IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received February 8, 2019, accepted February 20, 2019, date of publication March 5, 2019, date of current version April 3, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2902853

A Note on Multiple Secret Sharing Using Chinese Remainder Theorem and Exclusive-OR

HERI PRASETYO[1] AND JING-MING GUO[2], (Senior Member, IEEE)
[1]Department of Informatics, Universitas Sebelas Maret (UNS), Surakarta 57126, Indonesia
[2]Department of Electrical Engineering, National Taiwan University of Science and Technology (NTUST), Taipei 106, Taiwan
Corresponding author: Heri Prasetyo (heri.prasetyo@staff.uns.ac.id)

ABSTRACT This paper reviews the former existing scheme on (n, n)-multiple secret sharing (MSS) for color images along with its slight limitation. This scheme generates a set of n shared images from a set of n secret images using the Chinese remainder theorem (CRT) and Boolean exclusive-OR (XOR) operation. This scheme works well if the number of secret images n is even number. However, the former scheme has a slight problem while the number of secret images n is an odd number. This paper proposes a new technique to overcome this problem by introducing symmetric and transferred masking coefficients to generate a set of shared images. To further improve the security level of the proposed method, a set of secret images is first transformed with hyperchaotic scrambling method before generating shared images. The security of the proposed (n, n)-MSS can also be increased by merging a shared color image into 2-D matrix representation. As documented in the experimental results, the proposed method offers a promising result on (n, n)-MSS scheme regardless of the number of secret images n is odd or even number. In addition, the proposed method outperforms the former existing (n, n)-MSS schemes in terms of quantitative measurements.

INDEX TERMS Chinese remainder theorem, exclusive OR, secret sharing, symmetric masking coefficient, transferred masking.

I. INTRODUCTION

The image integrity is very important in the digital era since the digital transmission is very common along various parties. Providing the security aspect on digital transmission becomes very urgent. In this situation, the copyright protection as well as the secrecy of information should not be leaked out by unauthorized parties. Transmitting the secret information can be performed via digital imaging. In this transmission scenario, the sender side embeds or renders the secret information into digital imaging file before sending to the receiver module via transmission channel. On the other side, the receiver simply accepts this rendered digital image from the transmission channel. The received image is further processed to recover the embedded secret information or to reveal the rendered data. The receiver will decide a set of particular processes based on the revealed secret information.

Several approaches have been proposed in the literatures regarding to the information hiding and revealing into and from digital images. Some of them can be classified as reversible data hiding [3]–[5], image watermarking [6]–[10], image steganography [11]–[13], secret sharing [3], [14], and MSS schemes [15]–[21]. In the reversible data hiding, secret information are embedded into image in a specific way such that the recovered image after extracting the secret information is maintained as similar as possible to the input image. The image watermarking tries to hide secret information as much as possible with the constraint that the extracted watermark and watermarked image should be identical as possible to the original watermark and host image, respectively. Image steganography simply renders the secret information into image such that its appearance cannot be perceived by human vision. Whereas the MSS scheme generates a set of shared images from a set of secret images before sending to the receiver. A set of recovered secret images can only be obtained while all shared images are collected and computed by the receiver module. Thus, the MSS offers flexibility on sending the secret information with high payload.

Several attempts [15]–[21] have been devoted in order to propose and improve the performance of MSS scheme. Most of them are based on the CRT and XOR operation. The MSS-based scheme [21] has been proposed in which a set of n shared images are generated from a set of n secret

The associate editor coordinating the review of this manuscript and approving it for publication was Sudhakar Radhakrishnan.

images. This scheme performs the multiple color images in (n, n)-MSS setting. As reported in [21], this scheme achieves a good result on MSS task. However, this scheme has limitation while the number of secret image is odd number. This paper tries to solve this problem by involving the symmetric and transferred masking coefficients. The proposed method also improves the security level by applying the hyperchaotic image scrambling method.

The rest of this paper is organized as follows. A brief review of the former existing MSS scheme is provided in Section II. Section III presents the proposed MSS method for color images. Section IV gives the fusion strategy between the proposed (n, n)-MSS method. Extensive experimental results are reported at Section IV. Finally, the conclusions and future works are drawn at the end of this paper.

II. PREVIOUS WORK ON SECRET SHARING USING CRT AND BIT-XOR

This section reviews the former scheme on the MSS (n, n) of color images [21]. This scheme generates n shared images from the n secret images. All images are in Red-Green-Blue (RGB) color space. This method exploits the effectiveness of binary eXclusive-OR operation (XOR) to perform the masking task of a given secret image to generate shared image. This method also involves the Chinese Remainder Theorem (CRT) with several secret keys for obtaining the masking coefficient. These secret keys are only known by the sender and receiver in both encoder and decoder, respectively. Thus, a counterfeit secret key as well as counterfeit masking coefficient is not easily duplicated or obtained by malicious attacker. Fig. 1 illustrates the general framework

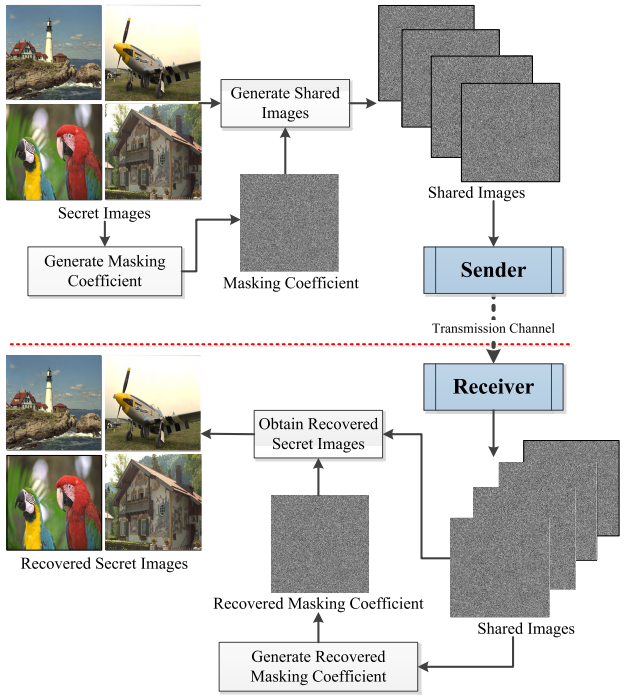

FIGURE 1. General framework of the multiple secret sharing for color images.

of the former (n, n)-MSS. This scheme requires n secret images. The masking coefficient is firstly computed from n secret images by utilizing the boolean XOR and CRT operation. The n shared images are subsequently generated by performing the boolean XOR operation between each secret image with the computed masking coefficient. In the reverse process, the recovered secret images can be obtained by performing the boolean XOR operation between each shared image and the recovered masking coefficient. Herein, the recovered masking coefficient is computed by XOR-ed all shared images and performed the CRT process. It should be noted that all n shared images are required to get back n recovered secret images without any distortion. The quality of reconstructed secret images should be as similar as possible to the original secret images to satisfy a good MSS algorithm design. In addition, an attacker could not reveal any information about reconstructed/secret images if he/she cannot obtain n shared images. In whole discussion of this paper, we will use a set of secret images, i.e. Baboon (I_1), Lake (I_2), Peppers (I_3), and Barbara (I_4), as shown in Fig. 2. All images are in RGB color space of size 512×512.

A. CHINESE REMAINDER THEOREM AND EXCLUSIVE-OR OPERATION

The CRT aims to find a unique solution of a given set of numbers under the modulus congruent constraint. Please refer [1] for detail explanation of CRT operation over a set of numbers. Suppose $\{q_1, q_2, q_3\}$ be three relatively prime numbers which can be regarded as a secret key on CRT process. Let $\{p_1, p_2, p_3\}$ be three arbitrary numbers. In this paper, these arbitrary numbers are from the current processed pixel values in RGB color channel. The CRT operation on these numbers is formally defined as:

$$x = \Im\{p_1, p_2, p_3 \,|\, q_1, q_2, q_3\}, \tag{1}$$

where x is a unique solution satisfying the CRT constraint. The symbol $\Im\{\cdot\}$ denotes the CRT operator. Specifically, the value of x can be computed as:

$$x = \left(\prod_{i=1}^{3}\left(p_i \times Q_i \times Q_i^{-1}\right)\right) \bmod \prod_{i=1}^{3} q_i, \tag{2}$$

where Q_i and Q_i^{-1} the individual divisor and its inverse, respectively, over a given set of relatively prime numbers (CRT secret key).

The inverse CRT operation recovers back the arbitrary numbers while the value of x is available by using the following process:

$$p_i = x \bmod q_i, \tag{3}$$

for $i = 1, 2, 3$. For example, let $\{12, 3, 25\}$ and $\{29, 31, 37\}$ be a set of three arbitrary numbers and a set of relatively prime numbers as CRT secret key, respectively. The CRT produces $x = 8683$. By performing the inverse CRT process, one can reveal three arbitrary numbers as $p_1 = x \bmod 29 = 12$, $p_2 = x \bmod 31 = 3$, and $p_3 = x \bmod 37 = 25$.

It should be noted that the CRT secret keys must be greater than the processed arbitrary number to meet CRT congruent constraint, specifically $p_i < \max(q_1, \ldots, q_3)$.

At the other hand, the MSS scheme employs the boolean XOR operation for generating a set of shared and recovered images. This operation is unary process in the bitwise-level. Suppose that there are two real numbers A and R. The binary string representations between these two numbers are denoted as $A = \bigcup_{i=0}^{k} a_i$ and $R = \bigcup_{i=0}^{k} r_i$, where $a_i, r_i \in \{0, 1\}$. The k denotes the length of binary string. The XOR operation can be formally defined as:

$$A \oplus R = \bigcup_{i=0}^{k} a_i \oplus r_i = \bigcup_{i=0}^{k} a_i' r_i + a_i r_i', \tag{4}$$

where symbol $\oplus$ and a_i' denote the XOR operator and complement of bit a_i, respectively. For example, $2 \oplus 3 = 1$. The XOR operation is very simple making it very suitable for MSS task requiring fast computational response.

The XOR operation has several important properties as described bellow:

- **Identity**:

$$R \oplus 0 = R. \tag{5}$$

The result of performing XOR between arbitrary number with zero yields the arbitrary number itself. For example $5 \oplus 0 = 5$.

- **XOR operation over "even number" times**:

$$\underbrace{R \oplus R \oplus \ldots \oplus R}_{n \text{ is even}} = R \oplus R = 0. \tag{6}$$

The XOR-ed result over "even number" times of arbitrary number R is 0. For example $5 \oplus 5 \oplus 5 \oplus 5 = 5 \oplus 5 = 0$.

- **XOR operation over "odd number" times**:

$$\underbrace{R \oplus R \oplus \ldots \oplus R}_{n \text{ is odd}} = R \oplus (R \oplus R) = R \oplus 0 = R. \tag{7}$$

Given "odd number" times of arbitrary number R, the XOR-ed result is R. For example $5 \oplus 5 \oplus 5 = 5$. The "even" and "odd" properties are very important for reversible MSS scheme.

- **Symmetric Inverse**:

$$\text{If } A \oplus R = B, \quad \text{then } B \oplus R = A. \tag{8}$$

The XOR operation performs differently with the ordinary mathematical operation. The XOR operation employs the similar computation, i.e. $\oplus$, for dealing the symmetric inverse process, whereas the ordinary mathematic requires different operation such as addition (+) is with subtraction (-) operator. For example $5 \oplus 3 = 6$, then we can apply the same $\oplus$ to get back 5 such as $6 \oplus 3 = 5$.

- **Commutative**:

$$A \oplus R = R \oplus A. \tag{9}$$

This property can be trivially proved as $A \oplus R = B$ and $R \oplus A = B$. This property holds $5 \oplus 3 = 6$ and $3 \oplus 5 = 6$.

- **Distributive**:

$$A \oplus (B \oplus R) = (A \oplus B) \oplus R. \tag{10}$$

This property can be easily proved as similar in the commutative property. This property tells that the XOR operation does not involve the operator precedence as usually applied on the ordinary mathematic. This property is very important in MSS since the order of shared or reconstructed secret images can be neglected and ignored. For example $1 \oplus (2 \oplus 3) = 0$ and $(1 \oplus 2) \oplus 3 = 0$.

- **The required bit for XOR result**:

Let $A = \bigcup_{i=0}^{k} a_i$ be an arbitrary number with length k in binary representation, while $R = \bigcup_{i=0}^{l} r_i$ be arbitrary number with binary length l. The XOR operation between these two numbers can be denoted as:

$$A \oplus R = \bigcup_{i=0}^{\max(k,l)} a_i \oplus r_i. \tag{11}$$

The length of binary representation of this XOR-ed result is $\max(k, l)$. It implies that the binary length of XOR-ed result depends on the highest length of binary representation over two processed arbitrary numbers. For example $2 \oplus 100 = 102$. The numbers 2 and 100 can be decoded as 2-bit and 7-bit binary representation. While the XOR-ed result should be encoded as 7-bit binary, i.e. $max\left(\lceil \log_2 A \rceil, \lceil \log_2 R \rceil\right)$. Thus, the required bit for XOR-ed result between two arbitrary numbers A and R can be obtained as follow:

$$\langle A \oplus R \rangle \leq \max\{\langle A \rangle, \langle R \rangle\}, \tag{12}$$

where $\langle \cdot \rangle$ denotes the required bit for representing a given number. Under the similar deduction, the entropy of XOR-ed result can also be obtained. This property is very important to improve the security aspect of MSS scheme in terms of visibility aspect.

In the MSS scheme, the crucial task is on determining the length of binary representation in the XOR computation. Since the MSS works on 8-bit individual image pixel (thus, RGB has 24-bit), lower length of binary representation induces the visibility artifact of the MSS result. Higher length reduces the visibility aspect with the tradeoff on higher payload for the transmission channel requirement. Fig. 3 shows the XOR-ed result between the Baboon image and random image, i.e. $I_1 \oplus R$. While R is uniformly random image drawn at interval $[a, b]$, i.e. $R \sim U(a, b)$. As shown in this figure, the required bit or magnitude of R affect the visibility aspect of XOR-ed result. The XOR-ed image can still be recognized by applying R with low interval/magnitude. However, the information of XOR-ed cannot easily perceived when R is in high interval/magnitude. Thus, the interval R should be chosen as high enough to meet the imperceptibility aspect in MSS method. In addition, the image scrambling method effectively improves the randomized result on the XOR-ed image as shown in Fig. 3.

B. FORMER APPROACH ON MULTIPLE SECRET SHARING

This subsection presents the former existing MSS scheme on color images [21]. This scheme exploits the boolean XOR

FIGURE 2. A set of secret images: (a) Baboon, I_1, (b) Lake, I_2, (c) Peppers, I_3, and (d) Barbara, I_4.

operation and CRT for performing secure (n, n)-MSS. The n shared images are required to reconstruct n recovered secret images. Let $\{I_1, I_2, \ldots, I_n\}$ be a set of secret images, while I_i denotes the i-th secret image. The (n, n)-MSS requires the masking coefficient for generating the shared images. Herein, the masking coefficient is computed as:

$$R = \Im\{I_1 \oplus I_2 \oplus \ldots \oplus I_n\}, \tag{13}$$

where R is masking coefficient. In simple word, the masking coefficient R is obtained by performing CRT of the XOR-ed all secret images. A shared image can be easily computed by performing XOR operation between the secret image I_i and R as follow:

$$S_i = I_i \oplus R, \tag{14}$$

for $i = 1, 2, \ldots, n$. The dimensionality of R must be identical to that of the secret image. An easy way to deal with this issue is to duplicate the CRT result into three dimensional R if the secret image is in RGB color space. Each CRT result is recorded and duplicated for red, green, and blue of a given pixel. In addition, the CRT requires the secret keys which must be identical in both encoder/sender and decoder/receiver sides.

In the (n, n)-MSS scheme, all n shared images are required to reconstruct the n secret images. The secret image reconstruction can be regarded as the inverse process of shared image generation. This process firstly compute the masking coefficient from all shared images as:

$$\tilde{R} = \Im\{S_1 \oplus S_2 \oplus \ldots \oplus S_n\}, \tag{15}$$

where $\tilde{R}$ is recovered masking coefficient. Herein, the CRT secret keys must be identical as used in (13). The recovered secret image can be further obtained from each shared image as follow:

$$\tilde{I}_i = S_i \oplus \tilde{R}, \tag{16}$$

for $i = 1, 2, \ldots, n$. Where $\tilde{I}_i$ denotes the i-th recovered secret image.

C. LIMITATION ON FORMER APPROACH

This subsection investigates the performance of the former existing MSS scheme on color images [21]. Suppose that there are four secret images $\{I_1, I_2, \ldots, I_4\}$ as depicted at Fig. 2. This scheme employs the CRT with a set of secret keys as $\{3, 5, 17\}$ which are relatively prime numbers. For $n = 4$, the former scheme produces four shared images as shown in Fig. 4(a-d) along with their histogram on each color channel depicted at the bottom-left on each image. Four recovered secret images can be reconstructed by using the inverse MSS scheme involving four shared images. As shown in Figs. 4 (e-h), a set of recovered secret images are visually similar to that of a set of secret images. Yet, the former MSS scheme yields a good result on secret sharing task while the number of secret images n is even number (i.e. $n = 4$, in this experiment).

