Multiple Secret Sharing with Simple Image Encryption

Heri Prasetyo[1], Chih-Hsien Hsia[2], Jing-Yi Deng[2]

[1] Department of Informatics, Universitas Sebelas Maret (UNS), Indonesia
[2] Department of Computer Science and Information Engineering, National Ilan University, Taiwan
heri.prasetyo@staff.uns.ac.id, chhsia625@gmail.com, jinee5232@gmail.com

Abstract

Multiple Secret Sharing (MSS) aims to secure the image transmission by improving the ambiguity on image contents. The former (n, n)-MSS scheme generates n shared images from n secret images and reconstruct n recovered secret images from n shared images. This scheme hides the content of secret image by performing the eXclusive-OR (XOR) with specific masking coefficient. It exploits the Chinese Remainder Theorem (CRT) approach for generating the masking coefficient. However, the former scheme cannot work if n is odd. It overcomes the aforementioned problem by incorporating random image, transforming into nk encrypted secret images, and employing double masking coefficients. The presented MSS scheme utilizes an image encryption technique with simple chaotic maps for increasing the ambiguity of shared image content. The experimental results reveal that the proposed MSS method solves the problem on former MSS scheme and yields better performances.

Keywords: CRT, Image encryption, Secret sharing, Simple chaotic, XOR

1 Introduction

Nowadays, some confidential and secret information become handily to be distributed and transmitted over several parties via transmission channel. Some parties need to transfer some secret information using the transmission channel. Thus, image security technique becomes a very urgent to maintain the image integrity and information consistency. Many studies have been proposed to hide and render secret information into digital imaging media such as secret sharing [1-7], image watermarking [8], reversible data hiding [9-11], image encryption [12], etc. Among of them, the secret sharing transfers several secret images by firstly destroying the content of secret images. It has been proved effectively to transmit several secret images with the constraint of hiding the secret image content.

Several attempts have been devoted to propose a new technique for Multiple Secret Sharing (MSS) task such as [1-7]. Some of them have tried to improve the performance of MSS scheme. For example, the former schemes [1-2] extended the usability of MSS scheme for grayscale image. It broads the usability and performance of the other schemes [3-6] which are only limited for the grayscale secret images. Whereas, the former scheme [7] and proposed method develop the MSS system for color images. The former schemes [3-6] use (t, n)-threshold scenario, whereas the other methods are with (n, n+1) and (n, n)-threshold. The former method [7] employs the (n, n)-threshold scenario. This scheme offers a promising result if n is even. However, this scheme less resists from the incorrectness problem on facing n as odd number. The proposed method simply overcomes this problem by using three different approaches. In addition, it enjoys the advantage of simple image encryption [12] for improving security. The proposed method can be effectively implemented in the cloud computing environments under using the frameworks such as in [14-16]. The proposed method can also be deployed into another applications.

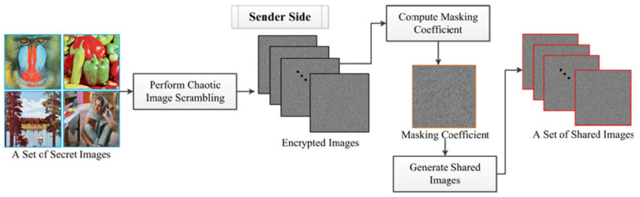
The rest of this paper is organized as follows. Related work on former MSS scheme with its problem on dealing odd number is provided in Section 2. Section 3 proposes some approaches for overcoming the problem of former scheme [7] by incorporating random image, transforming into nk encrypted secret images, and exploiting double masking coefficients. Extensive experimental results on the proposed image encryption and MSS system are detailed reported and discussed in Section 4. The conclusions and future works are finally delivered at the last part.

2 Related Work

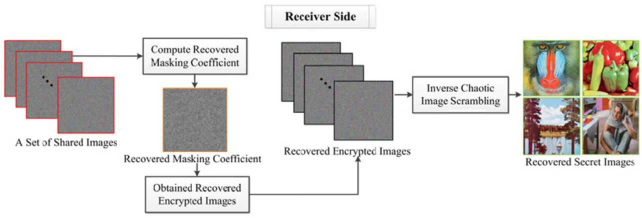
This section reviews the former existing scheme on MSS (n, n) and its slight limitation for color image. The MSS scheme aims to pull n shared images out from n secret images before sending it to the decoder via communication channel. Figure 1 illustrates the general framework of MSS (n, n) scheme. Herein, the sender side produces n shared images. Whereas, the receiver module performs reconstruction process to

*Corresponding Author: Chih-Hsien Hsia; E-mail: chhsia625@gmail.com
DOI: 10.3966/160792642020032102002

obtain n recovered secret images. The MSS scheme should maintain the reconstruction error as minimum as possible. It also needs to satisfy the strong threshold property in which the secret key in the reconstruction process is infeasible to be derived. In addition, an attacker cannot correctly obtain recovered secret images if only partial shared images are available. This section firstly discusses a slight limitation of former scheme [7].



(a) Sender



(b) Receiver sides

Figure 1. Illustration of MSS scheme while the secret images are in color space

The former scheme [7] requires n secret images, i.e. $\{I_1, I_2, \ldots, I_n\}$. The sender side firstly generates a set of shared images. The former scheme employs the CRT and XOR processes on shared images generation as well as in the reconstruction purpose. The former scheme firstly computes the masking coefficient M as follow:

$$M = \mathbb{C}\{I_1 \oplus I_2 \oplus \cdots \oplus I_n\}, \quad \textbf{(1)}$$

where $\mathbb{C}\{\cdot\}$ denotes the CRT operator with specific secret key. The symbol $\oplus$ represents XOR operator on bitwise level. Performing XOR between the i-th secret image, I_i, and M yields the shared image S_i for $i = 1, 2, \ldots, n$ as defined bellow:

$$S_i = I_i \oplus M. \quad \textbf{(2)}$$

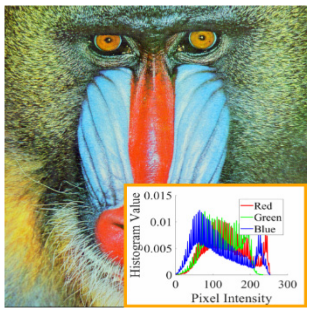
It produces n shared images $\{S_1, S_2, \ldots, S_n\}$ which are ready to be sent to the decoder side. On the other hand, the receiver collects these shared images from transmission channel. To reconstruct the secret image, the receiver needs to perform the reverse process of sender module. The receiver firstly computes the recovered masking coefficient $\tilde{M}$. This computation is formally defined as follow:

$$\tilde{M} = \mathbb{C}\{S_1 \oplus S_2 \oplus \cdots \oplus S_n\}. \quad \textbf{(3)}$$

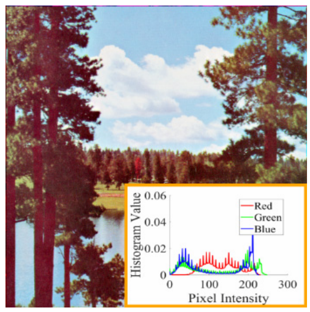
The CRT secret key for computing $\tilde{M}$ should be identically maintained as used in M for satisfying the reversible process in both shared image generation and secret image reconstruction. The i-th recovered secret image, $\tilde{I}_i$, is reconstructed by XOR-ing S_i with recovered masking coefficient $\tilde{M}$ as:

$$\tilde{I}_i = S_i \oplus \tilde{M}, \quad \textbf{(4)}$$

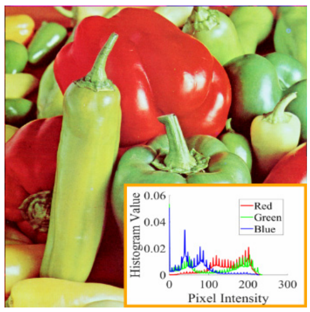
for $i = 1, 2, \ldots, n$. In [7], the former MSS scheme yields correct result for $n = 4$. The former scheme works well on the MSS task if n is even. However, it has problem on dealing with odd number. This paper uses four secret images [13] to experimentally validate the performance in Figure 2. Figure 3 shows the result of former scheme while the number of secret image is odd number, i.e. $n = 3$. A set of shared images are shown in Figures 3(a) to Figures 3(c) with a set of secret images from Figures 2(a) Figures 2(c). As it can be seen from this figure, the former scheme produces a good shared image as indicated with uniformly image histogram depicted in the bottom-right side of each image. While Figures 3(d) to Figures 3(f) shows the recovered and original secret images which are totally different. This experiment tells that the former scheme cannot suffer from n odd number problem. The following gives analysis of the former scheme performance.



