sharing using S-box and CRT," in *Proc. 27th Int. Conf. Autom. Comput. (ICAC)*, Sep. 2022, pp. 1–6.
- [20] A. H. Elsafty, M. F. Tolba, L. A. Said, A. H. Madian, and A. G. Radwan, "Enhanced hardware implementation of a mixed-order nonlinear chaotic system and speech encryption application," *AEU-Int. J. Electron. Commun.*, vol. 125, Oct. 2020, Art. no. 153347.
- [21] W. S. Sayed, M. Roshdy, L. A. Said, and A. G. Radwan, "Design and FPGA verification of custom-shaped chaotic attractors using rotation, offset boosting and amplitude control," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 68, no. 11, pp. 3466–3470, Nov. 2021.
- [22] S. M. Mohamed, W. S. Sayed, A. G. Radwan, and L. A. Said, "FPGA implementation of reconfigurable CORDIC algorithm and a memristive chaotic system with transcendental nonlinearities," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 69, no. 7, pp. 2885–2892, Jul. 2022.
- [23] A. H. ElSafty, M. F. Tolba, L. A. Said, A. H. Madian, and A. G. Radwan, "Hardware realization of a secure and enhanced S-box based speech encryption engine," *Anal. Integr. Circuits Signal Process.*, vol. 106, no. 2, pp. 385–397, Feb. 2021.

- [24] H. A. Abdullah and H. N. Abdullah, "FPGA implementation of color image encryption using a new chaotic map," *Indonesian J. Electr. Eng. Comput. Sci.*, vol. 13, no. 1, pp. 129–137, 2019.
- [25] E. Monmasson and M. N. Cirstea, "FPGA design methodology for industrial control systems—A review," *IEEE Trans. Ind. Electron.*, vol. 54, no. 4, pp. 1824–1842, Aug. 2007.
- [26] J. Ma, Y. Ma, and C. Li, "Infrared and visible image fusion methods and applications: A survey," *Inf. Fusion*, vol. 45, pp. 153–178, Jan. 2019.
- [27] N. I. Chervyakov, M. G. Babenko, N. N. Kuchero, and A. I. Garianina, "The effective neural network implementation of the secret sharing scheme with the use of matrix projections on FPGA," in *Proc. Int. Conf. Swarm Intell.* Cham, Switzerland: Springer, 2015, pp. 3–10.
- [28] J. Stangl, T. Lorunser, and S. M. P. Dinakarrao, "A fast and resource efficient FPGA implementation of secret sharing for storage applications," in *Proc. Design, Autom. Test Eur. Conf. Exhib. (DATE)*, Mar. 2018, pp. 654–659.
- [29] J. Kraft and L. Washington, *An Introduction to Number Theory With Cryptography*, 2nd ed. Orange, CA, USA: Chapman, 2018.
- [30] S. K. Abd-ElHafiz, A. G. Radwan, S. H. A. Haleem, and M. L. Barakat, "A fractal-based image encryption system," *IET Image Process.*, vol. 8, pp. 742–752, 2014.
- [31] (2017). *Genesys 2 FPGA Board Reference Manual*. [Online]. Available: <https://digilent.com>
- [32] A. Weber, "The USC-SIPI image database," Signal Image Process. Inst. Univ. South. California, Los Angeles, CA, USA, Tech. Rep. 432, Version 6, 2018. [Online]. Available: <https://sipi.usc.edu/database/>
- [33] S. H. AbdElHaleem, S. K. Abd-El-Hafiz, and A. G. Radwan, "A generalized framework for elliptic curves based PRNG and its utilization in image encryption," *Sci. Rep.*, vol. 12, no. 1, p. 13278, Aug. 2022.
- [34] A. G. Radwan, S. H. AbdElHaleem, and S. K. Abd-El-Hafiz, "Symmetric encryption algorithms using chaotic and non-chaotic generators: A review," *J. Adv. Res.*, vol. 7, no. 2, pp. 193–208, 2016.
- [35] Y. Wu, S. Member, J. P. Noonan, L. Member, S. Agaian, and S. Member, "NPCR and UACI randomness tests for image encryption," *Cyber J., Multidisciplinary J. Sci. Technol., J. Sel. Areas Telecommun. (JSAT)*, vol. 1, pp. 31–38, Apr. 2011.
- [36] S. Lian, *Multimedia Content Encryption: Techniques and Applications*, 1st ed. New York, NY, USA: Auerbach, 2008.



processing, and waste valorization.