However, the former MSS scheme has a limitation while the number of secret images n is odd number. Fig. 5 gives illustration for this limitation by setting $n = 3$. Suppose that there are three secret images $\{I_1, \ldots, I_3\}$. Using the aforementioned MSS method, a set of shared images $\{S_1, \ldots, S_3\}$ can be obtained as depicted in Figs. 5(a-c). With the inverse MSS scheme, a set of recovered secret images $\left\{\tilde{I}_1, \ldots, \tilde{I}_3\right\}$ can be reconstructed as it can be seen in Figs. 5(d-f). As reported in these figures, the former MSS scheme is not able to reconstruct a set of recovered secret images correctly while the number of secret images are $n = 3$. The same problem also occurs on the former existing MSS scheme by setting the number of secret images n as odd number. This limitation causes an unpleasant problem for transferring secret information while choosing some images as sharing media.

D. ANALYSIS OF FORMER APPROACH

The problem in former MSS scheme is caused by unsymmetrical computation on shared images generation and recovered secret images computation stages. This method does not follow a strict requirement on symmetric MMS masking coefficient. The masking coefficient in shared image generation R must be idential to that of the recovered masking coefficient

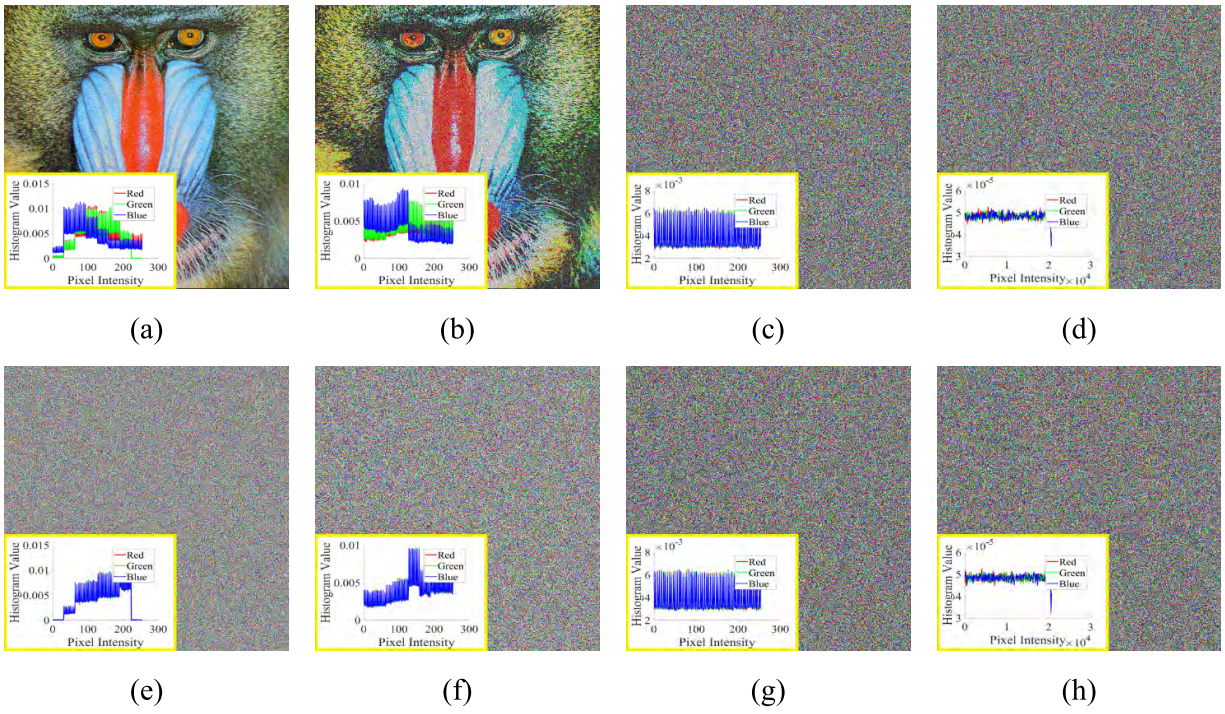

FIGURE 3. Result of XOR operation between I_1 with random image in intervals (a) $R \sim U(0, 30)$, (b) $R \sim U(0, 105)$, (c) $R \sim U(0, 255)$, and (d) $R \sim U(0, 20677)$. Whereas (e-h) are the XOR-ed results while the secret image is in scrambled version.

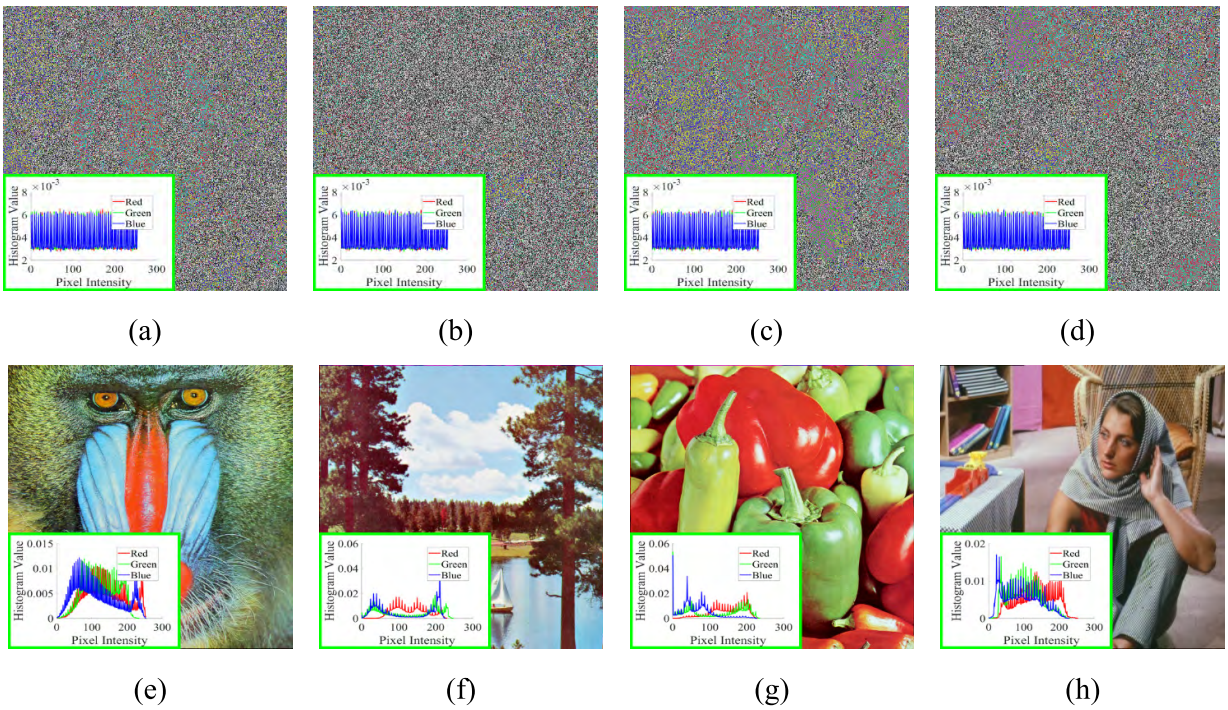

FIGURE 4. Result of the former scheme [21] on multiple secret sharing while $n = 4$: (a-d) a set of shared images $\{S_1, S_2, S_3, S_4\}$, and (e-h) a set of recovered secret images $\left\{\tilde{I}_1, \tilde{I}_2, \tilde{I}_3, \tilde{I}_4\right\}$. The corresponding histogram of each image is given at bottom-left part of each image.

$\tilde{R}$ used in recovered image process, i.e.:

$$R = \tilde{R}. \tag{17}$$

The problem in the former MSS scheme can be mathematically proved as follow. Suppose that there are n secret images, while n is even number. In the shared image generation, the masking coefficient is computed by performing CRT over XOR-ed all secret images as follow:

$$R = \Im\left\{I_1 \oplus I_2 \oplus \ldots \oplus I_n\right\}. \tag{18}$$

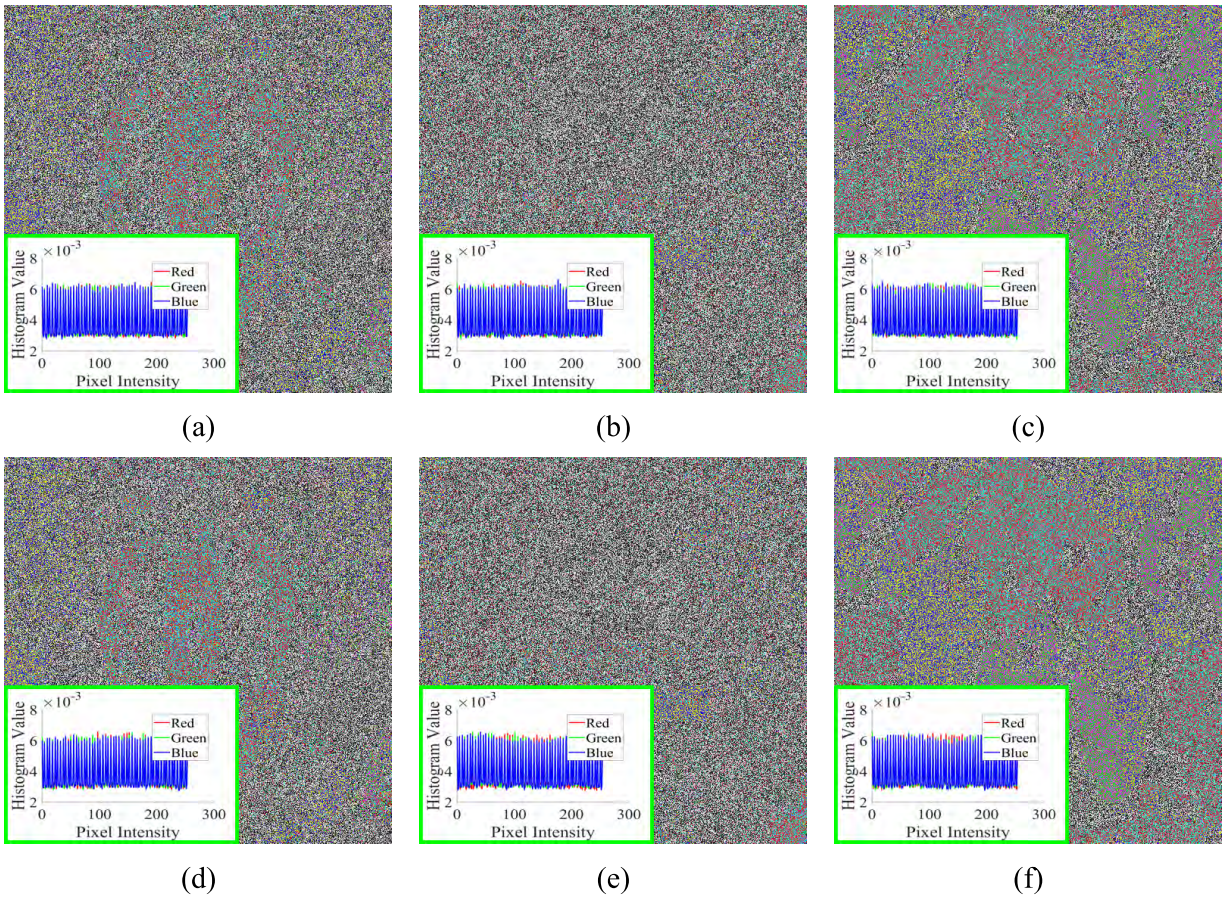

FIGURE 5. Result of the former scheme [21] on multiple secret sharing while $n = 3$: (a-c) a set of shared images $\{S_1, S_2, S_3\}$, and (d-f) a set of recovered secret images $\left\{\tilde{I}_1, \tilde{I}_2, \tilde{I}_3\right\}$.

In the recovered secret images computation, the recovered masking coefficient is calculated by CRT and XOR-ed processes over all shared images as follow:

$$\tilde{R} = \Im\left\{S_1 \oplus S_2 \oplus \ldots \oplus S_n\right\}. \tag{19}$$

Since the shared image is the XOR-ed result between the secret image with the masking coefficient R, i.e. $S_i = I_i \oplus R$, the recovered masking coefficient can be further computed as follow:

$$\tilde{R} = \Im\left\{I_1 \oplus R \oplus I_2 \oplus R \oplus \ldots \oplus I_n \oplus R\right\},$$

$$\tilde{R} = \Im\left\{I_1 \oplus I_2 \oplus \ldots \oplus I_n \oplus \underbrace{R \oplus R \oplus \ldots \oplus R}_{n \text{ is even}}\right\}.$$

With the XOR property involving "even number" times, the last form can be rewritten as:

$$\tilde{R} = \Im\left\{I_1 \oplus I_2 \oplus \ldots \oplus I_n \oplus 0\right\}.$$

This form implies the following simplification:

$$\tilde{R} = \Im\left\{I_1 \oplus I_2 \oplus \ldots \oplus I_n\right\}. \tag{20}$$

It can be seen that the $\tilde{R}$ is a result of CRT on XOR-ed all secret images. The last form trivially tells that the recovered masking coefficient $\tilde{R}$ as given in (20) is identical to that of the masking coefficient R as given in (18), i.e. $R = \tilde{R}$. Thus, a set of recovered secret images are exactly similar to that of a set of secret images while the number of secret images n is even number.

In case of the number of secret image n is odd number, the recovered masking coefficient $\tilde{R}$ can be obtained as follow:

$$\tilde{R} = \Im\left\{S_1 \oplus S_2 \oplus \ldots \oplus S_n\right\}$$

$$= \Im\left\{I_1 \oplus I_2 \oplus \ldots \oplus I_n \oplus \underbrace{R \oplus R \oplus \ldots \oplus R}_{n \text{ is odd}}\right\}.$$

By considering the XOR property on "odd number" times, this form can be simplified as:

$$\tilde{R} = \Im\left\{I_1 \oplus I_2 \oplus \ldots \oplus I_n \oplus R\right\}. \tag{21}$$

Herein, the recovered masking coefficient contains R. As we know that the masking coefficient $R = \Im\left\{I_1 \oplus I_2 \oplus \ldots \oplus I_n\right\}$. Thus, the masking coefficient is totally different with the recovered masking coefficient, i.e. $R \neq \tilde{R}$. It is a reason that we cannot obtain a correct recovered image while the number of secret images is odd number.

III. PROPOSED METHOD ON MULTIPLE SECRET SHARING

This section presents the proposed method on (n, n)-MSS. Several techniques will be described in detail to solve

the aforementioned problem in (n, n)-MSS. The proposed method utilizes n secret images to generate n shared images. The proposed method requires n shared images to reconstruct back a set of recovered secret images. The partial information of secret image cannot be revealed out while the number of involved shared image is less than n. There are two types of masking coefficient used in the proposed method, i.e. symmetric masking coefficient and transferred masking coefficient. To further improve the security level, the proposed scheme exploits the hyperchaotic image scrambling method to reduce the perceptual recognition of secret image.

A. PROPOSED METHOD WITH SYMMETRIC MASKING COEFFICIENT

In this scheme, the masking coefficient in decoder/receiver side is set as identical to that of used in encoder/sender side. This scenario is to satisfy a strict requirement, i.e. symmetric MSS masking coefficient. Specifically, the masking coefficient and recovered masking coefficient should be designed to achieve requirement $R = \tilde{R}$. The simplest way to deal with this requirement is to generate the masking coefficient which is independent with the secret and shared images. Herein, the masking coefficient and its recovered version can be generated on both sender and receiver sides with random number generator by involving the same secret key on both parties. The uniform random number cannot be utilized in this scheme since it will produce different random number over different time stamp. The chaotic random number offers a good solution for symmetric masking coefficient. The generated random number is influenced by the initial seed or secret key. Thus, the sender and receiver sides can obtain the identical chaotic random number while using identical seed or secret key. Specifically, the masking coefficient and recovered version can be obtained as follow:

$$R = \tilde{R} = \Im\{B\}, \tag{22}$$

while B is chaotic random image which is a matrix of the same size with the secret image. All pixels in B are generated from chaotic random number in the interval $[0, 255]$, (the same interval as in secret image). Each entry of random image B of size $M \times N$ is given as:

$$B = \bigcup_{i=1}^{3MN} b_i, \tag{23}$$

where b_i is chaotic random number. In this paper, the chaotic random number is generated by using the logistic maps [1] as described bellow:

$$b_i = \alpha b_i (1 - b_i), \tag{24}$$

where α denotes the logistic coefficient, i.e. $\alpha = 4$. The initial seed of random number is denoted as b_0, where its value is in $b_0 \in (0, 1)$. This initial seed can be regarded as secret key on the proposed MSS scheme. However, the chaotic random number generation should consider the bifurcation condition. The wrong initial seed will not produce random number in a specific range. For example, the initial seed $b_0 \notin \{0, 0.25, 0.5, 0.75, 1\}$ cannot generate random number. Fig. 6 illustrates the chaotic random number over various initial seed. It can be seen from this figure that some values of initial seeds cannot provide a good random number.