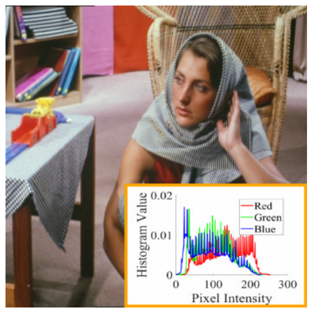
(a) Baboon I_1



(b) Lake I_2

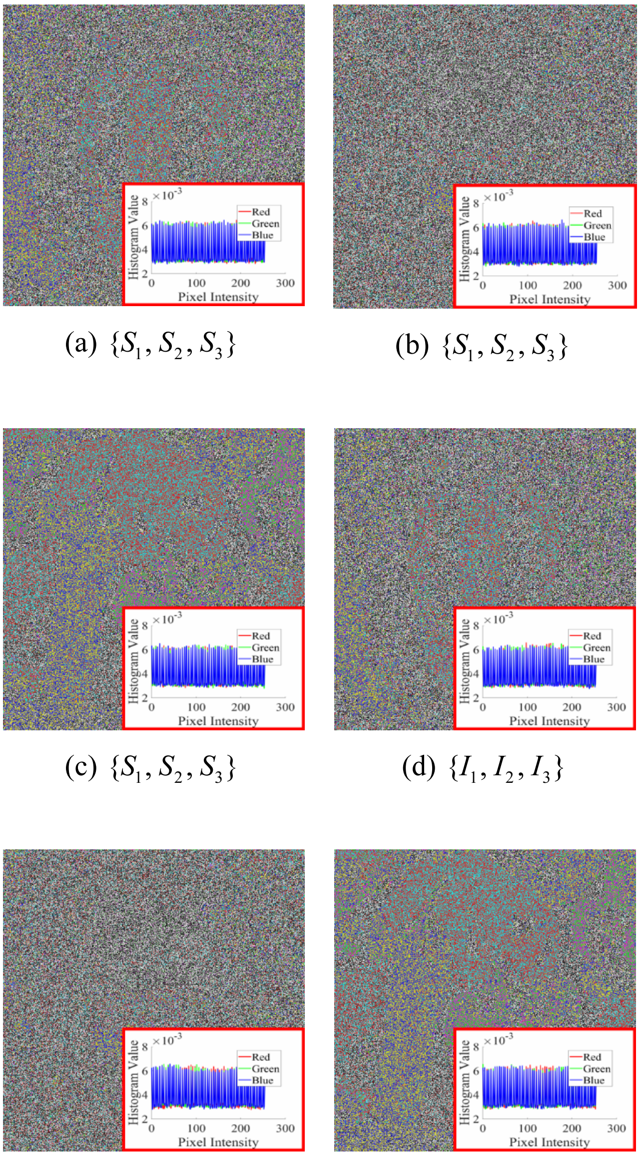


(c) Peppers I_3



(d) Barbara I_4

Figure 2. Secret images used for experiment



(a) $\{S_1, S_2, S_3\}$ (b) $\{S_1, S_2, S_3\}$

(c) $\{S_1, S_2, S_3\}$ (d) $\{I_1, I_2, I_3\}$

(e) $\{I_1, I_2, I_3\}$ (f) $\{I_1, I_2, I_3\}$

Figure 3. Results of [7] for $n = 3$

Theorem 2.1: *The former scheme satisfies the symmetric property if n is even.*

Proof: The value of $\tilde{M}$ (if n is even) is defined as $\tilde{M} = \mathbb{C}\{S_1 \oplus S_2 \oplus \cdots \oplus S_n\}$. From the fact that $S_i = I_i \oplus M$ and $\underbrace{M \oplus M \oplus \cdots \oplus M}_{n \text{ is even number}} = M \oplus M = 0$, the value of $\tilde{M}$ is simply recomputed as:

$$\begin{aligned}
&\tilde{M} = \mathbb{C}\{I_1 \oplus M \oplus I_2 \oplus M \oplus \cdots \oplus I_n \oplus M\} \\
&\mathbb{C} = \{I_1 \oplus I_2 \oplus \cdots \oplus I_n \oplus \underbrace{M \oplus M \oplus \cdots \oplus M}_{n \text{ is even number}}\}, \\
&\tilde{M} = \mathbb{C}\{I_1 \oplus I_2 \oplus \cdots \oplus I_n \oplus 0\} = \\
&\mathbb{C} = \{I_1 \oplus I_2 \oplus \cdots \oplus I_n\}.
\end{aligned} \tag{5}$$

In this case, the value $\tilde{M}$ in (5) is the same to that of the value of M in (1). If n is even number, the former scheme satisfies the symmetric property on masking coefficient, i.e. $\tilde{M} = M$.

If n is odd, the value of $\tilde{M}$ is defined as $\tilde{M} = \mathbb{C}\{S_1 \oplus S_2 \oplus \cdots \oplus S_n\}$. . Since $S_i = I_i \oplus M$ and $\underbrace{M \oplus M \oplus \cdots \oplus M}_{n \text{ is even number}} = M \oplus M \oplus M = 0 \oplus M = M$, the value $\tilde{M}$ is then given as:

$$\begin{aligned}
&\tilde{M} = \mathbb{C}\{I_1 \oplus M \oplus I_2 \oplus M \oplus \cdots \oplus I_n \oplus M\} = \\
&\mathbb{C} = \{I_1 \oplus I_2 \oplus \cdots \oplus I_n \oplus \underbrace{M \oplus M \oplus \cdots \oplus M}_{n \text{ is odd number}}\}, \\
&\tilde{M} = \mathbb{C}\{I_1 \oplus I_2 \oplus \cdots \oplus I_n \oplus M\}.
\end{aligned} \tag{6}$$

In this case, the values of $\tilde{M}$ in (6) and M in (1) are not identical, i.e. $\tilde{M} \neq M$. Thus, the former scheme cannot satisfy the symmetric property on masking coefficient in case the number of n is odd. It completes the proof.

3 Proposed Method on Multiple Secret Sharing

This section presents the proposed method on (n, n)-MSS. It employs the CRT and XOR process to generate shared images and to recover secret images. Herein, three different techniques are proposed in this paper. It solves the problem on [7] if n is odd. The first approach utilizes random image to remove this problem. The second method solves the former scheme problem by transforming each secret image into even number. The third technique employs double masking coefficients to avoid the ambiguity if n is odd. The image encryption with simple chaotic maps [12] is injected into three methods to further improve the security level.

3.1 Incorporating Random Image

This scheme solves the problem in [7] by incorporating random image. This scenario is to maintain symmetric property of masking coefficient in the sender/encoder side and receiver/decoder side. Let $\{I_1, I_2, \ldots, I_n\}$ be a set of secret image. The value of n denotes the number of secret images which can be odd or even. This proposed scheme firstly performs image encryption [12] for each secret image using secret key x for $i = 1, 2, \ldots, n$ as:

$$I_{i,k} = \mathbb{E}\{I_i; k\} \tag{7}$$

where $\mathbb{E}\{*;*\}$ denotes the encryption operator. This process produces a set of encrypted secret images $\{I_{1,k}, I_{2,k}, \ldots, I_{n,k}\}$. The proposed MSS method adds random image before computing M. Suppose that $\{I_{1,k}, I_{2,k}, \ldots, I_{n,k}, I_{n+1}\}$ be secret images after adding the random image. The value of M can be computed as:

$$M = \mathbb{C}\{I_{1,k} \oplus I_{2,k} \oplus \cdots \oplus I_{n,k} \oplus I_{n+1}\}, \tag{8}$$

where I_{n+1} is an additional random image. However, the strict restriction should be taken into account for n is odd/even. This restriction is to satisfy the symmetric property of masking coefficient for good reversible MSS scheme. For n is even, the additional random image can be set as $I_{n+1} = 0$. If n is odd, the additional random image can be selected as:

$$I_{n+1} = A = \text{ROUND}\{255 * C_k\}, \tag{9}$$

where A and C_k denote the additional random image and chaotic number generated using secret key k , respectively. Then, the value of M in (13) can be simplified as follow:

$$M = \begin{cases} \mathbb{C}\{I_{1,k} \oplus I_{2,k} \oplus \cdots \oplus I_{n,k} \oplus A\}, \text{if } n \text{ is odd} \\ \mathbb{C}\{I_{1,k} \oplus I_{2,k} \oplus \cdots \oplus I_{n,k} \oplus A\}, \text{if } n \text{ is even} \end{cases}. \tag{10}$$

Several shared images can be trivially produced after obtaining the masking coefficient M. This process is defined as:

$$S_{1,k} = I_{1,k} \oplus M, \tag{11}$$

for $i = 1, 2, \ldots, n+1$. The symbol $S_{i,k}$ represents an encrypted shared image with encryption secret key k. This process produces encrypted shared images $\{S_{1,k}, S_{2,k}, \ldots, S_{n+1,k}\}$. To reconstruct the secret image, a recovered masking coefficient should be firstly computed by XOR-ed all shared image. This process is simply defined as:

$$\tilde{M} = \mathbb{C}\{S_{1,k} \oplus S_{2,k} \oplus \cdots \oplus S_{n+1,k}\}, \tag{12}$$

where $\tilde{M}$ denotes the recovered version of masking coefficient. A recovered secret image is subsequently obtained by XOR-ing $S_{i,k}$ with $\tilde{M}$ as follow:

$$\tilde{I}_{i,k} = S_{i,k} \oplus \tilde{M}, \tag{13}$$

for $i = 1, 2, \ldots, n$. In this process, we simply consider the recovery process for n shared images. The computation for $n+1$ -th shared image is neglegted since I_{n+1} contains meaningless information, i.e. $I_{n+1} = A$ or $I_{n+1} = 0$ if n is odd/even number, respectively. An additional step should be taken for $\tilde{I}_{1,k}$ since it is still in encrypted version as:

$$\tilde{I}_i = \mathbb{D}\{\tilde{I}_{1,k}; k\}, \tag{14}$$

where $\mathbb{D}\{*;*\}$ denotes decrypted operator. To yield correct result, the secret key for performing encryption should be identical as used for decryption process. Images $\{I_1, I_2, \ldots, I_n\}$ are subsequently produced at the receiver side. Thus, the proposed MSS scheme overcomes the problem in [7] if n is odd. A new approach with random image also increases the MSS security level by incorporating the image encryption.

Theorem 3.1: *The first method satisfies symmetric property of masking coefficient.*

Proof: Let $\{S_{1,k} \oplus S_{2,k} \oplus \cdots \oplus S_{n+1,k}\}$ be shared images after adding a random image. The value of $\tilde{M}$ can be simply computed as $\tilde{M} = \mathbb{C}\{S_{1,k} \oplus S_{2,k} \oplus \cdots \oplus S_{n+1,k}\}$. Since of $S_{i,k} = I_{i,k} \oplus M$, it simplifies computation as $\tilde{M} = \mathbb{C}\{I_{1,k} \oplus M \oplus I_{2,k} \oplus M \oplus \cdots \oplus I_{n+1,k} \oplus M\}$.