**BISHOY K. SHAROBIM** received the dual bachelor's degree in computer science from Modern Sciences and Arts (MSA) University, Egypt, and the University of Greenwich, U.K., in 2020. He is currently pursuing the master's degree in informatics with Nile University, Egypt. He is also a Research Assistant with the Nanoelectronics Integrated Systems Center (NISC), Nile University. His research interests include quantum computing, information security, number theory, image processing, and waste valorization.

**MARWAN A. FETTEHA** received the bachelor's degree in electronics and communication engineering from Alexandria University, in 2021. He is currently pursuing the master's degree in microelectronics design with Nile University, Egypt. He is also a Research Assistant with the Nanoelectronics Integrated Systems Center (NISC), Nile University. His research interests include hardware design for image and video encryption systems and micro processors design.



**SALWA K. ABD-EL-HAFIZ** (Senior Member, IEEE) received the B.Sc. degree from the Cairo University–Faculty of Engineering (CUFE), Egypt, in 1986, and the M.Sc. and Ph.D. degrees in computer science from the University of Maryland, College Park, MD, USA, in 1990 and 1994, respectively. Since 1994, she has been a Faculty Member with the Engineering Mathematics and Physics Department, CUFE, where she was promoted to a Full Professor, in 2004. From August 2014 to October 2020, she was the Director of the Technical Center for Career Development, CUFE, and the Department Chair and the Vice Dean of Graduate Studies and Research, CUFE. She has coauthored more than 100 publications. Her research interests include chaos theory, number theory, computational intelligence, and software engineering.



**WAFAA S. SAYED** received the B.Sc. degree in electronics and communications engineering and the M.Sc. and Ph.D. degrees in engineering mathematics from the Faculty of Engineering, Cairo University, Egypt, in 2012, 2015, and 2020, respectively. Currently, she is an Assistant Professor with the Faculty of Engineering, Cairo University. She participated as a Researcher and a Senior Researcher with several research grants from different organizations. She has 40 publications, H-index of 11, and 271 citations, based on the Scopus database. Her research interests include chaos theory, chaotic cryptography, fractional dynamics, mathematical software, and adaptive personalized e-learning.



**LOBNA A. SAID** (Senior Member, IEEE) received the B.Sc., M.Sc., and Ph.D. degrees in electronics and electrical communications from Cairo University, Egypt, in 2007, 2011, and 2016, respectively. She is currently a full-time Associate Professor with the Faculty of Engineering and Applied Science, Nile University (NU). She has been the Director of the Microelectronics System Design Master Program (MSD) and the Co-Director of the Nanoelectronics Integrated System Design Research Center (NISC), since September 2021. She has over 144 publications distributed between high-impact journals, conferences, and book chapters. She has an H-index of 25, as reported by the Scopus database. Her research interests include interdisciplinary, including modeling, control, optimization techniques, analog and digital integrated circuits, fractional-order circuits and systems, memristors, non-linear analysis, and chaos theory.



**AHMED G. RADWAN** (Senior Member, IEEE) is currently the Vice President of Research and the Dean of the School of Engineering and Applied Sciences, Nile University. He is also a Professor with the Faculty of Engineering, Cairo University, Egypt. He was the former Center Director of the Nanoelectronics Integrated Systems Center (NISC), Nile University, and the Technical Center for Career Development (TCCD), Cairo University, and the Center Director of the Nanoelectronics Integrated Systems Design (NIESC), Nile University. He has more than 400 papers, H-index of 49, more than 7900 citations, and six U.S. patents in several interdisciplinary concepts ranging from mathematics and engineering applications. He is selected as a member of the National Committee of Mathematics and Applied Science Research Council and the First Council of the Egyptian Young Academy of Science and MC Observer to COST Action CA15225. He is a fellow of the African Academy of Sciences.

...