Let $\{I_1, I_2, \ldots, I_n\}$ be a set of secret images in which the number of secret images n can be odd or even number. The proposed scheme firstly generates masking coefficient using a specific chaotic secret key as indicated in (22). A set of shared images can be further obtained using the proposed method by applying the XOR operation between each secret image I_i and the masking coefficient R as follow:

$$S_i = I_i \oplus R. \tag{25}$$

for $i = 1, 2, \ldots, n$. At the end of shared image generation, one may obtain a set of shared images $\{S_1, S_2, \ldots, S_n\}$. These images are required to recover secret images. To deal with it, the proposed method calculates the recovered masking coefficient $\tilde{R}$ with identical secret key as used for computing R. Reversely, the recovered secret image can be obtained by performing XOR operation between each shared image with recovered masking coefficient as:

$$\tilde{I}_i = S_i \oplus \tilde{R}. \tag{26}$$

for $i = 1, 2, \ldots, n$. At the end of recovery process, a set of reconstructed secret images $\left\{\tilde{I}_1, \tilde{I}_2, \ldots, \tilde{I}_n\right\}$ can be obtained. Herein, the quality of original secret image I_i and recovered secret image $\tilde{I}_i$ is identical since it involves the same masking coefficient, i.e. $R = \tilde{R}$.

Alternatively, the masking coefficient R can be transferred from the sender to the received module by performing the encryption technique. This encrypted masking coefficient can be transferred as an additional shared image, i.e. S_{n+1}. At the receiver side, the decryption process is then performed on this additional shared image to obtain the recovered masking coefficient, i.e. $\tilde{R}$. Thus, a set of recovered secret images can be obtained at the end of this process.

B. PROPOSED METHOD WITH TRANSFERRED MASKING COEFFICIENT

This section presents the proposed (n, n)-MSS method using the transferred masking coefficient. In this scheme, the value of masking coefficient depends on a set of secret and shared images. The terms "transferred" refers to the recovered masking coefficient computation while the shared images are transferred via transmission channel. The recovered masking coefficient can be computed while all contributed shared images are perfectly transferred and obtained at the receiver/decoder side. This approach solves the problem occurred in the former existing MSS scheme [21].

Let $\{I_1, I_2, \ldots, I_n\}$ be a set of secret images while the number of secret images can be odd or even number. The proposed method firstly computes the masking coefficient as follow:

$$R = \Im\{I_1 \oplus I_2 \oplus \ldots \oplus I_n\}. \tag{27}$$

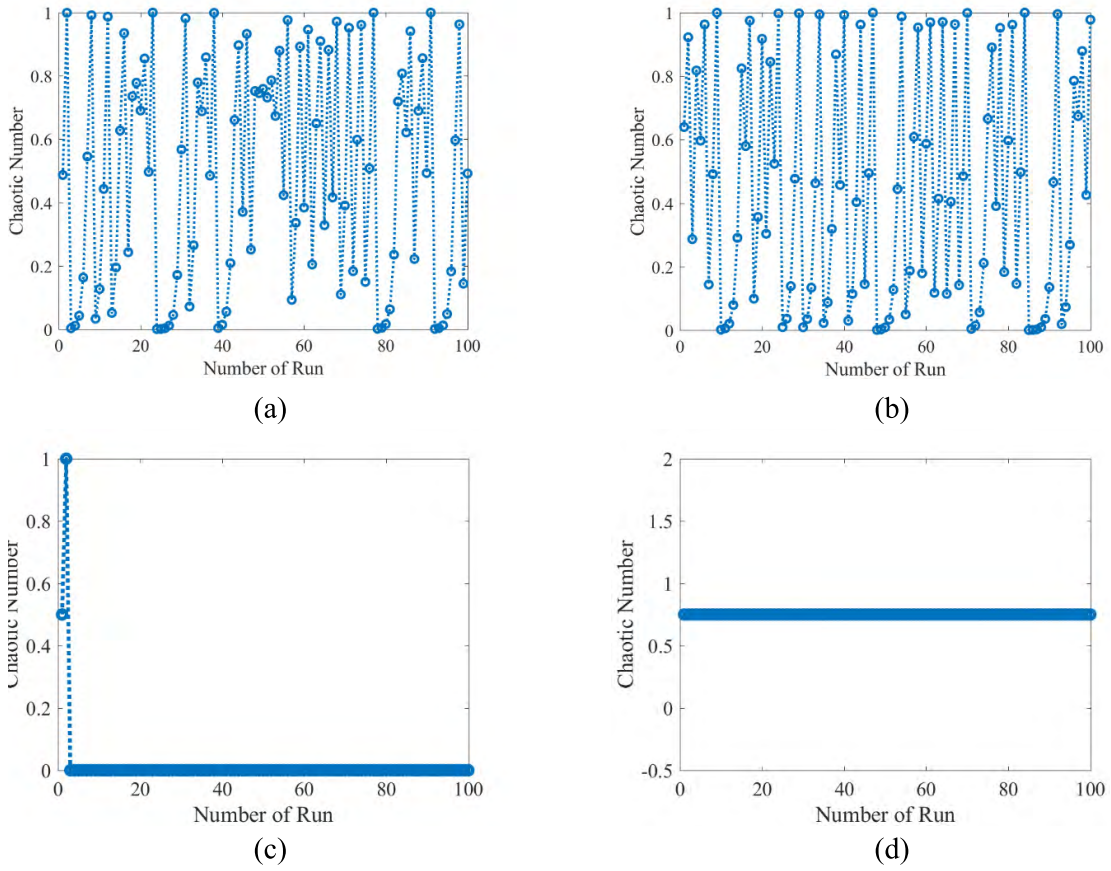

FIGURE 6. Chaotic numbers under different keys: (a) $b_0 = 0.14189$, (b) $b_0 = 0.80028$, (c) $b_0 = 0.5$, and (d) $b_0 = 0.75$.

A set of shared images can be subsequently obtained by performing XOR operation between the secret image I_i and R as follow:

$$S_i = I_i \oplus R, \tag{28}$$

for $i = 1, 2, \ldots, n-1$. The shared image S_n needs a special attention in order to deal with even or odd number of secret/shared images. The S_n can be computed from I_n as:

$$S_n = I_n \oplus A, \tag{29}$$

while A is auxilary image. If n is even number, this auxiliary image can be simply set as $A = R$. If n is odd number, the auxilary image can be computed from the results of CRT and XOR-ed over $n-1$ secret images as follow:

$$A = \Im\left\{I_1 \oplus I_2 \oplus \ldots \oplus I_{n-1}\right\}. \tag{30}$$

A set of shared images $\{S_1, S_2, \ldots, S_n\}$ can be obtained at the end of this process. Special restriction is only for the last secret image on shared image generation.

In the recovered image generation, all shared image should be taken into account to produce a set of recovered secret images. Herein, we need special consideration whether the number of shared images are odd or even number. In case of the number of shared images n is even, the recovered masking coefficient can be simply computed as bellow:

$$\tilde{R} = \Im\left\{S_1 \oplus S_2 \oplus \ldots \oplus S_n\right\}. \tag{31}$$

The recovered secret images can be trivially obtained as follow:

$$\tilde{I}_i = S_1 \oplus \tilde{R}. \tag{32}$$

If the number of shared images n is odd, the recovered auxilary image is firstly computed from a set of $n-1$ shared images as follow:

$$\tilde{A} = \Im\left\{S_1 \oplus S_2 \oplus \ldots \oplus S_{n-1}\right\}. \tag{33}$$

A recovered secret image $\tilde{I}_n$ can be easily obtained as:

$$\tilde{I}_n = S_n \oplus \tilde{A}. \tag{34}$$

In order to recover back a set of secret images $\left\{\tilde{I}_1, \tilde{I}_2, \ldots, \tilde{I}_{n-1}\right\}$, we need to compute the recovered masking coefficient $\tilde{R}$ from $\{S_1, S_2, \ldots, S_{n-1}\}$ and $\tilde{I}_n$ which can be formally described as:

$$\tilde{R} = \Im\left\{S_1 \oplus S_2 \oplus \ldots \oplus S_{n-1} \oplus \tilde{I}_n\right\}. \tag{35}$$

Thus, the recovered secret image can be easily obtain as:

$$\tilde{I}_i = S_i \oplus \tilde{R}, \tag{36}$$

for $i = 1, 2, \ldots, n-1$. The proposed method effectively solves the aforementioned problem in the former scheme [21] by utilizing the auxiliary image. The number of secret/shared images is not necessary to be considered for the proposed method, since it works well whether n is odd or even number.

The following analysis supports the correctness of proposed method using the transferred masking coefficient. In case of n is odd number, the recovered masking coefficient is computed as follow:

$$\tilde{R} = \Im\left\{S_1 \oplus S_2 \oplus \ldots \oplus S_{n-1} \oplus \tilde{I}_n\right\}.$$

Since $S_i = I_i \oplus R$, then the value of $\tilde{R}$ can be recomputed as:

$$\tilde{R} = \Im\left\{I_1 \oplus R \oplus I_2 \oplus R \ldots \oplus I_{n-1} \oplus R \oplus \tilde{I}_n\right\}.$$

With a simple XOR algebraic approach and considering the XOR properties, $\tilde{R}$ can be simply formed as:

$$\tilde{R} = \Im\left\{I_1 \oplus I_2 \oplus \ldots \oplus I_{n-1} \oplus \underbrace{R \oplus R \oplus \ldots \oplus R}_{n \text{ is even}} \oplus \tilde{I}_n\right\},$$

$$\tilde{R} = \Im\left\{I_1 \oplus I_2 \oplus \ldots \oplus I_{n-1} \oplus \tilde{I}_n\right\}.$$

In a good MSS design, the secret image and its recovered version must be identical without any distortion, i.e. $\tilde{I}_n = I_n$. The last form of $\tilde{R}$ can be further simplified as:

$$\tilde{R} = \Im\left\{I_1 \oplus I_2 \oplus \ldots \oplus I_{n-1} \oplus I_n\right\}. \tag{37}$$

The $\tilde{R}$ in (37) is identical to that of (27). The proposed (n, n)-MSS method satisfies a strict requirement on symmetric masking coefficient, i.e. $R = \tilde{R}$, regardless the number of secret/shared images n is odd or even number. The similar analysis can also be applied for auxiliary image A. With simple analysis, we can show that the proposed method yields $A = \tilde{A}$. Thus, the proposed (n, n)-MSS method can be alternatively candidate for transferring correct secret information on digital imaging.

C. PROPOSED METHOD WITH HYPERCHAOTIC IMAGE SCRAMBLING

An additional process can be added into the proposed method in order to improve the security level. The simplest way to increase the security level is by applying the hyperchaotic image scrambling method [2]. This image scrambling destroys an image appearance such that the image content cannot be easily recognized and perceived by human vision. This scrambling also extends or transforms a single given image into a set of scrambled image by choosing several hyperchaotic keys. These scrambled images are subsequently fed into the proposed (n, n)-MSS method before sending to the receiver module. At the receiver side, an inverse image scrambling method should be performed to reconstruct a set of recovered secret images. It should be noted that the sender and receiver modules need to use the identical hyperchaotic secret keys to obtain a correct result.

TABLE 1. Hyperchaos discrete nonlinear dynamic systems.

Hyperchaos Type (Key)	2D Hyperchaos System	Parameters
1	$x_{n+1} = a_4 y_n + a_5 y_n^2$	$a_4 = 1.55, a_5 = -1.3$
	$y_{n+1} = b_2 x_n + b_4 y_n$	$b_2 = -1.1, b_4 = 0.1$
2	$x_{n+1} = a_2 x_n + a_4 y_n$	$a_2 = -0.95, a_4 = -1.3$
	$y_{n+1} = b_1 + b_3 x_n^2 + b_4 y_n$	$b_1 = -0.45, b_3 = 2.4, b_4 = 1.05$
3	$x_{n+1} = a_5 y_n^2$	$a_5 = 1.3$
	$y_{n+1} = b_1 + b_2 x_n + b_4 y_n$	$b_1 = -1.05, b_2 = 1.15, b_4 = -0.2$
4	$x_{n+1} = a_2 x_n + a_5 y_n^2$	$a_2 = 0.1, a_5 = 1.8$
	$y_{n+1} = b_1 + b_2 x_n + b_4 y_n$	$b_1 = 0.3, b_2 = -2.2, b_4 = 0.2$
5	$x_{n+1} = a_1 + a_2 x_n + a_4 y_n$	$a_1 = 0.2, a_2 = 0.3, a_4 = 0.5$
	$y_{n+1} = b_1 + b_3 x_n^2$	$b_1 = -1.6, b_3 = 3.7$
6	$x_{n+1} = a_1 + a_4 y_n + a_6 x_n y_n$	$a_1 = -0.7, a_4 = 3.3, a_6 = -2.3$
	$y_{n+1} = b_3 x_n^2$	$b_3 = 0.6$

The formal procedure on applying hyperchaotic image scrambling for the proposed method is described as follow. Suppose there are a set of secret images $\{I_1, I_2, \ldots, I_n\}$. Each secret image is firstly processed using the hyperchaotic image scrambling method [2] as follow:

$$I_i^h = \mathcal{H}\{I_i, h\}, \tag{38}$$

for $h = 1, 2, \ldots, \kappa$, where h represents the hyperchaotic secret key. The $\mathcal{H}\{\cdot\}$ is an image scrambling operator. Table 1 gives hyperchaotic coefficients for computing the hyperchaotic image scrambling. The symbol κ denotes the number of utilized hyperchaotic secret key. Thus, we may obtain κ scrambled secret images after applying the scrambling method on a single secret image I_i. At total, we can have a set of scrambled secret images as follow:

$$\left\{I_1^1, I_1^2, \ldots, I_1^\kappa, \ldots, I_n^1, I_n^2, \ldots, I_n^\kappa\right\}. \tag{39}$$

The masking coefficient can be simply computed as bellow:

$$R = \Im\left\{I_1^1 \oplus I_1^2 \oplus \ldots \oplus I_1^\kappa \oplus \ldots \oplus I_n^1 \oplus I_n^2 \oplus \ldots \oplus I_n^\kappa\right\}. \tag{40}$$

The proposed method can be applied on a set of scrambled secret images with this masking coefficient and additional auxiliary random image depending on the number of scrambled secret images. At the end of this process, one can obtain a set of scrambled shared images as:

$$\left\{S_1^1, S_1^2, \ldots, S_1^\kappa, \ldots, S_n^1, S_n^2, \ldots, S_n^\kappa\right\}. \tag{41}$$

On reverse side, the recovered masking coefficient can be computed from a set of scrambled shared images as:

$$\tilde{R} = \Im\left\{S_1^1 \oplus S_1^2 \oplus \ldots \oplus S_1^\kappa \oplus \ldots \oplus S_n^1 \oplus S_n^2 \oplus \ldots \oplus S_n^\kappa\right\}. \tag{42}$$

This illustration is workable for n even number. A slight modification should be carried out for n is odd number. Using this recovered masking coefficient, a set of scrambled recovered shared images can be calculated and obtained as follow:

$$\left\{\tilde{I}_1^1, \tilde{I}_1^2, \ldots, \tilde{I}_1^\kappa, \ldots, \tilde{I}_n^1, \tilde{I}_n^2, \ldots, \tilde{I}_n^\kappa\right\}. \tag{43}$$

The inverse image scrambling method should be applied to generate a correct recovered shared images:

$$I_i = H^{-1}\left\{\tilde{I}_i^h, h\right\}, \tag{44}$$

where $H^{-1}\{\cdot\}$ denotes the inverse hyperchaotic image scrambling method. A set of hyperchaotic secret keys should be kept in both sender and receiver sides such that a malicious attacker cannot reveal a set of recovered secret images.

D. MERGING INTO TWO DIMENSIONAL MATRIX REPRESENTATION

To further improve the security, a set of shared images can be transformed into another form before sending to the receiver module. Herein, each pixel of shared image which is originally in three dimensional matrix (in RGB color space) can be merged into two dimensional matrix representation. It can be realized by performing CRT on each pixel of shared image. Suppose that we have a set of scrambled shared images as $\left\{S_1^1, S_1^2, \ldots, S_1^\kappa, \ldots, S_n^1, S_n^2, \ldots, S_n^\kappa\right\}$. Each pixel of shared image of size $M \times N$ can be denoted as $S_i^h = \bigcup_{j=1}^{3MN}\left(r_j, g_j, b_j\right)$ consisting red, green, and blue component. The merging process for each pixel of shared image can be performed as:

$$\Im\left\{S_i^h\right\} = \bigcup_{j=1}^{3MN} I\left\{r_j, g_j, b_j\right\}. \tag{45}$$

Three components of each pixel can be transformed into one component using the CRT process as illustrated in Section II.A. Herein, the CRT secret keys should be chosen as higher than the maximum value of all pixels in shared images. The merged shared images can be further sent into receiver module via transmission channel.