For n is odd, the computation of $\tilde{R}$ can be rearranged as $\tilde{M} = \mathbb{C}\{I_{1,k} \oplus I_{2,k} \oplus \cdots \oplus I_{n+1,k} \oplus \underbrace{M \oplus M \oplus \cdots M}_{n \text{ is odd number}}\}$. As we know that $I_{n+1,k} = A$ and $\underbrace{M \oplus M \oplus \cdots \oplus M}_{n \text{ is odd number}} = M \oplus M \oplus M = M$, the value of $\tilde{M}$ can be further obtained as:

$$\begin{aligned} \tilde{M} &= \mathbb{C}\{I_{1,k} \oplus I_{2,k} \oplus \cdots \oplus I_{n,k} \oplus (A \oplus M) \oplus M\}, \\ \tilde{M} &= \mathbb{C}\{I_{1,k} \oplus I_{2,k} \oplus \cdots \oplus I_{n,k} \oplus A\}. \end{aligned} \tag{15}$$

The values of $\tilde{M}$ in (15) and M used in (10) are now identical. Thus, this scheme satisfies the symmetric property, i.e. $M = \tilde{M}$, for n is odd.

The value of $\tilde{M}$ (for n is even) is simply calculated as $\tilde{M} = \mathbb{C}\{I_{1,k} \oplus I_{2,k} \oplus \cdots \oplus I_{n+1,k} \oplus \underbrace{M \oplus M \oplus \cdots \oplus M}_{n \text{ is even number}}\}$. Since $I_{n+1,k} = A = 0$ and $\underbrace{M \oplus M \oplus \cdots \oplus M}_{n \text{ is even number}} = M \oplus M = 0$, the coefficient $\tilde{M}$ is then given as follow:

$$\begin{aligned} \tilde{M} &= \mathbb{C}\{I_{1,k} \oplus I_{2,k} \oplus \cdots \oplus I_{n,k} \oplus A \oplus 0\}, \\ \tilde{M} &= \mathbb{C}\{I_{1,k} \oplus I_{2,k} \oplus \cdots \oplus I_{n,k}\}. \end{aligned} \tag{16}$$

It can be concluded that the values of $\tilde{M}$ in (16) and M in (10) are now identical. It indicates that this scheme satisfies symmetric property, i.e. $M = \tilde{M}$, for n is even. Yet, the first method is correct for n is odd/even.

3.2 Converting into *nk* Secret Images

To yield correct MSS result, the masking coefficient in encoder/sender side is maintained as identical to that of used in decoder/receiver side. This scheme avoids the former scheme problem by converting each secret image into several encrypted images. By choosing k as arbitrary even number, the proposed method transforms n secret images into nk encrypted secret images. The multiplication between n and k yields nk as even number, since k and n are even and arbitrary number, respectively. This conversion can be simply performed by using the proposed image encryption over several different chaotic keys.

Let $\{I_1, I_2, \ldots, I_n\}$ be secret images. The proposed method encrypts each secret image for $i = 1, 2, \ldots, n$ and $j = 1, 2, \ldots, k$ using:

$$I_{i,j} = \mathbb{E}\{I_i; k_1, k_2, ..., k_k\} \quad \textbf{(17)}$$

where k denotes the arbitrary even number. The symbol $\mathbb{E}\{*;*\}$ denotes the encryption operator. The value of M is computed as:

$$\tilde{M} = \mathbb{C}\{I_{1,1} \oplus \cdots \oplus I_{1,k} \oplus I_{2,1} \oplus \cdots \oplus I_{2,k} \oplus \cdots \oplus I_{n,1} \oplus \cdots \oplus I_{n,k}\}. \quad \textbf{(18)}$$

The next step generates encrypted shared image $S_{i,j}$ for $i = 1, 2, \ldots, n$ and $j = 1, 2, \ldots, k$ denoted as:

$$S_{i,j} = I_{i,j} \oplus M. \quad \textbf{(19)}$$

It yields nk shared images.

At the receiver side, some shared images are accumulated and utilized to obtain some recovered secret images. The recovered masking coefficient $\tilde{M}$ needs to be calculated. This computation is formally defined as:

$$\tilde{M} = \mathbb{C}\{S_{1,1} \oplus \cdots \oplus S_{1,k} \oplus S_{2,1} \oplus \cdots \oplus S_{2,k} \oplus \cdots \oplus S_{n,1} \oplus \cdots \oplus S_{n,k}\}. \quad \textbf{(20)}$$

A recovered secret image $\tilde{I}_{1,j}$ for $i = 1, 2, \ldots, n$ and $j = 1, 2, \ldots, k$ is subsequently reconstructed as:

$$\tilde{I}_{i,j} = S_{i,j} \oplus \tilde{M}. \quad \textbf{(21)}$$

The image $\tilde{I}_{1,j}$ is still in encryption version. Thus, the decryption procedure should be performed on each $\tilde{I}_{1,j}$. This process is given as follow:

$$I_i = \mathbb{D}\{\tilde{I}_{i,j}; k_1, k_2, ..., k_k\} \quad \textbf{(22)}$$

where $\mathbb{D}\{*;*\}$ denotes the decryption operator. Transforming k secret images into nk encrypted secret images solves the problem in [7]. In addition, it avoids the ambiguity while n is even/odd number.

Theorem 3.2: *The second method satisfies symmetric property of masking coefficient.*

Proof: Let $\{S_{1,1}, \ldots, S_{1,k}, S_{2,1}, \ldots, S_{2,k}, \ldots, S_{n,1}, \ldots, S_{n,k}\}$ be shared images after converting n secret images into nk encrypted images. The value of $\tilde{M}$ can be computed as $\tilde{M} = \mathbb{C}\{S_{1,1} \oplus \cdots \oplus S_{1,k} \oplus S_{2,1} \oplus \cdots \oplus S_{2,k} \oplus \cdots \oplus S_{n,1} \oplus \cdots \oplus S_{n,k}\}$. The value of $\tilde{M}$ can be recomputed by knowing the fact that $S_{i,j} = I_{i,j} \oplus M$ as $\tilde{M} = \mathbb{C}\{I_{1,1} \oplus M \oplus \cdots \oplus I_{1,k} \oplus M \oplus I_{2,1} \oplus M \oplus \cdots \oplus I_{2,k} \oplus M \oplus \cdots \oplus I_{n,1} \oplus M \oplus \cdots \oplus I_{n,k} \oplus M\} = \mathbb{C}\{I_{1,1} \oplus \cdots \oplus I_{1,k} \oplus I_{2,1} \oplus \cdots \oplus I_{2,k} \oplus \cdots \oplus I_{n,1} \oplus \cdots \oplus I_{n,k} \oplus \underbrace{M \oplus M \oplus \cdots \oplus M}_{n \text{ is even number}}\}$. The multiplication result of nk is always even, if k is an arbitrary even number, regardless the value of n. Yet, $\underbrace{M \oplus M \oplus \cdots \oplus M}_{n \text{ is even number}} = M \oplus M = 0$. The coefficient $\tilde{M}$ is then simplified as follow:

$$\tilde{M} = \mathbb{C}\{I_{1,1} \oplus \cdots \oplus I_{1,k} \oplus I_{2,1} \oplus \cdots \oplus I_{2,k} \oplus \cdots \oplus I_{n,1} \oplus \cdots \oplus I_{n,k}\}. \quad \textbf{(23)}$$

It clearly reveals that the values of $\tilde{M}$ in (23) and M used in (18) are identical. Thus, the proposed method satisfies the symmetric property, i.e. $\tilde{M} = M$. This finding proves the correctness for this proposed method.

3.3 Utilizing Double Masking Coefficients

This subsection presents the proposed MSS method using double masking coefficients. These two masking coefficients are to solve problem in [7]. Let $\{I_1, I_2, \ldots, I_n\}$ be secret images. Inverse encryption with specific key k is applied for each secret image while $i = 1, 2, \ldots, n$ as:

$$I_{i,k} = \mathbb{E}\{I_i; k\}. \quad \textbf{(24)}$$

Then, we obtain encrypted secret images $\{I_{1,k}, I_{2,k}, \ldots, I_{n,k}\}$. Two different approaches are employed to generate shared images by considering the value of n. The proposed method generates shared image $S_{i,k}$ for $i = 1, 2, \ldots, n$ and n is even as follow:

$$S_{i,k} = I_{i,k} \oplus M. \quad \textbf{(25)}$$

Then, one obtains encrypted shared image $\{S_{1,k}, S_{2,k}, \ldots, S_{n,k}\}$. In this work, the masking coefficient M is derived from:

$$M = \mathbb{C}\{I_{1,k} \oplus I_{2,k} \oplus \cdots \oplus I_{n,k}\}. \quad \textbf{(26)}$$

On opposite side, the reconstruction process of secret images $\tilde{I}_{1,k}$ for $i = 1, 2, \ldots, n$ is formulated by:

$$\tilde{I}_{i,k} = S_{i,k} \oplus \tilde{M}. \quad \textbf{(27)}$$

The value of $\tilde{M}$ is then calculated as:

$$\tilde{M} = \mathbb{C}\{S_{1,k} \oplus S_{2,k} \oplus \cdots \oplus S_{n,k}\}. \quad \textbf{(28)}$$

The proposed method generates shared images in different way if n is odd. This scheme employs double or two masking coefficients to avoid the problem in [7]. A shared image $S_{i,k}$ can be obtained by performing XOR operation using two masking coefficient as follow:

$$S_{1,k} = \begin{cases} I_{1,k} \oplus M_1, & \text{for } i = 1, 2, \ldots n-1 \\ I_{1,k} \oplus M_2, & \text{for } i = n \end{cases}, \tag{29}$$

where M_1 and M_2 are two different masking coefficients which can be simply computed as:

$$M_1 = \mathbb{C}\{I_{1,k} \oplus I_{2,k} \oplus \cdots \oplus I_{n,k}\}, \tag{30}$$

$$M_2 = \mathbb{C}\{I_{1,k} \oplus I_{2,k} \oplus \cdots \oplus I_{n-1,k}\}. \tag{31}$$