In the receiver side, each pixel of merged shared images can be recovered back using an inverse CRT process as described bellow:

$$S_i^h = \Im^{-1}\left\{S_i^h\right\}, \tag{46}$$

where $\Im^{-1}\{\cdot\}$ denotes the inverse CRT process. This result has no distortion as long as the sender and receiver utilize the identical CRT secret keys. Thus, the security level of the proposed method can be increased using this merging scenario.

E. INTEGRATING INTO TWO COMPLETE (n, n)-MSS SCHEMES

The hyperchaotic image scrambling and merging into two dimensional matrix representation offer great benefit for our proposed (n, n)-MSS system. These two approaches can be integrated into our proposed MSS method with symmetric or transferred masking coefficients. Fig. 7 shows the schematic diagram of this integration strategy. Since of the paper space limitation, we only provide the schematic diagram for the encoder/sender side. The process in decoder/receiver side can be trivially obtained by reversing the process in encoder/sender module. Firstly, n secret images are permuted with the hyperchaotic image scrambling with some chaotic secret keys to yield $n\kappa$ scrambled secret images, where κ denotes the number of hyperchaotic types used in the image permutation. These $n\kappa$ scrambled secret images are subsequently fed into the proposed (n, n)-MSS method to obtain $n\kappa$ shared images. One may employ the symmetric or transferred masking coefficients in the shared image generation. It should be noted that each shared image is in three tuples color space while the secret images are in the same color channel (RGB color). Each pixel in shared image is then merged from three into two dimensional matrix representation. All shared images in the merged matrix representation are then sent into the receiver module via transmission channel. The receiver simply performs the reverse process to obtain the recovered secret images. As a result, the performance of proposed method can be increased by integrating the hyperchaotic image scrambling and merging two dimensional approach.

IV. EXPERIMENTAL RESULTS

This section elaborates and reports some extensive experiments for demonstrating the effectiveness and usefulness of the proposed (n, n)-MSS method. The proposed method performance is investigated using a set of color images of size 512×512 as shown in Fig. 2, which are turned as a set of secret images. The correctness of the proposed method is examined using subjective observation. The proposed method is regarded to yield a correct result if the secret image and recovered secret image are visually similar. The proposed method is also objectively measured in terms of quantitative measurement between the secret image and recovered secret image.

A. QUANTITATIVE MEASUREMENT

Several quantitative measurements [3], [14]–[21] can be adopted to assess the proposed method performance. These measurement metrics investigate the similarity level between two images. Let X and Y be two images of size $M \times N$. On dealing with the color image, the similarity between two images can be measured by averaging over all three color spaces of an image. The following quantitative metrics are used to assess the proposed method performance:

- Correlation:

$$Corr\,(X, Y) = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}\left(X(i,j)-\bar{X}\right)\left(Y(i,j)-\bar{Y}\right)}{\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N}\left(X(i,j)-\bar{X}\right)^2}\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N}\left(Y(i,j)-\bar{Y}\right)^2}}. \tag{47}$$

- Root Mean Squared Error (RMSE):

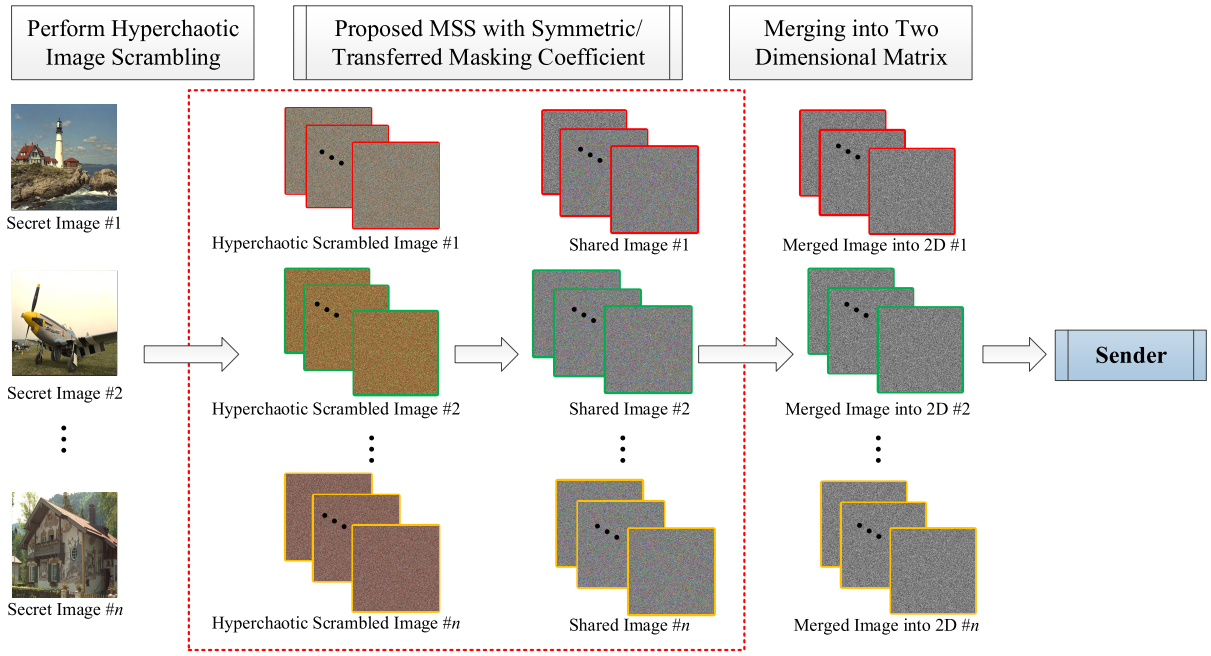

FIGURE 7. Integrating the hyperchaotic image scrambling and merging two dimensional matrix approaches on the multiple secret sharing.

$$RMSE\,(X,Y)=\sqrt{\frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}[X\,(i,j)-Y\,(i,j)]^2}. \tag{48}$$

- Peak-Signal-to-Noise Ratio (PSNR):

$$PSNR\,(X,Y)=10\log_{10}\frac{Z^2}{\frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}[X\,(i,j)-Y\,(i,j)]^2}. \tag{49}$$

- Mean Absolute Error (MAE):

$$MAE(X,Y)=\frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}|X\,(i,j)-Y(i,j)|\,. \tag{50}$$

- Number of Pixel Changing Rate (NPCR):

$$NPCR\,(X,Y)=\frac{1}{MN}\left[\sum_{i=1}^{M}\sum_{j=1}^{N}D(i,j)\right]\times 100\%, \tag{51}$$

$$\text{where } D\,(i,j)=\begin{cases}0 & if\ X\,(i,j)=Y(i,j)\\ 1 & if\ X\,(i,j)\neq Y(i,j).\end{cases}$$

- Unified Averaged Changed Intensity (UACI):

$$UACI\,(X,Y)=\frac{1}{MN}\left[\sum_{i=1}^{M}\sum_{j=1}^{N}\frac{|X\,(i,j)-Y(i,j)|}{Z}\right]\times 100\%, \tag{52}$$

where Z denotes the maximum support pixel in an image (this paper simply sets $Z = 255$ since we only consider 8-bits imaging system). The correlation value lies on interval $[-1, 1]$ in which the value -1 or 1 indicate that two images are highly related to each other, where the value 0 indicates that two images are totally not related (more independent). Higher values of PSNR and NPCR inform that two images are more similar. For the other quantitative measurements, lower value indicates a better result, i.e. two images are more similar.

B. PROPOSED METHOD PERFORMANCE USING SYMMETRIC MASKING COEFFICIENT

This subsection reports some experimental results for the proposed (n, n)-MSS scheme under visual investigation to examine its correctness. Herein, the proposed method employs the symmetric masking coefficient which is generated in both sender and receiver sides using an identical chaotic random image with selected secret key. In this experiment, the selected chaotic secret key is set as $b_0 = \{0.034, 0.401, 0.875\}$ for each RGB color channel and $\alpha = 4$. The CRT secret key is chosen as $\{3, 5, 17\}$ indicating that each pixel value of shared image lies on interval $[0, 255]$. It implies that each pixel of shared image requires 8 bits for representing and storing this pixel value. Since the result of CRT is only in two dimensional matrix, thus, this matrix can be duplicated into three dimensional matrix for performing the masking process with color image. Fig. 8 shows the proposed method performance using the symmetric masking coefficient while $n = 4$. As shown in this figure, the shared images cannot be easily recognized each other using visual investigation. The histogram of each image is given at the bottom-left part of each image. The histogram of each shared image seems to be uniformly distributed over all pixel values indicating a high entropy value (near 8 bits/pixel) and low correlation coefficient. The histograms of all shared images are relatively similar one to the other making it very difficult to be cryptanalyzed. Figs. 8(e-h) show a set of recovered secret images produced by the proposed method using correct

FIGURE 8. Result of the proposed method with symmetric masking coefficient while $n = 4$: (a-d) a set of shared images $\{S_1, S_2, S_3, S_4\}$, (e-h) a set of recovered secret images $\{\tilde{I}_1, \tilde{I}_2, \tilde{I}_3, \tilde{I}_4\}$ using correct chaotic secret key b_0, and (i-l) a set of recovered secret images $\{\tilde{I}_1, \tilde{I}_2, \tilde{I}_3, \tilde{I}_4\}$ using incorrect chaotic secret key b_0.

chaotic secret key b_0, whereas Figs. 8(i-l) are the results while using incorrect chaotic secret key $b_0 = \{0.46, 0.79, 0.155\}$. By using correct chaotic secret key, a set of recovered secret images are identical to that of the original secret images. An attacker obtain un-meaningful image while the counterfeit chaotic key is not identical to the owner chaotic secret key.

The result of the proposed method while $n = 3$ is shown in Fig. 9. A set of recovered secret images are similar to that of the original secret images as shown in Figs. 9(d-f) by utilizing correct chaotic secret key. Incorporating incorrect chaotic secret key, a set of recovered secret images are totally different compared to a set of original secret images as displayed in Figs. 9(g-i). This result proves that the proposed method works well in the (n, n)-MSS task with symmetric masking coefficient. In addition, the proposed method is directly applicable while the number of secret images n is odd or even. Yet, it solves the problem in the former existing scheme [21].

C. PROPOSED METHOD PERFORMANCE USING TRANSFERRED MASKING COEFFICIENT

The performance of the proposed (n, n)-MSS method using the transferred masking coefficient is reported in this subsection. In this experiment, the CRT secret key is chosen as $\{3, 5, 17\}$. Firstly, we investigate the correctness of the proposed method with $n = 4$. Figs. 10(a-d) give a set of shared images along with its histogram. The content and information of each shared image cannot be easily perceived. The histogram of all shared images are almost similar making it very difficult to be distinguished between one shared image to the other. While all shared images are involved to generate

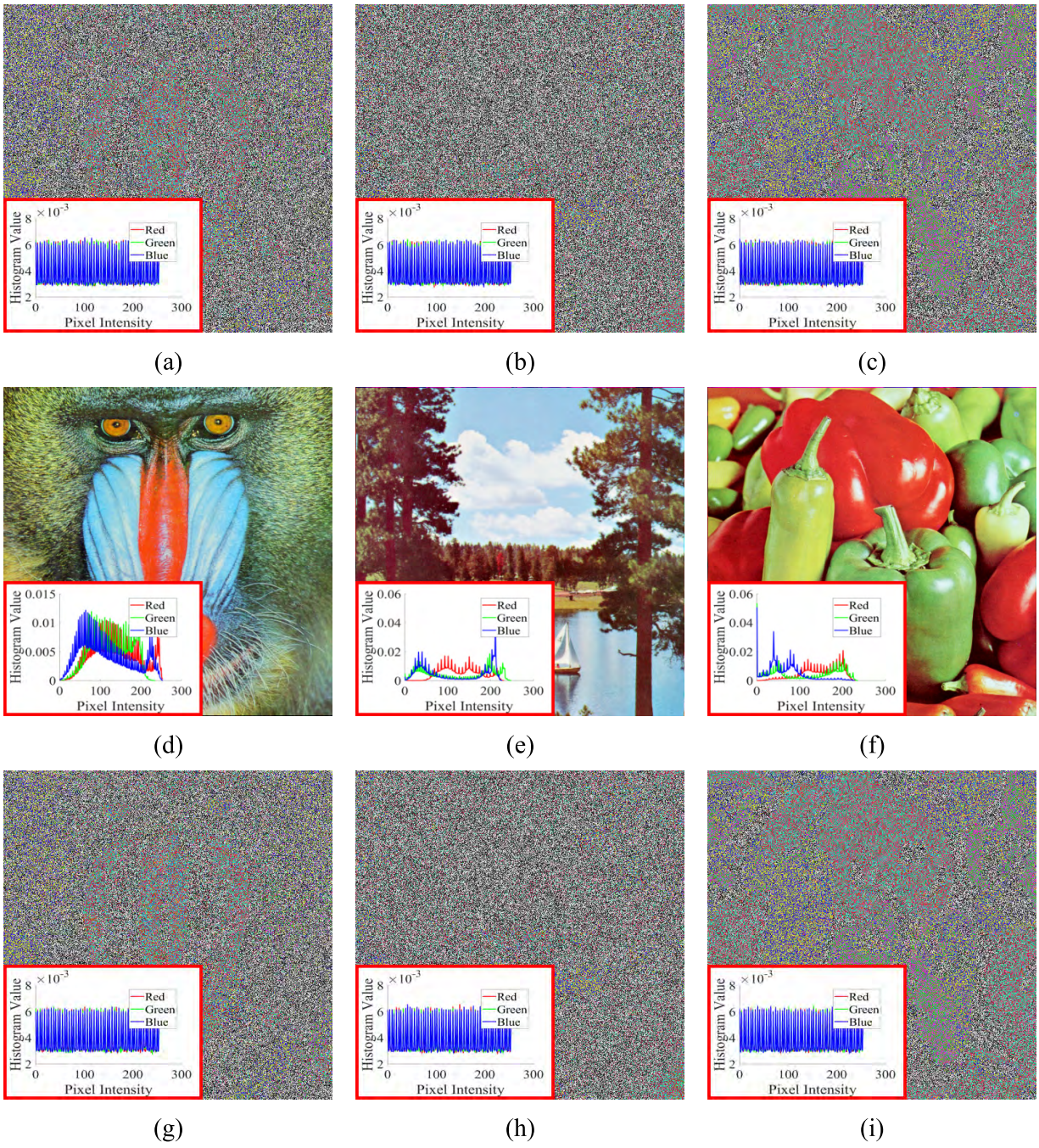

FIGURE 9. Result of the proposed method with symmetric masking coefficient while $n = 3$: (a-c) a set of shared images $\{S_1, S_2, S_3\}$, (d-f) a set of recovered secret images $\{\tilde{I}_1, \tilde{I}_2, \tilde{I}_3\}$ using correct chaotic secret key b_0, and (g-i) a set of recovered secret images $\{\tilde{I}_1, \tilde{I}_2, \tilde{I}_3\}$ using incorrect chaotic secret key b_0.

a masking coefficient, one may obtain a set of correct recovered secret images as shown in Figs. 10(e-h). However, a set of recovered secret images cannot be correctly revealed out while only partial set of shared images are collected and used to generate a recovered masking coefficient. These results are confirmed in Figs. 10(i-l).

An additional experiment was also carried out to further investigate the proposed method performance while $n = 3$. Fig. 11 depicts the shared and recovered secret images using the proposed method with $n = 3$. As similar to $n = 4$, a set of recovered secret images cannot be correctly obtained while using the partial set of shared images. It proves that the proposed method is workable for n even and odd number. This finding also confirms that the proposed (n, n)-MSS method satisfies the correctness aspect of a good MSS algorithm design which requires n contributed shared images to correctly reconstruct a set of recovered secret images.