We further obtain shared image $\{S_{1,k}, S_{2,k}, \ldots, S_{n,k}\}$. To recover back the secret images, the proposed method performs XOR between each shared image $S_{i,k}$ with two different masking coefficients. Firstly, we compute the n-th recovered secret image, i.e. $\tilde{I}_{1,k}$, using the following formula:

$$\tilde{I}_{n,k} = S_{n,k} \oplus \tilde{M}_2, \tag{32}$$

where $\tilde{M}_2$ denotes the second recovered masking coefficient which can be obtained as:

$$M_2 = \mathbb{C}\{S_{1,k} \oplus S_{2,k} \oplus \cdots \oplus S_{n-1,k}\}. \tag{33}$$

The other recovered secret images are trivially obtained by XOR-ing $S_{i,k}$ with $\tilde{M}_1$ for $i = 1, 2, \ldots, n-1$ as:

$$\tilde{I}_{i,k} = S_{i,k} \oplus \tilde{M}_1, \tag{34}$$

Herein, the value of $\tilde{M}_1$ is:

$$\tilde{M}_1 = \mathbb{C}\{S_{1,k} \oplus S_{2,k} \oplus \cdots \oplus S_{n-1,k} \oplus \tilde{I}_{n,k}\}. \tag{35}$$

This step yields recovered images $\{\tilde{I}_{1,k}, \tilde{I}_{2,k}, \ldots, \tilde{I}_{n,k}\}$. All recovered secret images need to be decrypted since they are still in encrypted version. It is formally defined for $i = 1, 2, \ldots, n$ as:

$$I_i = \mathbb{D}\{I_{i,k}; k\}, \tag{36}$$

where $\mathbb{D}\{*;*\}$ denotes the decryption operator. This scheme offers a simple approach to remove the problem in [7].

Theorem 3.3: *The third method satisfies symmetric property of masking coefficient.*

Proof: Suppose $\{S_{1,k}, S_{2,k}, \ldots, S_{n,k}\}$ be generated shared images. The coefficient $\tilde{M}$ (for n is even) can be obtained as $\tilde{M} = \mathbb{C}\{S_{1,k} \oplus S_{2,k} \oplus \cdots \oplus S_{n,k}\}$. Since $S_{i,k} = I_{i,k} \oplus M$ and $\underbrace{M \oplus M \oplus \cdots M}_{n \text{ is even number}} = 0$, the $\tilde{M}$ can be subsequently rewritten as:

$$\begin{aligned} \tilde{M} &= \mathbb{C}\{I_{1,k} \oplus M \oplus I_{2,k} \oplus M \oplus \cdots \oplus I_{n,k} \oplus M\}, \\ &= \mathbb{C}\{I_{1,k} \oplus I_{2,k} \oplus \cdots \oplus I_{n,k} \oplus \underbrace{M \oplus M \oplus \cdots \oplus M}_{n \text{ is even number}}\} \\ &= \mathbb{C}\{I_{1,k} \oplus I_{2,k} \oplus \cdots \oplus I_{n,k}\}. \end{aligned} \tag{37}$$

From this result, the coefficient $\tilde{M}$ in (37) is the same as M in (26). It tells that the proposed method satisfies the symmetric property, i.e. $\tilde{M} = M$.

For n is odd, the coefficient $\tilde{M}_2$ is given as $\tilde{M}_2 = \mathbb{C}\{S_{1,k} \oplus S_{2,k} \oplus \cdots \oplus S_{n-1,k}\}$. The value of $n-1$ is even number if and only if n is odd. Since $S_{i,k} = I_{i,k} \oplus M_1$ and $\underbrace{M_1 \oplus M_1 \oplus \cdots M_1}_{n \text{ is even number}} = 0$, the $\tilde{M}_2$ is then given as

$$\begin{aligned} \tilde{M}_2 &= \mathbb{C}\{I_{1,k} \oplus M_1 \oplus I_{2,k} \oplus M_1 \oplus \cdots \oplus I_{n-1,k} \oplus M_1\}, \\ &= \mathbb{C}\{I_{1,k} \oplus I_{2,k} \oplus \cdots \oplus I_{n-1,k} \oplus \underbrace{M_1 \oplus M_1 \oplus \cdots \oplus M_1}_{n \text{ is even number}}\} \\ &= \mathbb{C}\{I_{1,k} \oplus I_{2,k} \oplus \cdots \oplus I_{n-1,k}\}. \end{aligned} \tag{38}$$

As it can be seen, the values of $\tilde{M}_2$ in (38) and M_2 in (31) are identical. Thus, the proposed method satisfies the symmetric property, i.e. $\tilde{M}_2 = M_2$.

The value $\tilde{M}_1$ (for n is odd) is given as:

$$\begin{aligned} \tilde{M}_1 &= \mathbb{C}\{S_{1,k} \oplus S_{2,k} \oplus \cdots \oplus S_{n-1,k} \oplus \tilde{I}_{n,k}\} \\ &= \mathbb{C}\{I_{1,k} \oplus M_1 \oplus I_{2,k} \oplus M_1 \oplus \cdots \oplus I_{n-1,k} \oplus M_1 \oplus \tilde{I}_{n,k}\} \\ &= \mathbb{C}\{I_{1,k} \oplus I_{2,k} \oplus \cdots \oplus I_{n-1,k} \oplus \tilde{I}_{n,k} \oplus \underbrace{M_1 \oplus M_1 \oplus \cdots \oplus M_1}_{n \text{ is even number}}\} \\ &= \mathbb{C}\{I_{1,k} \oplus I_{2,k} \oplus \cdots \oplus I_{n-1,k} \oplus \tilde{I}_{n,k}\}. \end{aligned}$$

In a good MSS scheme, the recovered secret image should be without distortion, i.e. $\tilde{I}_{n,k} = I_{n,k}$. Then, the $\tilde{M}_1$ can be further obtained as:

$$\tilde{M}_1 = \mathbb{C}\{I_{1,k} \oplus I_{2,k} \oplus \cdots \oplus I_{n-1,k} \oplus M_1\}. \tag{39}$$

The value of $\tilde{M}_1$ in (39) is the same as the original M_1 used in (30), i.e. $\tilde{M}_1 = M_1$. A new approach with double masking coefficients satisfies the symmetric property. It indicates that the proposed MSS scheme is reversible. This gives complete proof.

4 Experimental Results

Three approaches for the proposed MSS scheme include utilizing random image, converting n secret images into nk encrypted secret images, and exploiting double masking coefficients. The comparison is measured under four different test images as shown in Figure 2. Several measurement metrics [1-7] are used to objectively evaluate performances such as Unified Averaged Changed Intensity (UACI), Number of Pixel Changing Rate (NPCR), Mean Absolute Error (MAE), Peak-Signal-to-Noise-Ratio (PSNR), Root Mean Squared Error (RMSE), and correlation coefficient. The value of correlation coefficient lies on range [-1,1] indicating the similarity degree between two images. The MSS is said to be successful when it produces the correlation coefficient around 0 indicating that the shared image is independent (or not similar) compared to the original image. It delivers a good result while RMSE, MAE, NPCR, and UACI are in high value since the shared image and original image are different. In contrast, the PSNR should be as lower as possible for good MSS method.

4.1 Performance of Proposed MSS with Random Image

The performance of a new approach with random image is delivered in this subsection. It incorporates random image A if n is odd. The chaotic secret keys for generating this random image is $x = \{x_0 = 0.1236, a = 3.95, b = 4, m = 1000\}$. A set {3, 5, 17} are selected as CRT secret keys. All secret images are firstly encrypted with [12]. Presented idea with random image produces shared images as shown in Figure 4(a) to Figure 4(d) for $n = 4$. The histogram of each shared image cannot be easily distinguished to the other since of its uniformity. It indicates the robustness of proposed method against histogram attacks. Figures 4(e) to Figure 4(h) and Figure 4(i) to Figure 4(l) are recovered images constructed with correct and incorrect encryption keys, respectively. The proposed method only produces correct recovered secret image while correct secret key is utilized to perform the image decryption. It also cannot yield correct recovered images if all shared images are not available in recovery process. Figure 5 depicts the results of new approach with random image for $n = 3$. It offers a promising result for n is odd/even. In addition, the presented approach with random image solves the problem in [7] for n is odd.

4.2 Performance of Proposed MSS with *nk* Encrypted Images

The performances of proposed method by converting n secret images into nk encrypted images are discussed in this subsection. The method in [12] encrypts all shared images. Herein, the CRT secret keys are chosen as {3, 5, 17} yielding M and $\tilde{M}$ lie on [0, 255]. We set the number of image encryption k as 2. Herein, $k = 1$ and $k = 2$ denote the diffusion process with arithmetic addition and substraction operator, respectively, on image encryption [12]. Figure 6 shows the results obtained from the proposed method for $n = 4$, while (a)-(d) are several generated shared images. The proposed yields correct results as shown in Figure 6(e) to Figure 6(h) while it utilizes correct encrypted keys. Figure 6(i) to Figure 6(l) are meaningless recovered secret images if we use incorrect chaotic keys. Figure 6(m) to Figure 6(p) are incorrect recovered secret images obtained if not all shared images are available. It also produces similar results for n is odd number. Figure 7 supports the similar finding for $n = 3$. From these experiments, the presented new approach is workable for n is even/odd. An attacker obtains nothing if all shared images are not fully collected for the secret image recovery.

4.3 Performance of Proposed MSS with Double Masking Coefficients

A new approach with double masking coefficients is reported in this subsection. Firstly, all secret images are processed with image encryption technique [12]. The CRT secret keys are set as {3, 5, 17} for computing M and $\tilde{M}$. Thus, the values of M_1, M_2, $\tilde{M}_1$, and $\tilde{M}_2$ lies on interval [0, 255]. Some experimental results of new approach with double masking coefficients for $n = 4$ are shown in Figure 8, while Figure 8(a) to Figure 8(d) are shared images. The proposed method produces randomize shared images with uniformly histogram making it very hard to be distinguished with the others. Figure 8(e) to Figure 8(h) and Figure 8(i) to Figure 8(l) are the recovered images obtained using correct and incorrect secret keys, respectively. The proposed method correctly produces the recovered secret images while it employs the correct secret key. If only partial or several shared image are available in the receiver side, the proposed method produces recovered secret images as Figure 8(m) to Figure 8(p). It can be seen that the recovered secret images cannot be correctly obtained using partial shared images. Proposed method also yields similar results while $n = 3$. Figure 9 gives the proposed method results for $n = 3$. It concludes that the new approach with double masking coefficients performs well for n is even or odd number.

4.4 Performance Comparisons Against Former Existing Schemes

Some comparisons between the proposed method and others [1-7] are reported in this subsection. The comparison is examined in terms of objective measurements. Herein, two criterions are investigated, i.e. the differential attacks and image similarity degree. For fair comparison, the experiments were conducted and examined under four secret images in Figure 2 as formerly used in [1-7] under an identical experimental setting. The performances are compared under the correlation coefficient, RMSE, PSNR, MAE, NPCR, and UACI, for all aforementioned methods. Firstly, the similarity between the secret images and recovered versions are compared in Table 1. From this table, the quality of secret images and its recovered version is totally identical indicated with high correlation (i.e. 1), low RMSE, MAE, NPCR, UACI (i.e. 1), and very high PSNR values. The proposed method produces the recovered secret images perfectly.

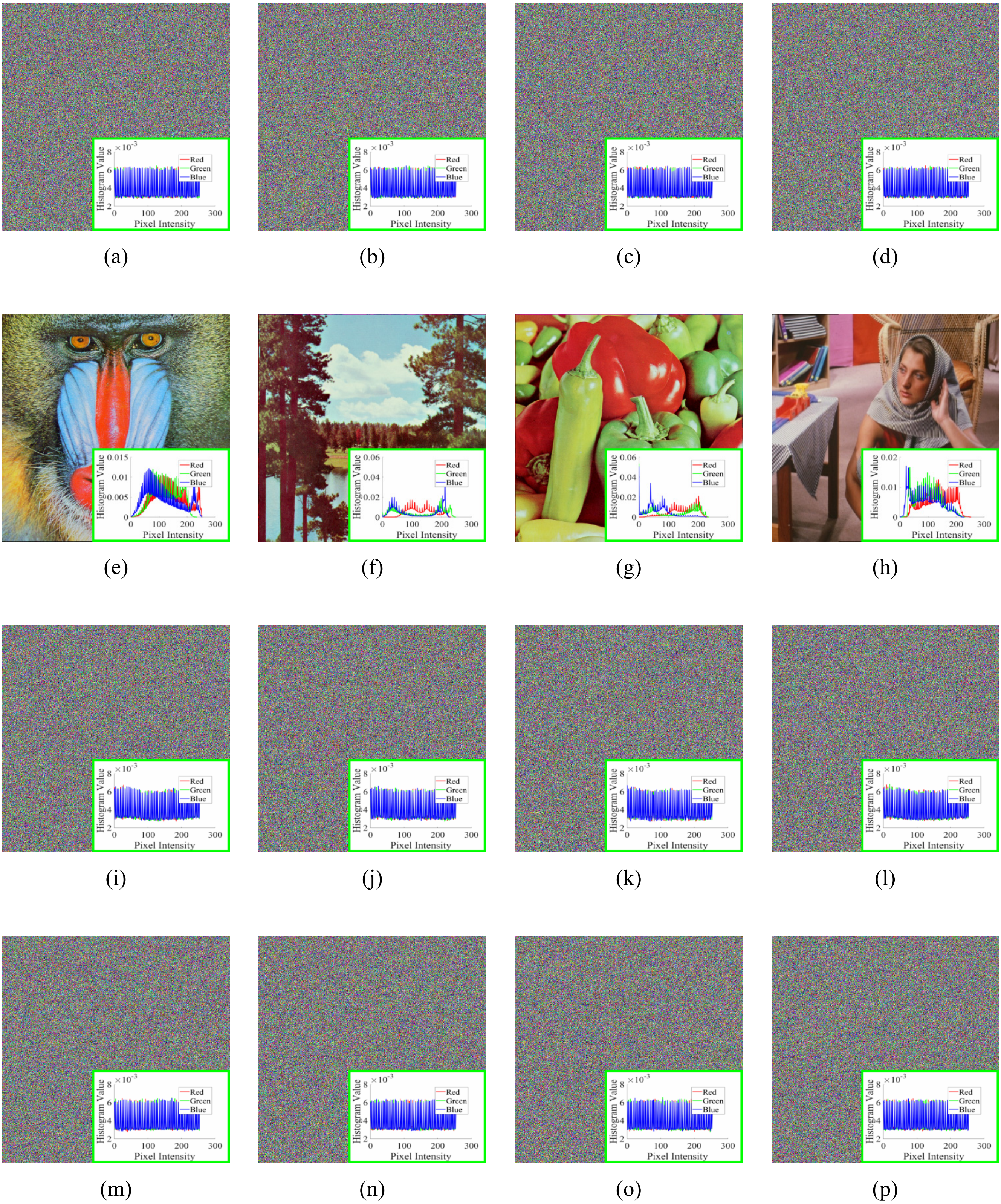


Figure 4. Proposed method with random image, for $n = 4$: (a)-(d) $\{S_1, S_2, S_3, S_4\}$. (e)-(h) $\{I_1, I_2, I_3, I_4\}$ recovered with correct chaotic keys. (i)-(l) $\{I_1, I_2, I_3, I_4\}$ recovered with incorrect chaotic keys. (m)-(n) $\{I_1, I_2\}$ recovered from $n-1$ shared images. (o)-(p) $\{I_1, I_2\}$ recovered from n-2 shared images.

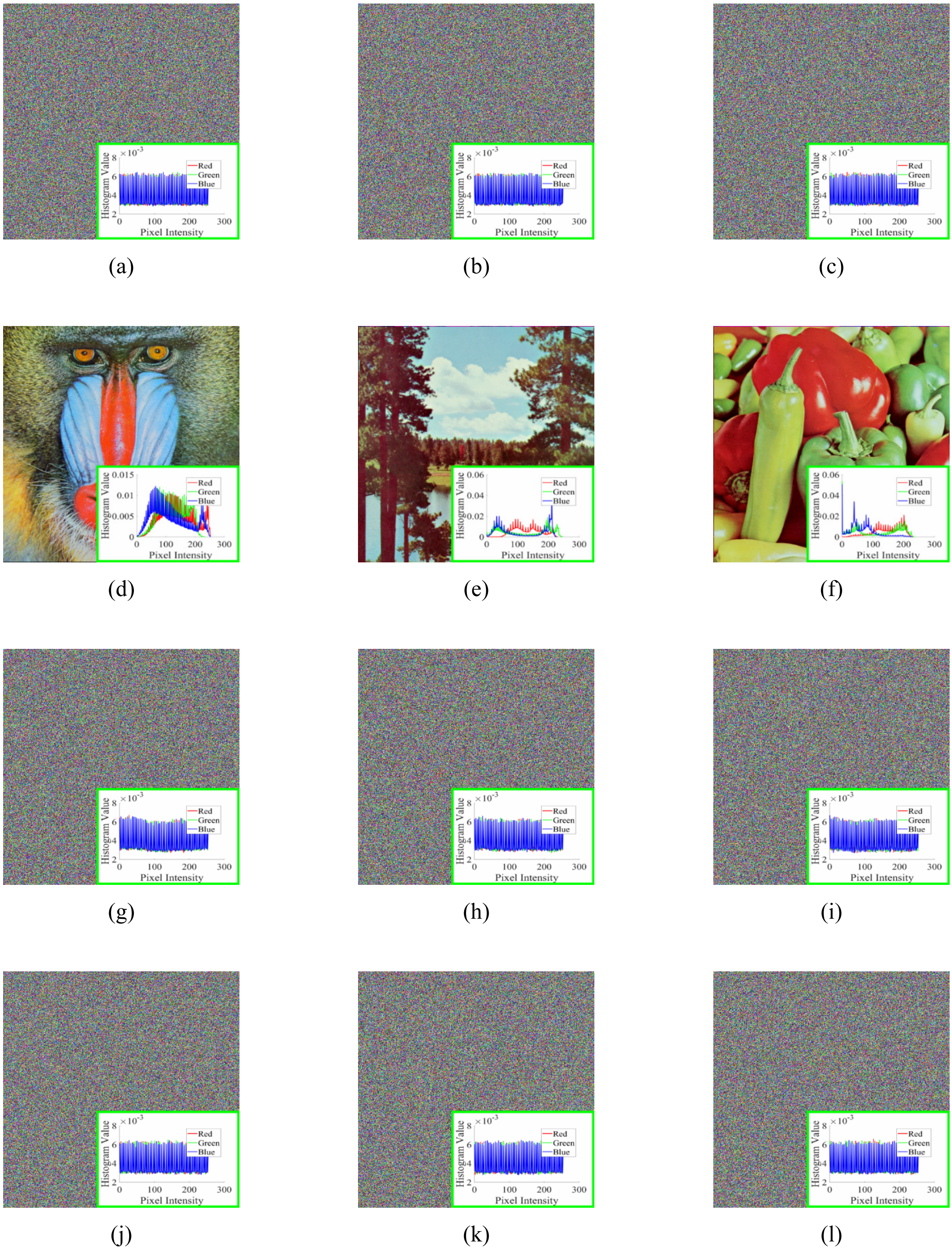


Figure 5. Proposed method with random image, for $n=3$: (a)-(c) $\{S_1, S_2, S_3\}$. (d)-(f) $\{I_1, I_2, I_3\}$ reconstructed with correct chaotic keys. (g)-(i) $\{I_1, I_2, I_3\}$ reconstructed with incorrect chaotic keys. (j)-(k) $\{I_1, I_2\}$ reconstructed from n-1 shared images. (l) $\tilde{I}_1$ reconstructed from n-2 shared images.