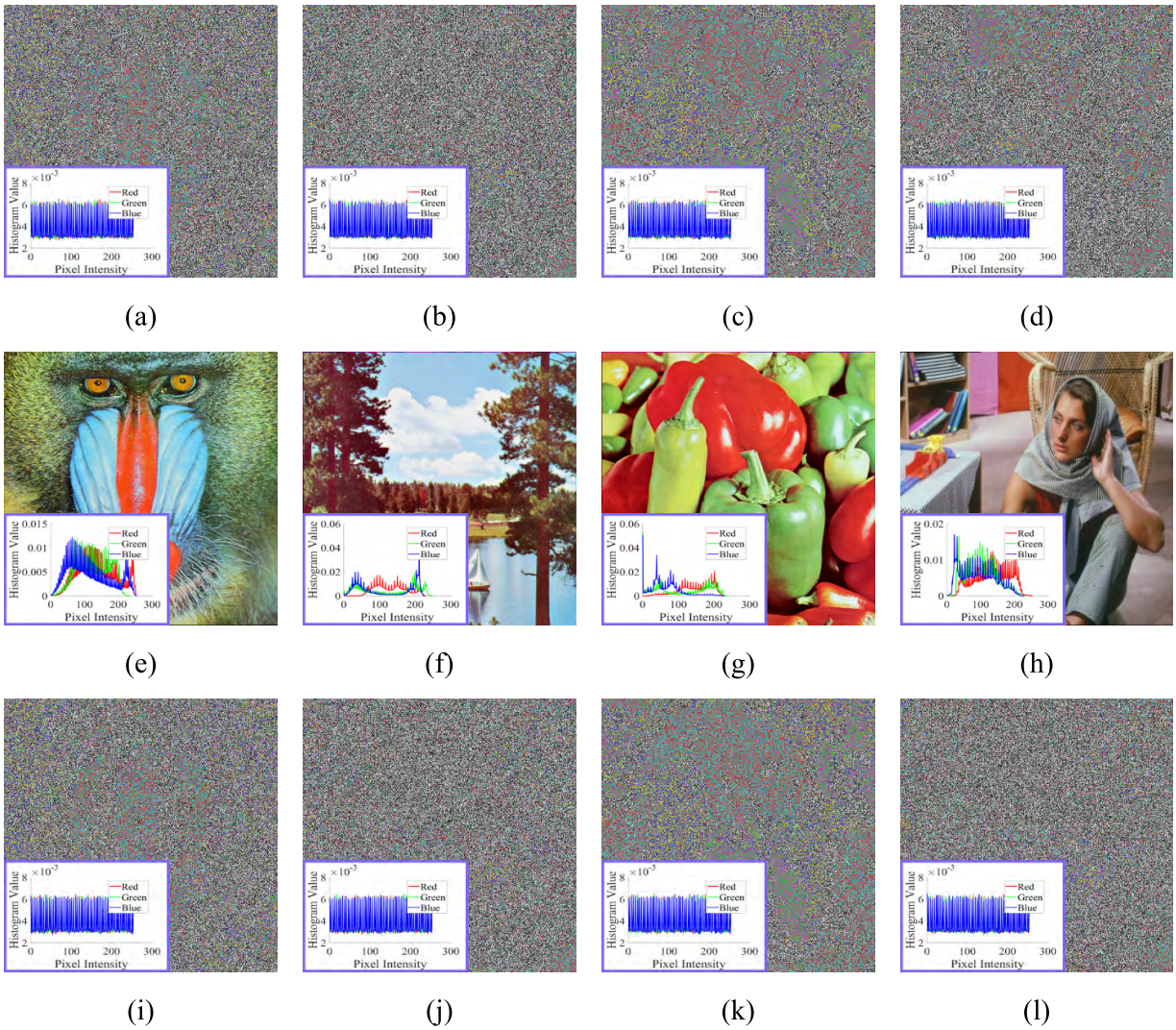

FIGURE 10. Result of the proposed method with transferred masking coefficient while $n = 4$: (a-d) a set of shared images $\{S_1, S_2, S_3, S_4\}$, (e-h) a set of recovered secret images $\{\tilde{I}_1, \tilde{I}_2, \tilde{I}_3, \tilde{I}_4\}$ while all shared images are available, (i-k) a set of recovered secret images $\{\tilde{I}_1, \tilde{I}_2, \tilde{I}_3\}$ using three shared images $\{S_1, S_2, S_3\}$, (l) recovered secret image $\tilde{I}_2$ using two shared images $\{S_1, S_2\}$.

D. PROPOSED METHOD PERFORMANCE USING HYPERCHAOTIC IMAGE SCRAMBLING

The performance of the proposed method is delivered in this section while all secret images are firstly scrambled using hyperchaotic image permutation. Herein, the number of secret images is firstly chosen as $n = 4$. Six hyperchaotic scrambling methods as given in Table 1 are applied for each secret image. In total, there are 24 hyperchaotic scrambled images which are regarded as secret images, i.e. $n = 24$. A hyperchaotic secret key is chosen as $\{x_0 = 0.0394, y_0 = 0.001\}$ for initial seed of hyperchaotic scrambling process. The CRT secret key is identically set as used in the previous experiment. Fig. 12 shows the result of the proposed method using hyperchaotic method with the symmetric masking coefficient. Because of space limitation, only four images are reported in this experiment. Figs. 12(a-b) are the scrambled images using hyperchaotic type 1 and 2 from the Babbon image, respectively. While Figs. 12(c-d) are the results of using hyperchaotic type 1 and 2, respectively, from the Lake images. Figs. 12(e-h) show some shared images produced by the proposed method. Figs. 12(i-l) are a set of recovered secret images obtained by the proposed method using correct hyperchaotic secret key. Figs. 12(m-p) give a set of recovered secret images computed by the proposed method using incorrect hyperchaotic secret key.

The similar phenomenon can be further deducted for the proposed method using the transferred masking coefficient and hyperchaotic scrambling method. The result is reported in Fig. 13. As it can be seen from this figure, a set of recovered secret images can be correctly obtained by using correct hyperchaotic secret key. Whereas, one cannot receive a set of recovered secret images correctly with incorrect hyperchaotic secret key even though all shared images are collected and obtained for generating the recovered masking coefficient. This result is reported in Figs. 13(m-p). It clearly reveals that the proposed method performance can be improved by

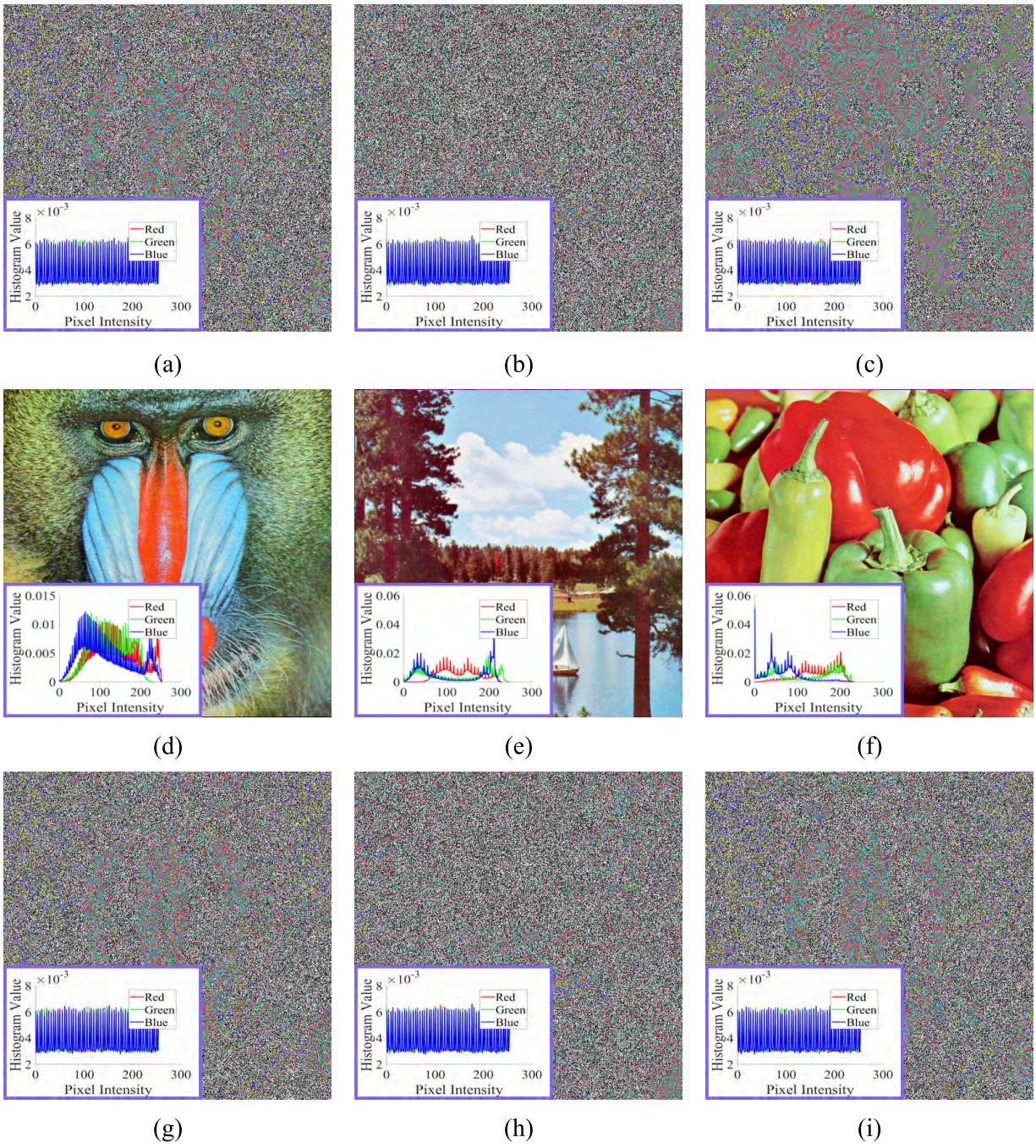

FIGURE 11. Result of the proposed method with transferred masking coefficient while $n = 3$: (a-c) a set of shared images $\{S_1, S_2, S_3\}$, (d-f) a set of recovered secret images $\{\tilde{I}_1, \tilde{I}_2, \tilde{I}_3\}$ while all shared images are available, (g-h) a set of recovered secret images $\{\tilde{I}_1, \tilde{I}_2\}$ using two shared images $\{S_1, S_2\}$, (i) recovered image $\tilde{I}_1$ using one shared images S_1.

incorporating the hyperchaotic image scrambling method. Yet, the proposed method can be regarded as a good candidate for sharing secret information in (n, n)-MSS framework.

E. INTEGRATING HYPERCHAOTIC IMAGE SCRAMBLING AND PIXEL MERGING APPROACH INTO COMPLETE (n, n)-MSS

This subsection elaborates some experiments which integrate the hyperchaotic image scrambling and the pixel merging approach into the complete (n, n)-MSS task. This integration technique aims to improve the security level of secret image communication in the MSS application. Herein, the hyperchaotic image scrambling firstly confuses the content of all secret images. The scrambled secret images are further fed into the proposed (n, n)-MSS module to obtain a set of shared images. The mode of proposed (n, n)-MSS can be selected as with symmetric or transferred masking coefficient depending on the user requirement. All generated shared images are

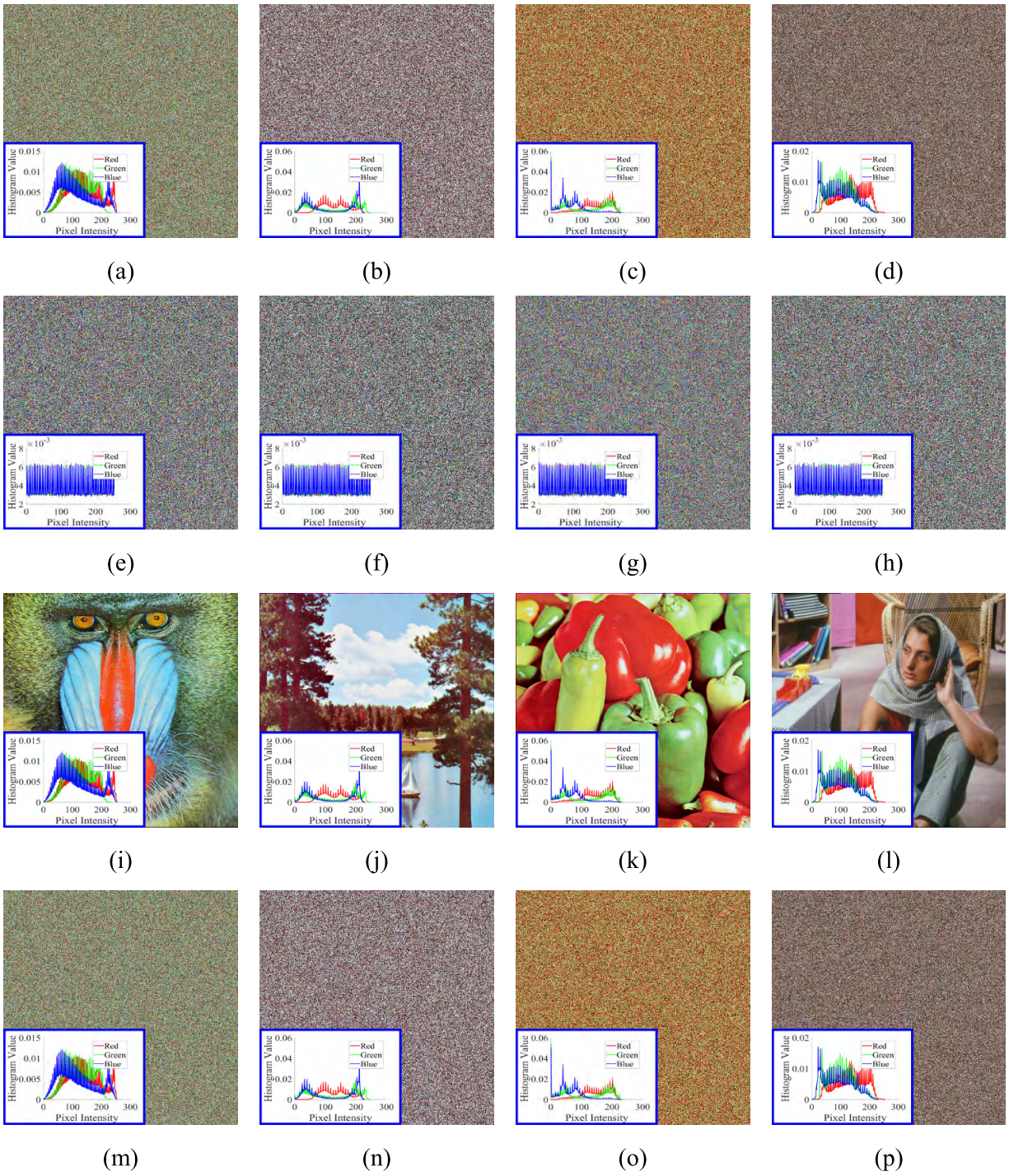

FIGURE 12. Result of the proposed method with hyperchaotic image scrambling and symmetric masking coefficient while $n = 4$: (a-d) a set of secret images after hyperchaotic process $\{I_1^1, I_2^1, I_3^1, I_4^1\}$, (e-h) a set of shared images $\{S_1^1, S_2^1, S_3^1, S_4^1\}$, (i-l) a set of recovered secret images using correct hyperchaotic secret key, and (m-p) a set of recovered secret images using incorrect hyperchaotic secret key.

subsequently converted into lower dimensional representation, i.e. two dimensional matrix representation, before transferring to the receiver module. The reverse process should be applied in the receiver module to obtain a set of correct recovered secret images.

In this experiment, we firstly investigate the effect of integration between the image scrambling and merging into two dimensional matrix approaches in the proposed (n, n)-MSS with symmetric masking coefficient. All secret images are simply permuted using some hyperchaotic image scrambling methods to obtain a set of scrambled secret images. The hyperchaotic secret key is set as $\{x_0 = 0.0394, y_0 = 0.001\}$ for all six hyperchaotic types. This approach also requires some additional secret chaotic

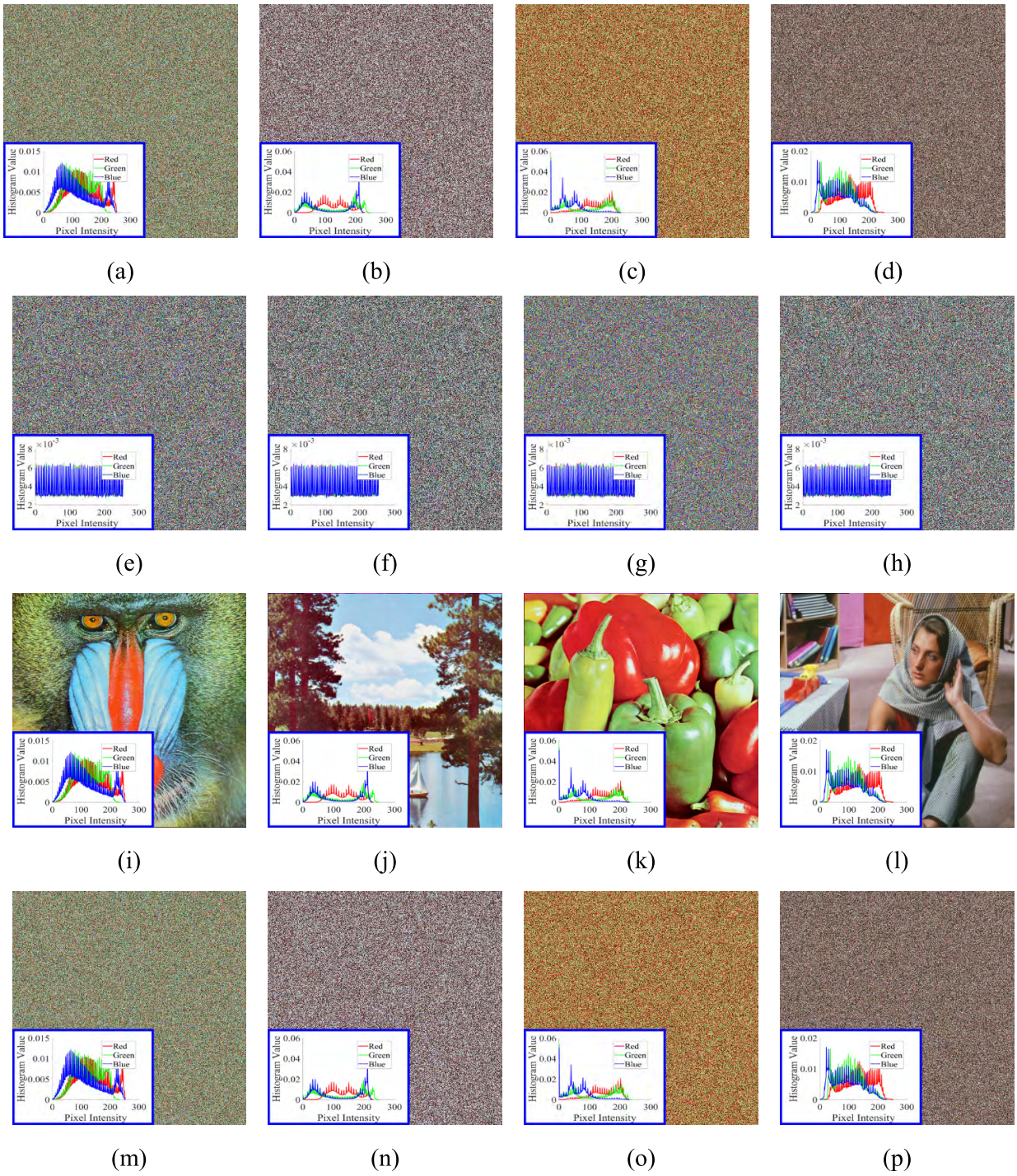

FIGURE 13. Result of the proposed method with hyperchaotic image scrambling and transferred masking coefficient while $n = 4$: (a-d) a set of secret images after hyperchaotic process $\{I_1^1, I_2^1, I_3^1, I_4^1\}$, (e-h) a set of shared images $\{S_1^1, S_2^1, S_3^1, S_4^1\}$, (i-l) a set of recovered secret images using correct hyperchaotic secret key, and (m-p) a set of recovered secret images using incorrect hyperchaotic secret key.