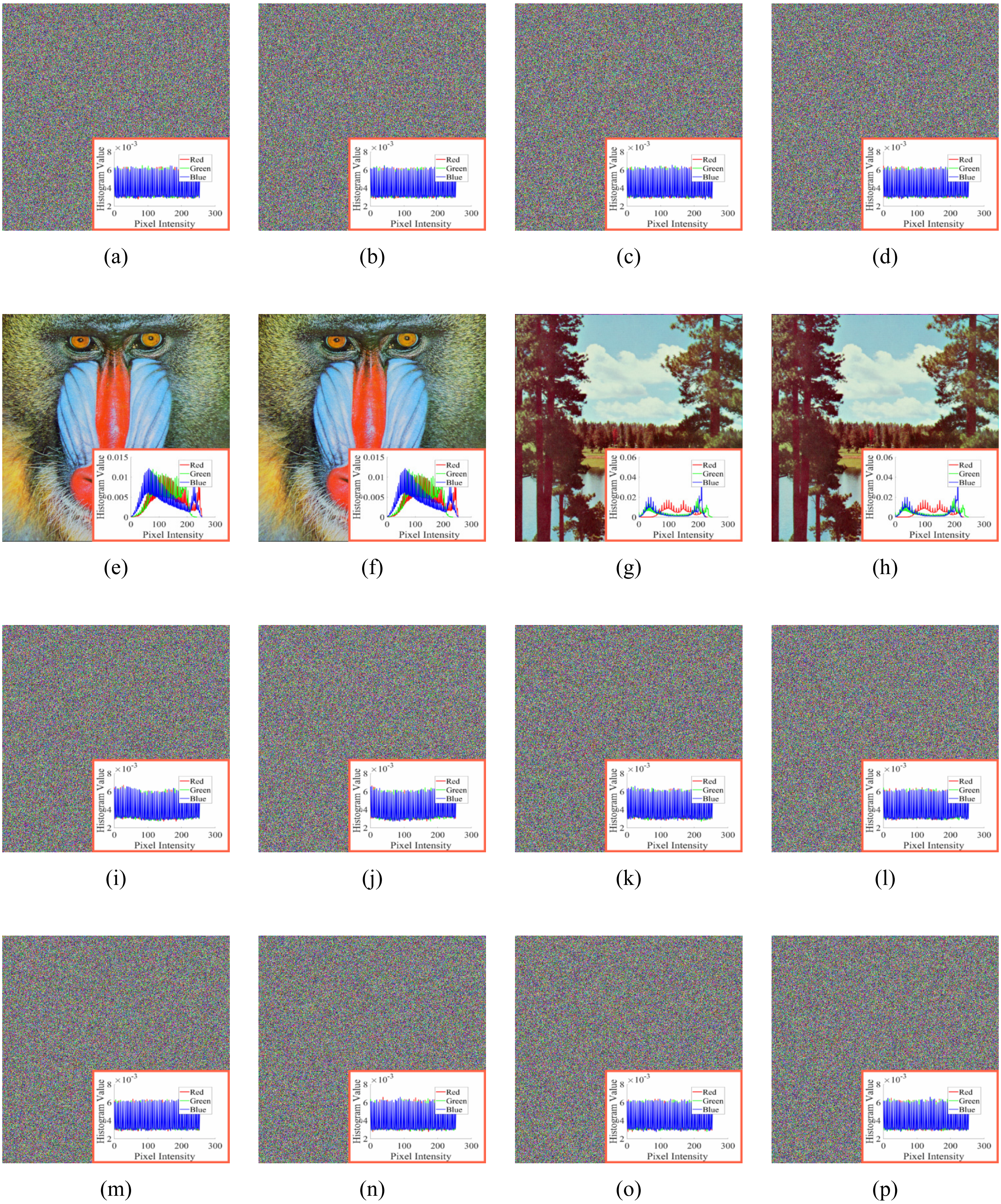


Figure 6. Proposed method which transform secret images into *nk* shared images, for n = 4 and k = 2: (a)-(d) $\{S_{1,1}, S_{1,2}, S_{2,1}, S_{2,2}\}$. (e)-(h) $\{\tilde{I}_{1,1}, \tilde{I}_{1,2}, \tilde{I}_{2,1}, \tilde{I}_{2,2}\}$ recovered with correct chaotic keys. (i)-(l) $\{\tilde{I}_{1,1}, \tilde{I}_{1,2}, \tilde{I}_{2,1}, \tilde{I}_{2,2}\}$ recovered with incorrect chaotic keys. (m)-(n) $\{\tilde{I}_{1,1}, \tilde{I}_{1,2}\}$ recovered from *nk*-1 shared images. (o)-(p) $\{\tilde{I}_{1,1}, \tilde{I}_{1,2}\}$ recovered from *nk*-2 shared images.

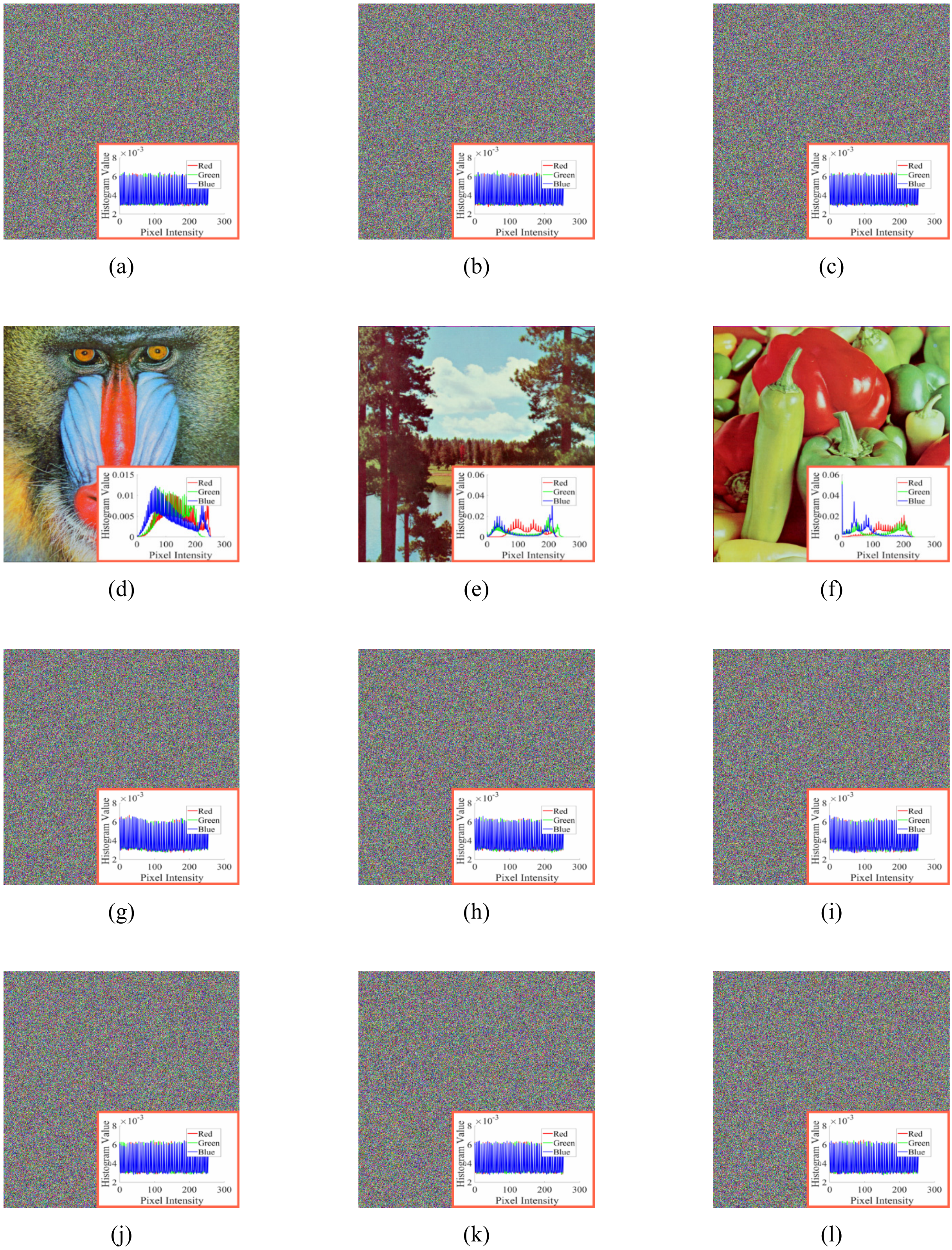


Figure 7. Proposed method which transforms secret images into *nk* shared images, for n = 3 and k = 2: (a)-(c) $\{S_{1,1}, S_{2,1}, S_{3,1}\}$. (d)-(f) $\{\tilde{I}_{1,1}, \tilde{I}_{2,1}, \tilde{I}_{3,1}\}$ reconstructed with correct chaotic keys. (g)-(i) $\{\tilde{I}_{1,1}, \tilde{I}_{2,1}, \tilde{I}_{3,1}\}$ reconstructed with incorrect chaotic keys. (j)-(l) $\tilde{I}_{1,1}$ reconstructed from *nk*-1, *nk*-2, and *nk*-3 shared images, respectively.