keys, i.e. $b_0 = \{0.034, 0.401, 0.875\}$ and $\alpha = 4$, to generate the random image or symmetric masking coefficient. Subsequently, each pixel in each shared image consisting three-tuples colors is then merging into one value by performing CRT process before transmitting to the receiver module. Herein, the CTR secret key for merging purpose is set as $\{331, 337, 349\}$. It indicates that each pixel of shared image needs $\lceil \log_2 331 \times 337 \times 349 \rceil \approx 26$ bits in the new representation (two dimensional approach). Yet, it requires two more bits compared to that of representing in original RGB color tuples.

Figs. 14(a-d) depict a set of shared images in two dimensional image representation. As shown in these figures, all shared images are now in two dimensional matrix form in

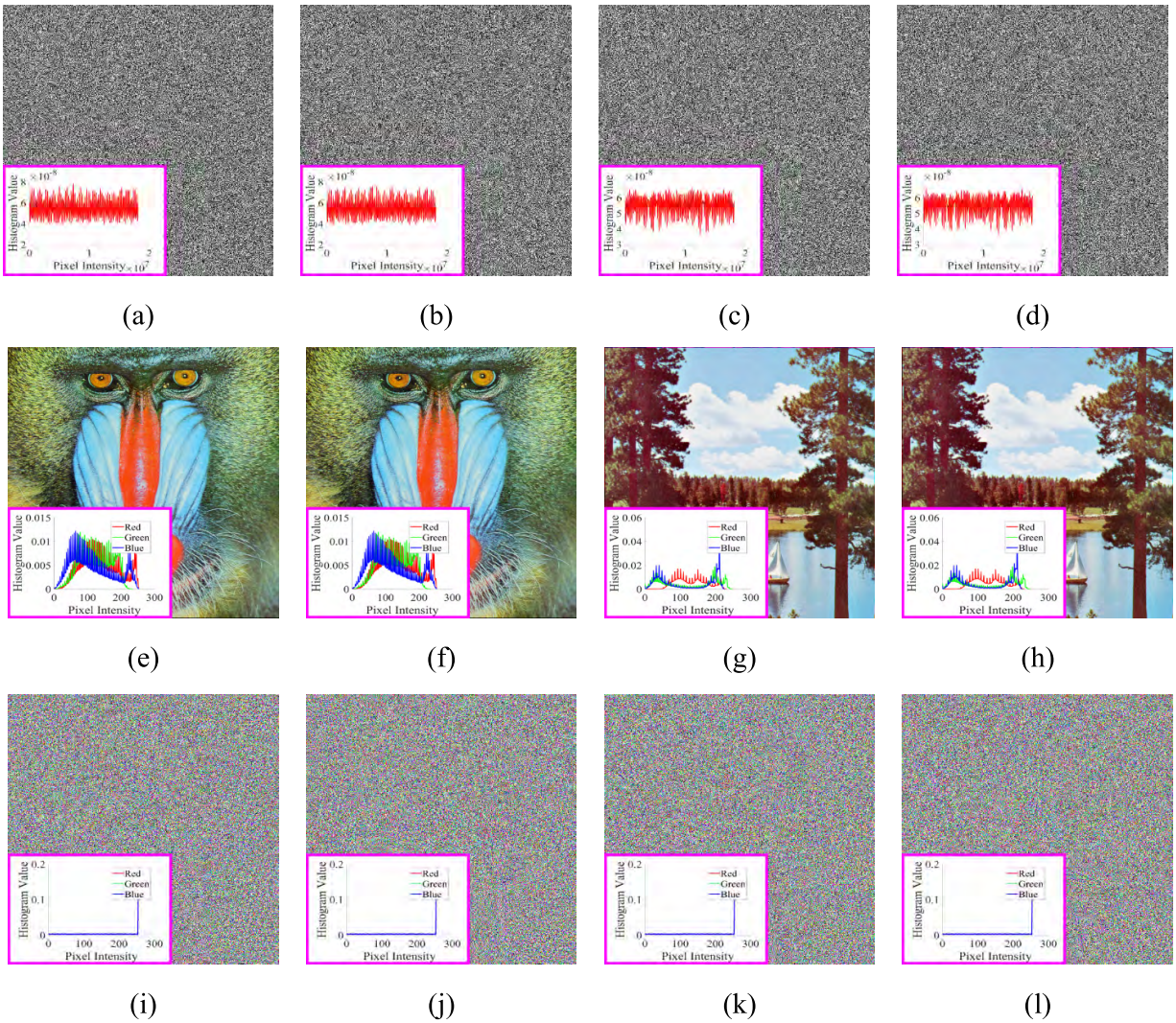

FIGURE 14. Proposed method performance by integrating hyperchaotic image scrambling, symmetric masking coefficient, and merging into two dimensional matrix strategy while $n = 4$: (a-d) a set of shared images in two dimensional image representation, (e-h) a set of recovered secret images using correct CRT secret key, and (i-l) a set of recovered secret images using incorrect CRT secret key.

which a single histogram is enough to summarize the image intensity. Figs. 14(e-h) show some recovered secret images using correct CRT secret key, whereas Figs. 14(i-l) display some recovered secret images obtained using incorrect CRT secret key, i.e. {311, 313, 317}. The proposed method performance can be improved by performing an additional step, i.e. merging process into two dimensional matrix representation, before sending a set of shared images into receiver module.

Another experiment was conducted to investigate the integration result between the hyperchaotic image scrambling and merging two dimensional matrix into the proposed (n, n)-MSS system with transferred masking coefficient. In this case, a set of shared images are obtained with the transferred masking coefficient approach by selecting CRT secret key as $\{3, 5, 17\}$. The reason of choosing this CRT secret key is to prevent a big number representation on two dimensional merging result. This CRT secret key indicates that each pixel of shared images lies on interval $[0, 255]$. Whereas, this approach involves the CRT secret key $\{331, 337, 349\}$ to perform the merging operation into two dimensional matrix.

TABLE 2. Performance evaluation of the proposed method in terms of similarity between the secret and recovered images.

Secret and Recovered Images	Correlation	RMSE	PSNR	MAE	NPCR	UACI
$I_1, \tilde{I}_1$	1	0	∞	0	0	0
$I_2, \tilde{I}_2$	1	0	∞	0	0	0
$I_3, \tilde{I}_3$	1	0	∞	0	0	0
$I_4, \tilde{I}_4$	1	0	∞	0	0	0

Figs. 15(a-d) show a set of shared images after performing a merging process. Each shared image is now in two dimensional matrix representation. In contrast, the inverse CRT process is then applied on receiver side with identical CRT secret key to correctly obtain a set of recovered secret images. Figs. 15(e-h) are a set of recovered secret images by

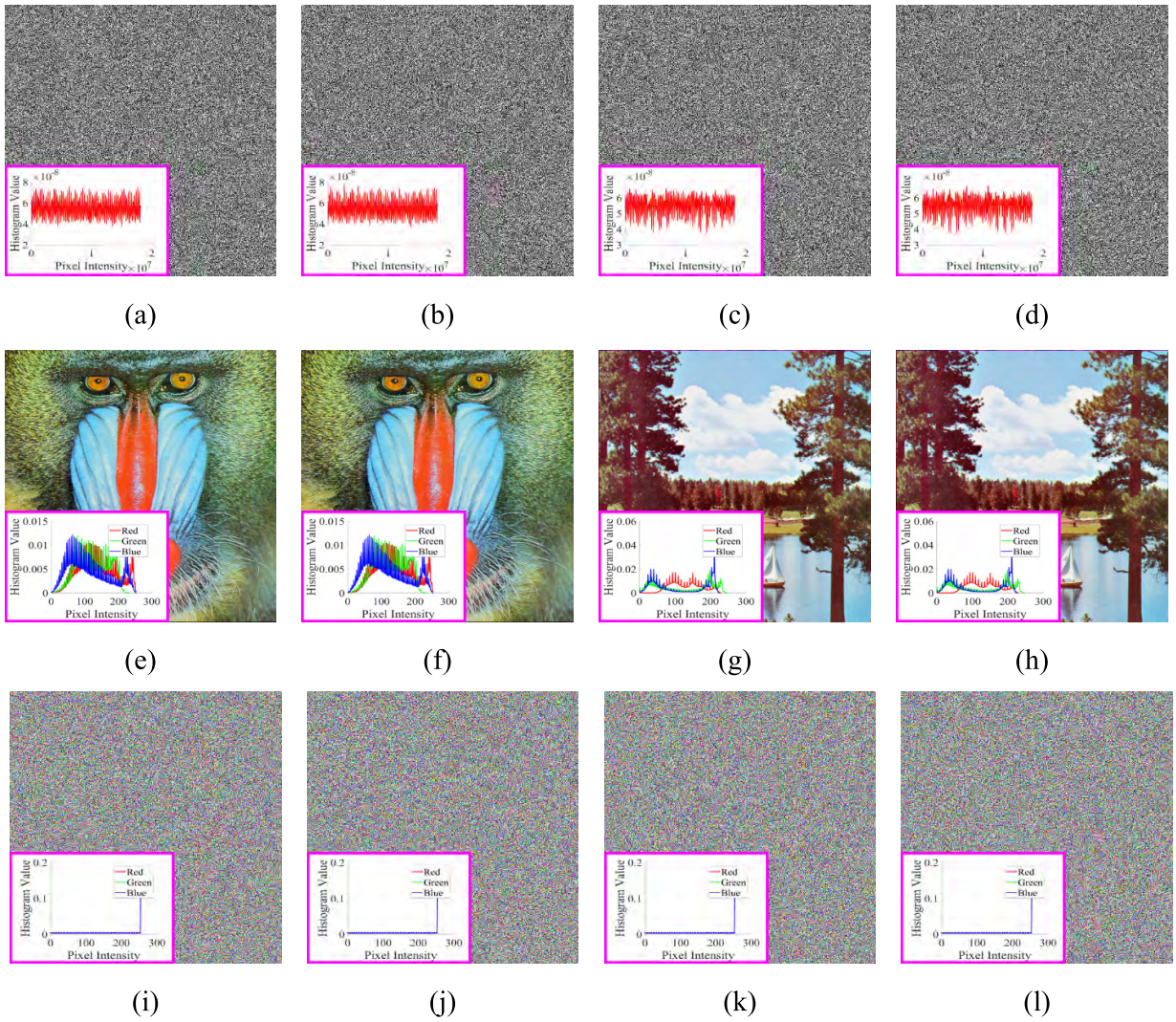

FIGURE 15. Proposed method performance by integrating hyperchaotic image scrambling, transferred masking coefficient, and merging into two dimensional matrix strategy while $n = 4$: (a-d) a set of shared images in two dimensional image representation, (e-h) a set of recovered secret images using correct CRT secret key, and (i-l) a set of recovered secret images using incorrect CRT secret key.

applying correct CRT and hyperchaotic secret keys. Whereas Figs. 15(i-l) illustrate a set of recovered secret images by applying incorrect CRT secret key, i.e. {311, 313, 317}, but with correct hyperchaotic secret key. In these figures, one obtains nothing with incorrect CRT secret key. These two experiments validates that the integration approach between the hyperchaotic image scrambling and merging into two dimensional matrix in the proposed method (with symmetric or transferred masking coefficient) yields satisfactory results. In addition, this integration scheme improves the security level of (n, n)-MSS method on delivering secret messages via digital imaginary data.

F. PERFORMANCE COMPARISON BETWEEN THE PROPOSED METHOD AGAINST FORMER EXISTING SCHEMES

Some additional experiments are conducted to further examine and investigate the proposed method performance against the former existing schemes in MSS domain. The performance of the proposed method is firstly evaluated by measuring the similarity between a set of secret images and its recovered version in terms of correlation, RMSE, PSNR, MAR, NPCR, and UACI scores. In this experiment, the CRT secret key for computing the masking coefficient is simply set as {3, 5, 17}. Table 2 gives performance evaluation for the proposed scheme with symmetric masking coefficient, transferred masking coefficient, hyperchaotic, and merging into two dimensional matrix. As it can be seen from this table, the proposed method identically produces a set of secret and recovered images indicated with high correlation value, zeros for RMSE, MAE, NPCR, and UACI. The proposed method yields ∞ for PNSR score meaning that secret image is totally the same as recovered secret image. The performance of the proposed method is also investigated under differential attacks. These evaluations are measured in terms of MAE, NPCR, and UACI scores. Table 3 reports this evaluation for the proposed method. From this table, the proposed method yields good results under differential

TABLE 3. Performance evaluation of the proposed method in terms of differential attacks. The abbreviations are as follow: Proposed method with symmetric masking coefficient (PM-SMC), proposed method with transferred masking coefficient (PM-TMC), proposed method with symmetric masking coefficient and hyperchaotic image scrambling (PM-SMC-H), proposed method with transferred masking coefficient and hyperchaotic image scrambling (PM-TMC-H), and proposed method with merging into two dimensional matrix (PM-MTD).

Secret and Shared Image	PM-SMC			PM-TMC			PM-SMC-H			PM-TMC-H			PM-MTD		
	MAE	NPCR	UACI	MAE	NPCR	UACI	MAE	NPCR	UACI	MAE	NPCR	UACI	MAE	NPCR	UACI
I_1, S_1	76.10	99.16	29.84	76.12	99.57	29.85	76.41	99.61	29.97	76.42	99.61	29.97	76.42	99.61	29.97
I_1, S_2	76.39	99.61	29.96	76.35	99.61	29.94	76.38	99.61	29.95	76.41	99.60	29.97	76.41	99.60	29.97
I_1, S_3	76.39	99.62	29.96	76.30	99.61	29.92	76.28	99.61	29.92	76.27	99.61	29.91	76.27	99.61	29.91
I_1, S_4	76.45	99.62	29.98	76.40	99.61	29.96	76.36	99.61	29.95	76.36	99.61	29.94	76.36	99.61	29.94
I_2, S_1	82.21	99.61	32.24	82.14	99.61	32.21	82.17	99.61	32.22	82.20	99.61	32.24	82.20	99.61	32.24
I_2, S_2	81.86	99.16	32.10	81.90	99.57	32.12	82.17	99.61	32.22	82.20	99.61	32.24	82.20	99.61	32.24
I_2, S_3	82.30	99.62	32.28	82.11	99.61	32.20	82.13	99.61	32.21	82.14	99.61	32.21	82.14	99.61	32.21
I_2, S_4	82.27	99.61	32.26	82.22	99.61	32.24	82.17	99.61	32.22	82.17	99.61	32.22	82.17	99.61	32.22
I_3, S_1	82.28	99.62	32.27	82.23	99.61	32.25	82.27	99.60	32.26	82.24	99.61	32.25	82.24	99.61	32.25
I_3, S_2	82.30	99.62	32.27	82.18	99.61	32.23	82.22	99.62	32.24	82.25	99.61	32.25	82.25	99.61	32.25
I_3, S_3	81.92	99.16	32.12	81.97	99.57	32.15	82.08	99.61	32.19	82.17	99.61	32.22	82.17	99.61	32.22
I_3, S_4	82.24	99.61	32.25	82.25	99.62	32.25	82.17	99.61	32.22	82.16	99.61	32.22	82.16	99.61	32.22
I_4, S_1	76.03	99.62	29.82	75.96	99.61	29.79	76.03	99.61	29.82	75.99	99.61	29.80	75.99	99.61	29.80
I_4, S_2	76.03	99.61	29.81	75.99	99.61	29.80	75.95	99.61	29.79	75.94	99.61	29.78	75.94	99.61	29.78
I_4, S_3	75.97	99.61	29.79	75.94	99.62	29.78	75.92	99.61	29.77	75.91	99.61	29.77	75.91	99.61	29.77
I_4, S_4	75.71	99.16	29.69	75.81	99.57	29.73	76.02	99.61	29.81	75.90	99.61	29.77	75.90	99.61	29.77
Average	79.15	99.50	31.04	79.12	99.60	31.03	79.17	99.61	31.05	79.17	99.61	31.05	79.17	99.61	31.05

attacks as indicated with high NPCR score, and low values of MAE and UACI.