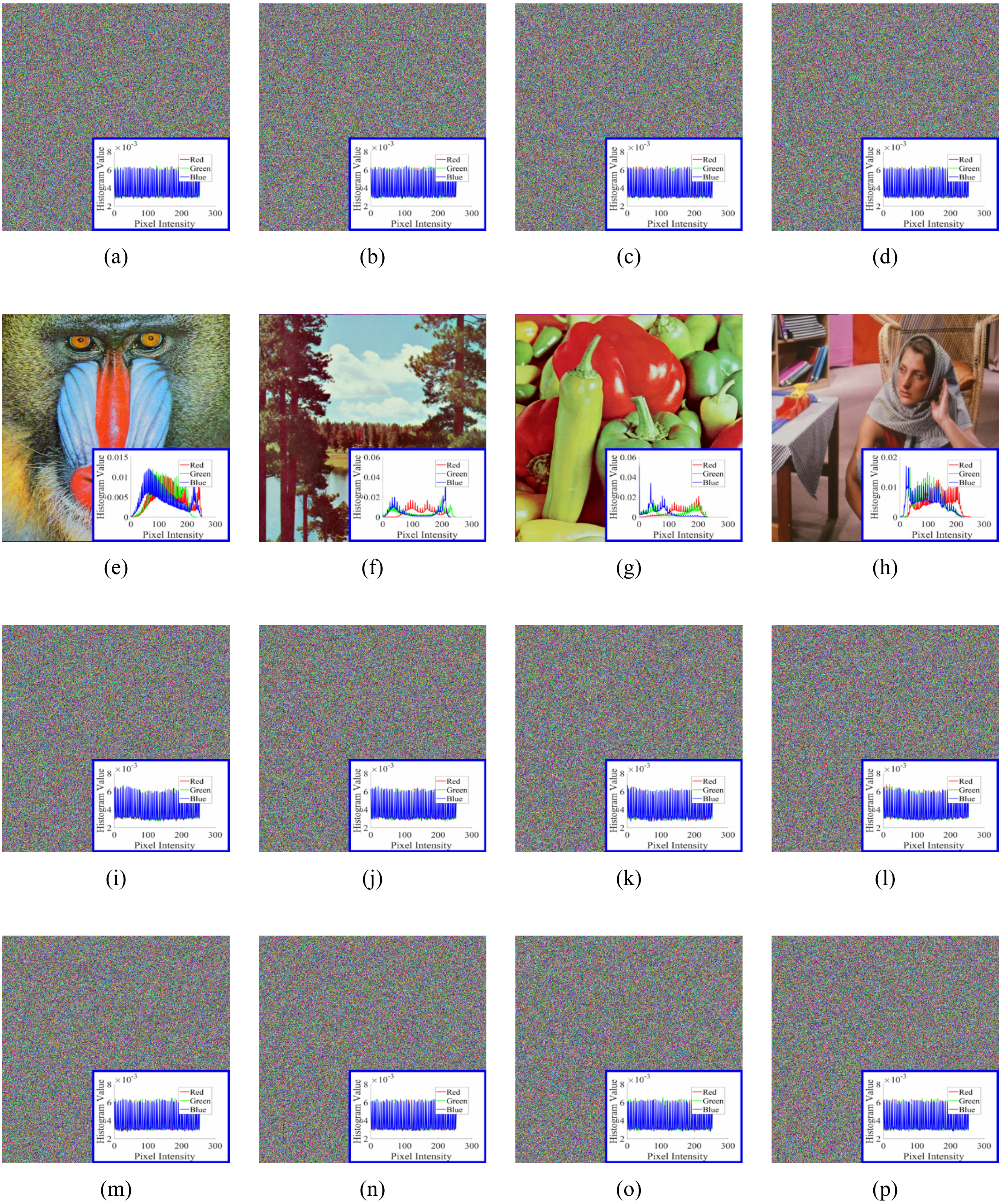


Figure 8. Proposed method with double masking coefficients, for n = 4: (a)-(d) $\{S_1, S_2, S_3, S_4\}$. (e)-(h) $\{\tilde{I}_1, \tilde{I}_2, \tilde{I}_3, \tilde{I}_4\}$ recovered with correct chaotic keys. (i)-(l) $\{\tilde{I}_1, \tilde{I}_2, \tilde{I}_3, \tilde{I}_4\}$ recovered with incorrect chaotic keys. (m)-(n) $\{\tilde{I}_1, \tilde{I}_2\}$ recovered from n-1 shared images. (o)-(p) $\tilde{I}_1$ recovered from n-2 and n-3 shared images, respectively.

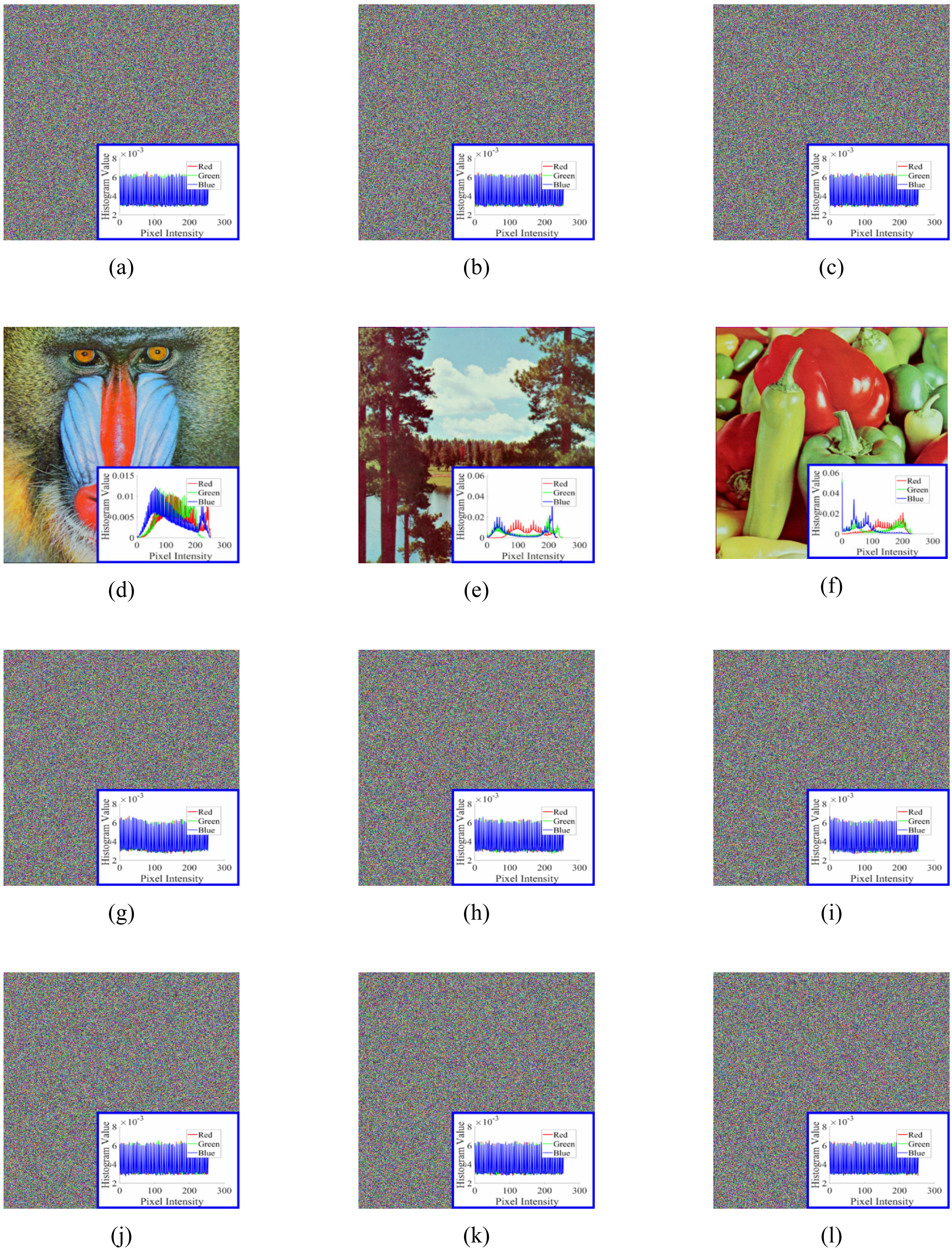


Figure 9. Proposed method with double masking coefficients, for n = 3: (a)-(c) $\{S_1, S_2, S_3\}$. (d)-(f) $\{I_1, I_2, I_3\}$ reconstructed with correct chaotic keys. (g)-(i) $\{\tilde{I}_1, \tilde{I}_2, \tilde{I}_3\}$ reconstructed with incorrect chaotic keys. (j)-(k) $\{\tilde{I}_1, \tilde{I}_2\}$ reconstructed from n-1 shared images. (l) $\tilde{I}_1$ reconstructed with n-2 shared images.

Table 1. Similarity comparisons over 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

Table 2 compares the differential attacks between the secret and shared images. Herein, the measurements are conducted in terms of MAE, NPCR, and UACI scores that show the superiority of proposed method against the other schemes. It indicates that the proposed method gives better randomize results on shared images in comparison with [7].