It will be more interesting to further compare the proposed method performance against several former existing schemes [15]–[21] in MSS domain. The experimental settings are identically maintained for all methods to make a fair comparison. Table 4 reports the performance comparison between the proposed method and former schemes in terms of correlation, RMSE, and PSNR scores over a set of secret and shared images. As reported in this table, the proposed method yields better performance compared to that of the former schemes based on the correlation, RMSE, and PSNR scores.

Table 5 demonstrates the performance comparison between the proposed method and former scheme in terms of correlation, RMSE, and PSNR scores over a set of shared images. The proposed method gives better performance compared to the former schemes in terms of average correlation coefficient as it can be seen in Table 5. This average score is higher than the former scheme and almost 1, indicating that each shared image is positively correlated to the other shared image. All shared images are very hard to be distinguished by human perception. It means that all shared images are very hard to be cryptanalyzed. This table also shows that the average PSNR score is low and the average RMSE is very high indicating that all shared images are not similar with each other. Thus, the proposed method is superior compared to the former existing schemes.

An additional comparison is then conducted between the proposed method and former schemes [15]–[21] in terms of randomness, recovery strategy, sharing capacity, etc. Table 6 summarizes this comparison. As it can be seen from this table, the proposed method offers better advantage compared to the former schemes [15]–[21] especially in randomness aspect. It clearly reveals that the proposed method can be viewed as a good candidate for (n, n)-MSS with avoiding the ambiguity if the number of secret images n is even or odd.

G. SECURITY ANALYSIS OF THE PROPOSED METHOD

This subsection discusses the security analysis of the proposed method. The security of MSS can be simply investigated by overlooking the pixel values of secret image and shared image [22]. This analysis involves the randomness investigation of shared image and combination of secret image. Let I and S be pixel of original secret image and shared image, respectively. There are four types of security level of SS and MSS based on the value of S, as given follow [22]:

Level 1: S is random. This condition implies that $Pr\{S = i\} = \frac{1}{P}$ for $i = \{1, 2, \ldots, P\}$. This level resembles "one-time pads" security and the most secure encryption.

Level 2: S is random and/or $S = c$, where c denotes a specific constant value. The values of I and c are uncorrelated. Thus, the information of I cannot be perceived and obtained from the value of S.

Level 3: $S = f(I^e)$. The symbols $f(\cdot)$ and I^e are the relational function and encrypted result of I, respectively. In this security level, the value of S depends on the encrypted version of I. If $I^e = I$, the the security level of S is only affected from original I. Herein, the security of SS or MSS depends on the encryption method, not on the SS or MSS itself.

TABLE 4. Performance comparisons between the proposed method and former schemes in terms of quantitative results over secret and shared images.

Correlation									
Secret and Shared Images	Chen [15]	Chen [16]	Yang [17]	Deshmukh [21]	PM-SMC	PM-TMC	PM-SMC-H	PM-TMC-H	PM-MTD
I_1, S_1	0.00	−0.0162	0.03	−0.0023	0.00	0.01	0.00	0.00	0.00
I_1, S_2	0.02	0.01	−0.0258	−0.0039	0.00	0.00	0.00	0.00	0.00
I_1, S_3	−0.0169	−0.0027	0.07	0.00	0.00	0.00	0.00	0.00	0.00
I_1, S_4	−0.0130	0.11	−0.1301	0.00	0.00	0.00	0.00	0.00	0.00
I_2, S_1	0.00	0.01	−0.0057	0.00	0.00	0.00	0.00	0.00	0.00
I_2, S_2	−0.0224	0.02	0.03	−0.0014	0.01	0.01	0.00	0.00	0.00
I_2, S_3	0.10	0.01	0.00	0.00	0.00	0.00	0.00	0.00	0.00
I_2, S_4	−0.0518	0.01	0.05	−0.0023	0.00	0.00	0.00	0.00	0.00
I_3, S_1	0.00	−0.0025	0.08	0.00	0.00	0.00	0.00	0.00	0.00
I_3, S_2	0.02	−0.0032	−0.0085	0.00	0.00	0.00	0.00	0.00	0.00
I_3, S_3	0.07	−0.0079	0.04	−0.0017	0.00	0.00	0.00	0.00	0.00
I_3, S_4	0.17	0.01	0.03	0.00	0.00	0.00	0.00	0.00	0.00
I_4, S_1	−0.0015	−0.0081	−0.0955	0.00	0.00	0.00	0.00	0.00	0.00
I_4, S_2	0.01	0.01	0.03	−0.0037	0.00	0.00	0.00	0.00	0.00
I_4, S_3	−0.0409	0.11	0.05	0.00	0.00	0.00	0.00	0.00	0.00
I_4, S_4	0.05	−0.0043	0.04	−0.0004	0.01	0.00	0.00	0.00	0.00
Average	0.05	0.03	0.04	0.00	0.00	0.00	0.00	0.00	0.00
RMSE									
Secret and Shared Images	Chen [15]	Chen [16]	Yang [17]	Deshmukh [21]	PM-SMC	PM-TMC	PM-SMC-H	PM-TMC-H	PM-MTD
I_1, S_1	10.92	10.68	10.53	10.77	92.58	92.55	92.83	92.85	92.85
I_1, S_2	11.47	10.83	10.94	10.81	92.82	92.78	92.80	92.84	92.84
I_1, S_3	10.52	10.88	10.81	10.79	92.81	92.73	92.71	92.71	92.71
I_1, S_4	11.16	10.11	10.93	10.78	92.88	92.86	92.81	92.80	92.80
I_2, S_1	10.73	10.58	10.53	10.62	100.08	100.01	100.04	100.08	100.08
I_2, S_2	10.86	10.64	10.80	10.58	99.76	99.81	100.02	100.04	100.04
I_2, S_3	10.47	10.75	10.61	10.58	100.14	99.98	100.00	100.01	100.01
I_2, S_4	10.68	10.68	10.68	10.61	100.14	100.09	100.06	100.05	100.05
I_3, S_1	10.26	9.88	9.92	10.11	100.36	100.38	100.38	100.37	100.37
I_3, S_2	10.40	10.03	10.05	9.97	100.35	100.28	100.32	100.34	100.34
I_3, S_3	9.87	10.06	10.27	9.95	100.07	100.11	100.22	100.28	100.28
I_3, S_4	10.66	9.94	10.30	10.15	100.38	100.36	100.30	100.28	100.28
I_4, S_1	10.03	9.39	9.74	9.53	92.35	92.29	92.35	92.31	92.31
I_4, S_2	10.38	9.50	9.92	9.52	92.34	92.30	92.28	92.26	92.26
I_4, S_3	9.66	8.81	9.88	9.56	92.30	92.24	92.24	92.22	92.22
I_4, S_4	10.29	9.44	9.97	9.45	92.07	92.13	92.34	92.21	92.21
Average	10.52	10.14	10.37	10.24	96.34	96.31	96.36	96.35	96.35
PSNR									
Secret and Shared Images	Chen [15]	Chen [16]	Yang [17]	Deshmukh [21]	PM-SMC	PM-TMC	PM-SMC-H	PM-TMC-H	PM-MTD
I_1, S_1	27.40	27.59	27.71	27.52	8.81	8.81	8.78	8.78	8.78
I_1, S_2	26.97	27.47	27.38	27.49	8.79	8.79	8.79	8.78	8.78
I_1, S_3	27.73	27.43	27.49	27.51	8.79	8.79	8.80	8.80	8.80
I_1, S_4	27.21	28.07	27.39	27.51	8.78	8.78	8.79	8.79	8.79
I_2, S_1	27.56	27.67	27.72	27.64	8.17	8.18	8.18	8.17	8.17
I_2, S_2	27.45	27.63	27.50	27.68	8.20	8.20	8.18	8.18	8.18
I_2, S_3	27.77	27.54	27.65	27.67	8.17	8.18	8.18	8.18	8.18
I_2, S_4	27.60	27.60	27.60	27.65	8.17	8.17	8.17	8.17	8.17
I_3, S_1	27.94	28.27	28.24	28.07	8.13	8.12	8.12	8.13	8.13
I_3, S_2	27.82	28.14	28.12	28.19	8.13	8.13	8.13	8.13	8.13
I_3, S_3	28.28	28.11	27.93	28.20	8.15	8.15	8.14	8.13	8.13
I_3, S_4	27.61	28.22	27.91	28.04	8.13	8.13	8.13	8.13	8.13
I_4, S_1	28.18	28.71	28.40	28.59	8.83	8.83	8.83	8.83	8.83
I_4, S_2	27.84	28.61	28.23	28.60	8.83	8.83	8.83	8.83	8.83
I_4, S_3	28.47	29.27	28.27	28.55	8.83	8.84	8.84	8.84	8.84
I_4, S_4	27.91	28.67	28.19	28.66	8.85	8.85	8.83	8.84	8.84
Average	27.73	28.06	27.86	27.97	8.48	8.49	8.48	8.48	8.48

Level 4: $S = f(I)$. In this case, the security of SS and MSS only depends on the relational function of I. The S may contain partial information from I making it very easy to get cryptanalysis.

TABLE 5. Performance comparisons between the proposed method and former schemes in terms of quantitative results over shared images.

Correlation									
Shared Images	Chen [15]	Chen [16]	Yang [17]	Deshmukh [21]	PM-SMC	PM-TMC	PM-SMC-H	PM-TMC-H	PM-MTD
S_1, S_2	−0.0002	0.03	0.04	0.03	0.04	0.04	0.01	0.01	0.01
S_1, S_3	−0.0038	−0.1014	0.04	0.04	0.06	0.06	0.06	0.06	0.06
S_1, S_4	0.00	0.02	0.00	0.01	0.04	0.04	0.03	0.03	0.03
S_2, S_3	0.05	0.04	−0.0816	−0.0123	-0.02	-0.03	0.06	0.06	0.06
S_2, S_4	0.01	0.00	0.06	0.16	0.05	0.05	0.03	0.03	0.03
S_3, S_4	0.00	0.02	0.01	0.04	0.12	0.12	0.03	0.03	0.03
Average	0.02	0.02	0.03	0.06	0.05	0.05	0.04	0.04	0.04
RMSE									
Shared Images	Chen [15]	Chen [16]	Yang [17]	Deshmukh [21]	PM-SMC	PM-TMC	PM-SMC-H	PM-TMC-H	PM-MTD
S_1, S_2	10.92	10.76	11.01	10.61	102.16	102.28	103.84	103.87	103.87
S_1, S_3	10.47	10.96	10.80	10.60	101.25	101.20	101.15	101.17	101.17
S_1, S_4	10.88	10.85	10.91	10.54	102.67	102.70	102.88	102.90	102.90
S_2, S_3	10.05	10.71	10.75	10.71	105.82	105.87	101.21	101.15	101.15
S_2, S_4	10.78	10.75	10.89	10.49	101.97	102.08	102.97	102.93	102.93
S_3, S_4	11.00	10.87	10.82	10.65	98.20	98.15	102.99	102.97	102.97
Average	10.68	10.82	10.86	10.60	102.01	102.04	102.51	102.50	102.50
PSNR									
Shared Images	Chen [15]	Chen [16]	Yang [17]	Deshmukh [21]	PM-SMC	PM-TMC	PM-SMC-H	PM-TMC-H	PM-MTD
S_1, S_2	27.40	27.53	27.33	27.65	7.95	7.94	7.80	7.80	7.80
S_1, S_3	27.76	27.37	27.50	27.66	8.04	8.05	8.04	8.04	8.04
S_1, S_4	27.43	27.46	27.41	27.71	7.90	7.90	7.89	7.88	7.88
S_2, S_3	28.12	27.57	27.53	27.57	7.64	7.64	8.04	8.04	8.04
S_2, S_4	27.57	27.53	27.42	27.75	7.96	7.95	7.88	7.88	7.88
S_3, S_4	27.34	27.48	27.48	27.61	8.30	8.31	7.88	7.88	7.88
Average	27.60	27.49	27.45	27.66	7.97	7.96	7.92	7.92	7.92

TABLE 6. Comparison between the proposed method and former schemes.

Parameters	Chen [16]	Chen [17]	Yang [18]	Feng [19]	Guo [20]	Guo [21]	Deshmukh [22]	Proposed Method
Image Type	Grayscale	Grayscale	Binary	Binary	Binary	Binary	Color	Color
Secret Sharing Scheme	$(n, n+1)$	(n, n)	(t, n)	(t, n)	(t, n)	(t, n)	(n, n) while n is even number	(n, n) with n is even/odd number
Multi-Threshold	No	No	Yes	Yes	Yes	Yes	No	No
Pixel Expansion	No	No	No	No	No	No	No	No
Information Reveal	Partial	Partial	Partial	Partial	Partial	Partial	No	No
Combination of Secrets	No	No	No	No	No	No	Yes	Yes
Randomness	Low	Average	Average	Average	Average	Average	High	Very High
Recovery Strategy	XOR	XOR	Boolean	Boolean	CRT	Lagranges	CRT	CRT
Sharing Capacity	$n/(+1)$	n/n	$1/n$	$1/n$	$1/n$	$1/n$	n/n	n/n
Recovery of Secrets	Lossless	Lossless	Lossless	Lossless	Lossless	Lossless	Lossless	Lossless

The proposed (n, n)-MSS method with symmetric and transferred masking coefficient can be regarded to fall in the Level 1. Since all pixel values of shared images are uniformly distributed, i.e. $Pr\{S = i\} = \frac{1}{P}$ for $i = 1, 2, \ldots, 255$. It indicates that the proposed (n, n)-MSS method is very secure. This condition is true for the proposed method with symmetric and transferred masking coefficient with and without applying the hyperchaotic image scrambling.

However, the proposed (n, n)-method falls into the Level 4 if the hyperchaotic image scrambling is not applied to the secret images. This condition occurs for the proposed method with symmetric and transferred masking coefficient. The proposed method is with the Level 4 if two or more shared images are overlaid with the XOR operation. Fig. 16(a) is overlying result of two shared images, i.e. $S_1 \oplus S_2$, whereas Fig. 16(b) is the result of $S_3 \oplus S_4$. We can have a clue about image content while two or more shared images are overlaid. This phenomenon can be analyzed as $S_1 \oplus S_2 = (I_1 \oplus R) \oplus (I_2 \oplus R) = I_1 \oplus I_2 \oplus R \oplus R = I_1 \oplus I_2$. Overlying two shared images is similar to perform the XOR operation between two original secret images. Thus, there is a clue about the image content if the hyperchaotic image is not applied to the proposed method. It is a reason why the hyperchaotic image scrambling is injected into the proposed method.

The proposed (n, n)-MSS method may falls in the Level 3 if the hyperchaotic image scrambling is utilized. This security

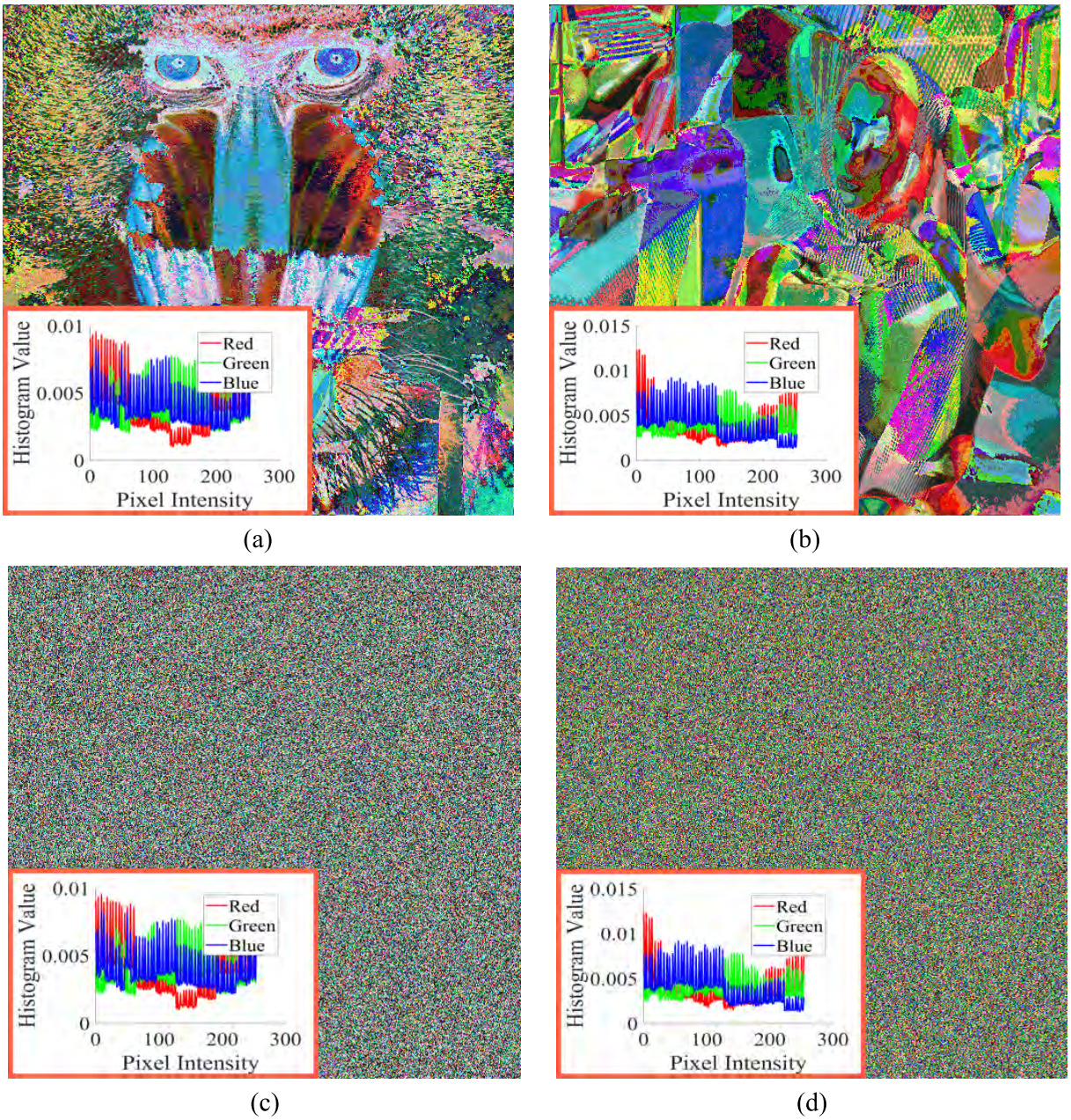

FIGURE 16. Effect of overlying two shared images: (a) $S_1 \oplus S_2$ and (b) $S_3 \oplus S_4$ while the hyperchaotic image scrambling is not applied to the secret images. Where (c-d) are $S_1 \oplus S_2$ and $S_3 \oplus S_4$, respectively while the secret images are confussed with the hyperchaotic image scrambling.

level is confirmed in Fig. 16. Herein, Fig. 16(c) and (d) show the overlying two shared images, i.e. $S_1 \oplus S_2$ and $S_3 \oplus S_4$, respectively, while all secret images are firstly confussed with the hyperchaotic image scrambling method. As shown in these figures, the clue of image contents cannot be obtained by overlying two shared images.

It is little regrettable that the security of proposed (n, n)-MSS method with hyperchaotic image scrambling falls in the Level 4 if we consider the histogram of overlaid image. It can be clearly seen that the histogram of overlaid images is identical with or without hyperchaotic image scrambling. To improve the security level of the proposed method, an additional technique can be applied for all secret images, i.e. simple image encryption. This simple encryption is formulated as follow:

$$I_i^e = (I_i + \text{Round}\{\beta \cdot B\}) \bmod 256, \tag{53}$$

where I_i^e and I_i are the encrypted and original secret image, respectively. The B is chaotic/uniformly random number. The value of β is for scaling purpose which can be set with relatively big number, e.g. $\beta = 601257013$. Figs. 17(a-d) are the encrypted secret images, whereas Figs. 17(e-h) are the overlying results of two or more encrypted shared images. As shown in these figures, the histogram of encrypted

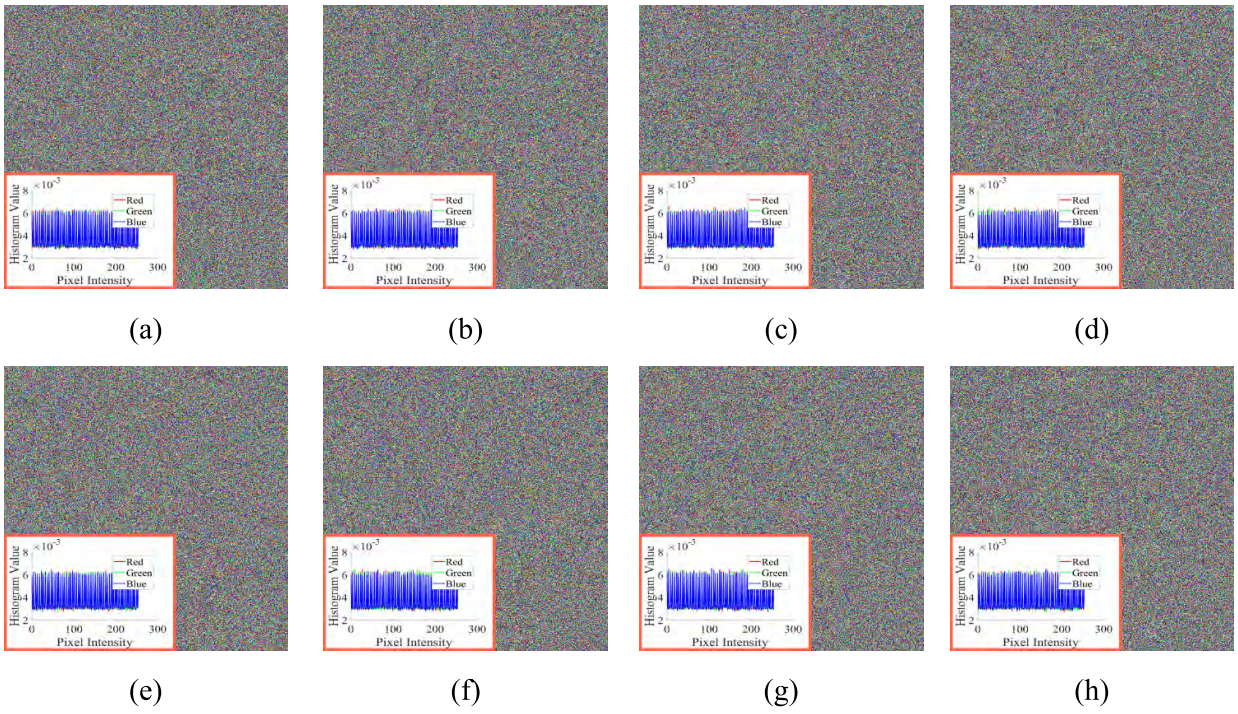

FIGURE 17. Effect of simple hyperchaotic image encryption: (a-d) encrypted images of $\{I_1, I_2, I_3, I_4\}$, overlaying several encrypted shared images (e) $S_1 \oplus S_2$, (f) $S_3 \oplus S_4$, (g) $S_1 \oplus S_2 \oplus S_3$, and (h) $S_1 \oplus S_2 \oplus S_3 \oplus S_4$.

images and overlaid encrypted shared images is uniformly distributed. The image content cannot be perceived. Thus, there is no clue about the image content of overlying two or more encrypted shared images. From this experiment, we can conclude that the security level of the proposed (n, n)-MSS method can be improved from Level 4 into Level 3 by applying simple image encryption technique. Now, the security of proposed method with image encryption scheme falls in the Level 3. This image encryption can be applied for the proposed method with symmetric and transferred masking coefficient. It is noteworthy that the security of proposed method is also in the Level 1. The proposed method is very competitive in the secure secret sharing compared to the former existing schemes.

V. CONCLUSIONS

A new method on MSS for color images has been proposed and presented in this paper. This method solves the problem occurred in the former existing MSS scheme [21] which exploits the CRT and XOR operations for generating a set of shared images. The proposed method offers a simple strategy on MSS-based color image with CRT and XOR using symmetric and transferred masking coefficients. This method overcomes the limitation of the former scheme if the number of secret images n is odd. The hyperchaotic-based MSS is also presented in this paper to further improve the security level of the proposed MSS scheme. The proposed method also involves the merging strategy into two dimensional matrix to increase the randomness of shared images. To further improve accuracy, some image scrambling techniques can be investigated. The other color spaces can also be explored to achieve better security level of the proposed MSS method. The entropy coding may be applied to the proposed method to further reduce the required bit and bandwith of the shared image before sending to the receiver.

REFERENCES

[1] R. M. May, "Simple mathematical models with very complicated dynamics," *Nature*, vol. 261, no. 5560, pp. 459–467, 1976. doi: 10.1038/261459a0.
[2] H. Zhu, C. Zhao, and X. Zhang, "A novel image encryption-compression scheme using hyper-chaos and Chinese remainder theorem," *Signal Process. Image Commun.*, vol. 28, no. 6, pp. 670–680, Jul. 2013.
[3] X. Wu, J. Weng, and W. Yan, "Adopting secret sharing for reversible data hiding in encrypted images," *Signal Process.*, vol. 143, pp. 269–281, Feb. 2018.
[4] Z. L. Liu and C. M. Pun, "Reversible data-hiding in encrypted images by redundant space transfer," *Inf. Sci.*, vols. 433–434, pp. 188–203, Apr. 2018.
[5] F. Khelifi, "On the security of a stream cipher in reversible data hiding schemes operating in the encrypted domain," *Signal Process.*, vol. 143, pp. 336–345, Feb. 2018.
[6] T. H. The, C. H. Hua, N. A. Tu, T. Hur, and S. Lee, "Selective bit embedding scheme for robust blind color image watermarking," *Inf. Sci.*, vol. 426, pp. 1–18, Feb. 2018.
[7] Y. Liu, S. Tang, R. Liu, L. Zhang, and Z. Ma, "Secure and robust digital image watermarking scheme using logistic and RSA encryption," *Expert Syst. Appl.*, vol. 97, pp. 95–105, May 2018.
[8] I. A. Ansari and M. Pant, "Multipurpose image watermarking in the domain of DWT based on SVD and ABC," *Pattern Recognit. Lett.*, vol. 94, pp. 228–236, Jul. 2017.
[9] J. M. Guo and H. Prasetyo, "False-positive-free SVD-based image watermarking," *J. Vis. Commun. Image Represent.*, vol. 25, pp. 1149–1163, Jul. 2014.
[10] B. Harjito and H. Prasetyo, "False-positive-free GSVD-based image watermarking for copyright protection," in *Proc. Int. Symp. Electron. Smart Devices*, Nov. 2016, pp. 143–147.
[11] H. Sajedi, "Steganalysis based on steganography pattern discovery," *J. Inf. Secur. Appl.*, vol. 30, pp. 3–14, Oct. 2016.
[12] S. Mahato, D. K. Yadav, and D. A. Khan, "A minesweeper game-based steganography scheme," *J. Inf. Secur. Appl.*, vol. 32, pp. 1–14, Feb. 2017.

[13] C. Wang, H. Wang, and Y. Ji, "Multi-bit wavelength coding phase-shift-keying optical steganography based on amplified spontaneous emission noise," *Opt. Commun.*, vol. 407, pp. 1–8, Jan. 2018.
[14] T. Bhattacharjee, S. P. Maity, and S. R. Islam, "Hierarchical secret image sharing scheme in compressed sensing," *Signal Process. Image Commun.*, vol. 61, pp. 21–32, Feb. 2018.
[15] T. H. Chen and C. S. Wu, "Efficient multi-secret image sharing based on Boolean operations," *Signal Process.*, vol. 91, no. 1, 90-97, Sep. 2011.
[16] C. C. Chen and W. J. Wu, "A secure Boolean-based multi-secret image sharing scheme," *J. Syst. Softw.*, vol. 92, pp. 107–114, Mar. 2014.
[17] C. N. Yang, C. H. Chen, and S. R. Cai, "Enhanced Boolean-based multi secret image sharing scheme," *J. Syst. Softw.*, vol. 116, pp. 22–34, Jun. 2016.
[18] J. B. Feng *et al.*, "A new multi-secret images sharing scheme using Largranges interpolation," *J. Syst. Softw.*, vol. 76, no. 3, pp. 327–339, 2005.
[19] C. Guo, C. C. Chang, and C. Qin, "A multi-threshold secret image sharing scheme based on MSP," *Pattern Recognit. Lett.*, vol. 33, no. 12, pp. 1594–1600, 2012.
[20] C. Guo *et al.*, "A multi-threshold secret image sharing scheme based on the generalized Chinese reminder theorem," *Multimedia Tools Appl.*, pp. 1–18, 2015.
[21] 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.
[22] X. Yan, Y. Lu, L. Liu, S. Wan, and W. Ding, "Security analysis of secret image sharing," in *Proc. 3rd Int. Conf. Pioneering Comput. Scientist, Eng., Educators*, vol. 727, Aug. 2017, pp. 305–316.

HERI PRASETYO received the bachelor's degree from the Department of Informatics Engineering, Institut Teknologi Sepuluh Nopember (ITS), Indonesia, in 2006, the master's degree from the Department of Computer Science and Information Engineering, National Taiwan University of Science and Technology (NTUST), Taiwan, in 2009, and the Doctoral degree from the Department of Electrical Engineering, NTUST, in 2015. He is currently with the Department of Informatics, Universitas Sebelas Maret (UNS), Indonesia. His research interests include multimedia signal processing, computational intelligence, pattern recognition, and machine learning. He received the Best Dissertation Award from the Taiwanese Association for Consumer Electronics (TACE), in 2015, and the best paper awards from the International Symposium on Electronics and Smart Devices 2017 (ISESD 2017). He has served as a General Vice-Chair for the Fifth International Conference on Internet Applications, Protocols, and Services 2017 (NETAPPS 2017) and the Publication Chair for the 2019 International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS 2019).

JING-MING GUO received the Ph.D. degree from the Institute of Communication Engineering, National Taiwan University, Taipei, Taiwan, in 2004.

He was the Director of the Innovative Business Incubation Center, Office of Research and Development. From 2002 to 2003 and in 2014, he was a Visiting Scholar with the Signal Processing Lab, Department of Electrical and Computer Engineering, University of California, Santa Barbara, CA, USA. In 2015, he joined the Digital Video and Multimedia Lab, Department of Electrical Engineering, Columbia University, USA, as a Visiting Scholar. He was the Vice Dean of the College of Electrical Engineering and Computer Science, National Taiwan University of Science and Technology, Taipei, where he is currently a Professor with the Department of Electrical Engineering. His research interests include multimedia signal processing, biometrics, computer vision, and digital halftoning.

Dr. Guo is a Fellow of the IET. He has served as a Best Paper Selection Committee Member for the IEEE TRANSACTIONS ON MULTIMEDIA. He has been promoted as a Distinguished Professor, in 2012, for his significant research contributions. He received the Outstanding Professor Award on Electrical Engineering from the Chinese Institute of Electrical Engineering, in 2016, the Best Paper Award from the International Computer Symposium, in 2014, the Outstanding Youth Electrical Engineer Award from the Chinese Institute of Electrical Engineering, in 2011, the Outstanding Young Investigator Award from the Institute of System Engineering, in 2011, the Best Paper Award from the IEEE International Conference on System Science and Engineering, in 2011, and the Outstanding Paper Award from IPPR, Computer Vision and Graphic Image Processing, in 2005 and 2006. He was a recipient of the Excellence Teaching Award, in 2009, the Research Excellence Award, in 2008, the Acer Dragon Thesis Award, in 2005, and the Outstanding Faculty Award, in 2002 and 2003. He is the Chapter Chair of the IEEE Signal Processing Society, Taipei Section. He was the General Chair of the IEEE International Conference on Consumer Electronics, Taiwan, in 2015 and 2016, and the Technical Program Chair of the IEEE International Symposium on Intelligent Signal Processing and Communication Systems, in 2012, the IEEE International Symposium on Consumer Electronics, in 2013, and the IEEE International Conference on Consumer Electronics, Taiwan, in 2014. He has been invited as a Lecturer for the IEEE Signal Processing Society Summer School on Signal and Information Processing, in 2012 and 2013. He has been elected as the Chair of the IEEE Taipei Section GOLD Group, in 2012. He has served as a Guest Co-Editor of two special issues for the *Journal of the Chinese Institute of Engineers* and the *Journal of Applied Science and Engineering*. He serves on the Editorial Board for the *Journal of Engineering*, *The Scientific World Journal*, the *International Journal of Advanced Engineering Applications*, *Detection*, and the *Open Journal of Information Security and Applications*. He is currently an Associate Editor of the IEEE TRANSACTIONS ON IMAGE PROCESSING, the IEEE TRANSACTIONS ON MULTIMEDIA, IEEE SIGNAL PROCESSING LETTERS, *Information Sciences*, *Signal Processing*, and the *Journal of Information Science and Engineering*.