Table 2. Comparisons of differential attacks between secret and shared images

MAE				
Secret and Shared Images	[7]	Proposed 1	Proposed 2	Proposed 3
I_1, S_1	27.66	76.350	76.380	76.350
I_1, S_2	28.05	76.267	76.384	76.267
I_1, S_3	28.09	76.298	76.404	76.298
I_1, S_4	27.87	76.374	76.370	76.374
I_2, S_1	33.01	82.173	82.151	82.173
I_2, S_2	33.26	82.149	82.142	82.149
I_2, S_3	33.34	82.206	82.139	82.206
I_2, S_4	33.20	82.099	82.162	82.099
I_3, S_1	23.77	82.146	82.303	82.146
I_3, S_2	23.96	82.205	82.184	82.205
I_3, S_3	24.49	82.308	82.187	82.308
I_3, S_4	24.01	82.169	82.179	82.169
I_4, S_1	19.99	75.941	75.937	75.941
I_4, S_2	20.43	75.987	75.903	75.987
I_4, S_3	20.63	76.027	75.902	76.027
I_4, S_4	20.36	76.024	75.970	76.024
Average	26.383	79.170	79.169	79.170
NPCR				
Secret and Shared Images	[7]	Proposed 1	Proposed 2	Proposed 3
I_1, S_1	99.41	99.614	99.610	99.614
I_1, S_2	99.41	99.624	99.614	99.624
I_1, S_3	99.43	99.615	99.610	99.615
I_1, S_4	99.44	99.607	99.612	99.607
I_2, S_1	99.56	99.603	99.613	99.603
I_2, S_2	99.54	99.604	99.605	99.604
I_2, S_3	99.57	99.602	99.614	99.602
I_2, S_4	99.57	99.601	99.615	99.601
I_3, S_1	99.57	99.601	99.603	99.601
I_3, S_2	99.47	99.604	99.605	99.604
I_3, S_3	99.49	99.622	99.609	99.622
I_3, S_4	99.46	99.604	99.613	99.604
I_4, S_1	99.46	99.612	99.612	99.612
I_4, S_2	99.46	99.605	99.606	99.605
I_4, S_3	99.48	99.618	99.610	99.618
I_4, S_4	99.47	99.621	99.609	99.621
Average	99.49	99.610	99.610	99.610

Table 2. (continued)

UACI				
Secret and Shared Images	[7]	Proposed 1	Proposed 2	Proposed 3
I_1 , S_1	20.88	33.464	33.464	33.464
I_1 , S_2	21.18	33.464	33.464	33.464
I_1 , S_3	21.22	33.464	33.464	33.464
I_1 , S_4	21.02	33.464	33.464	33.464
I_2 , S_1	26.79	33.464	33.464	33.464
I_2 , S_2	26.99	33.464	33.464	33.464
I_2 , S_3	27.05	33.464	33.464	33.464
I_2 , S_4	26.92	33.464	33.464	33.464
I_3 , S_1	23.28	33.464	33.464	33.464
I_3 , S_2	23.42	33.464	33.464	33.464
I_3 , S_3	23.85	33.464	33.464	33.464
I_3 , S_4	23.44	33.464	33.464	33.464
I_4 , S_1	22.21	33.464	33.464	33.464
I_4 , S_2	22.55	33.464	33.464	33.464
I_4 , S_3	22.71	33.464	33.464	33.464
I_4 , S_4	22.48	33.464	33.464	33.464
Average	23.499	33.464	33.464	33.464

Other comparisons, i.e. correlation coefficient, RMSE, and PSNR values, measure similarity degree between the secret and shared images. These comparisons are conducted for the proposed method against the others [1-3, 7] in Table 3. The proposed method gives the lowest averaged correlation coefficient (around 0), highest average RMSE, and the lowest PSNR values. Table 4 gives comparisons over shared images under correlation coefficient, RMSE, and PSNR scores. The proposed method yields the highest RMSE and lowest PSNR values compared to the other schemes. However, it is slightly inferior under correlation coefficient. But, the proposed method still offers benefit in terms of shared images similarity.

Table 3. Similarity comparisons over secret and shared images

Correlation							
Secret and Shared Images	[1]	[2]	[3]	[7]	Proposed 1	Proposed 2	Proposed 3
I_1 , S_1	0.00	−0.0162	0.03	−0.0023	0.000	0.000	0.000
I_1 , S_2	0.02	0.01	−0.0258	−0.0039	0.002	-0.002	0.002
I_1 , S_3	−0.0169	−0.0027	0.07	0.00	0.002	-0.002	0.002
I_1 , S_4	−0.0130	0.11	−0.1301	0.00	-0.001	0.000	-0.001
I_2 , S_1	0.00	0.01	−0.0057	0.00	0.001	0.001	0.001
I_2 , S_2	−0.0224	0.02	0.03	−0.0014	0.000	0.000	0.000
I_2 , S_3	0.10	0.01	0.00	0.00	-0.001	0.000	-0.001
I_2 , S_4	−0.0518	0.01	0.05	−0.0023	0.002	0.000	0.002
I_3 , S_1	0.00	−0.0025	0.08	0.00	0.001	-0.001	0.001
I_3 , S_2	0.02	−0.0032	−0.0085	0.00	0.001	0.001	0.001
I_3 , S_3	0.07	−0.0079	0.04	−0.0017	-0.001	0.001	-0.001
I_3 , S_4	0.17	0.01	0.03	0.00	0.001	0.002	0.001
I_4 , S_1	−0.0015	−0.0081	−0.0955	0.00	0.001	0.001	0.001
I_4 , S_2	0.01	0.01	0.03	−0.0037	0.000	0.000	0.000
I_4 , S_3	−0.0409	0.11	0.05	0.00	-0.001	0.001	-0.001
I_4 , S_4	0.05	−0.0043	0.04	−0.0004	-0.002	0.000	-0.002
Average	0.05	0.03	0.04	0.00	0.000	0.000	0.000

Table 3. (continued)

RMSE							
Secret and Shared Images	[1]	[2]	[3]	[7]	Proposed 1	Proposed 2	Proposed 3
I_1, S_1	10.92	10.68	10.53	10.77	92.806	92.790	92.806
I_1, S_2	11.47	10.83	10.94	10.81	92.686	92.820	92.686
I_1, S_3	10.52	10.88	10.81	10.79	92.704	92.825	92.704
I_1, S_4	11.16	10.11	10.93	10.78	92.828	92.797	92.828
I_2, S_1	10.73	10.58	10.53	10.62	100.037	100.030	100.037
I_2, S_2	10.86	10.64	10.80	10.58	100.042	100.022	100.042
I_2, S_3	10.47	10.75	10.61	10.58	100.076	100.001	100.076
I_2, S_4	10.68	10.68	10.68	10.61	99.967	100.023	99.967
I_3, S_1	10.26	9.88	9.92	10.11	100.296	100.410	100.296
I_3, S_2	10.40	10.03	10.05	9.97	100.328	100.304	100.328
I_3, S_3	9.87	10.06	10.27	9.95	100.404	100.292	100.404
I_3, S_4	10.66	9.94	10.30	10.15	100.292	100.280	100.292
I_4, S_1	10.03	9.39	9.74	9.53	92.244	92.243	92.244
I_4, S_2	10.38	9.50	9.92	9.52	92.313	92.225	92.313
I_4, S_3	9.66	8.81	9.88	9.56	92.337	92.211	92.337
I_4, S_4	10.29	9.44	9.97	9.45	92.362	92.289	92.362
Average	10.52	10.14	10.37	10.24	96.358	96.348	96.358

PSNR(dB)							
Secret and Shared Images	[1]	[2]	[3]	[7]	Proposed 1	Proposed 2	Proposed 3
I_1, S_1	27.40	27.59	27.71	27.52	8.786	8.788	8.786
I_1, S_2	26.97	27.47	27.38	27.49	8.798	8.785	8.798
I_1, S_3	27.73	27.43	27.49	27.51	8.796	8.785	8.796
I_1, S_4	27.21	28.07	27.39	27.51	8.785	8.787	8.785
I_2, S_1	27.56	27.67	27.72	27.64	8.176	8.178	8.176
I_2, S_2	27.45	27.63	27.50	27.68	8.176	8.178	8.176
I_2, S_3	27.77	27.54	27.65	27.67	8.172	8.180	8.172
I_2, S_4	27.60	27.60	27.60	27.65	8.181	8.177	8.181
I_3, S_1	27.94	28.27	28.24	28.07	8.130	8.123	8.130
I_3, S_2	27.82	28.14	28.12	28.19	8.129	8.131	8.129
I_3, S_3	28.28	28.11	27.93	28.20	8.122	8.133	8.122
I_3, S_4	27.61	28.22	27.91	28.04	8.131	8.133	8.131
I_4, S_1	28.18	28.71	28.40	28.59	8.835	8.836	8.835
I_4, S_2	27.84	28.61	28.23	28.60	8.829	8.837	8.829
I_4, S_3	28.47	29.27	28.27	28.55	8.827	8.839	8.827
I_4, S_4	27.91	28.67	28.19	28.66	8.824	8.831	8.824
Average	27.73	28.06	27.86	27.97	8.481	8.483	8.481

Table 4. Similarity comparisons over shared images

Correlation							
Shared Images	[1]	[2]	[3]	[7]	Proposed 1	Proposed 2	Proposed 3
S_1, S_2	−0.0002	0.03	0.04	0.03	0.050	0.025	0.050
S_1, S_3	−0.0038	−0.1014	0.04	0.04	0.044	0.022	0.044
S_1, S_4	0.00	0.02	0.00	0.01	0.076	0.036	0.076
S_2, S_3	0.05	0.04	−0.0816	−0.0123	0.043	0.021	0.043
S_2, S_4	0.01	0.00	0.06	0.16	0.047	0.024	0.047
S_2, S_4	0.00	0.02	0.01	0.04	0.075	0.037	0.075
Average	0.02	0.02	0.03	0.06	0.056	0.028	0.056
RMSE							
Shared Images	[1]	[2]	[3]	[7]	Proposed 1	Proposed 2	Proposed 3
S_1, S_2	10.92	10.76	11.01	10.61	101.900	103.227	101.900
S_1, S_3	10.47	10.96	10.80	10.60	102.223	103.349	102.223
S_1, S_4	10.88	10.85	10.91	10.54	100.542	102.610	100.542
S_2, S_3	10.05	10.71	10.75	10.71	102.237	103.362	102.237
S_2, S_4	10.78	10.75	10.89	10.49	102.090	103.269	102.090
S_2, S_4	11.00	10.87	10.82	10.65	100.551	102.527	100.551
Average	10.68	10.82	10.86	10.60	101.591	103.057	101.591
PSNR (dB)							
Shared Images	[1]	[2]	[3]	[7]	Proposed 1	Proposed 2	Proposed 3
S_1, S_2	27.40	27.53	27.33	27.65	7.967	7.856	7.967
S_1, S_3	27.76	27.37	27.50	27.66	7.940	7.845	7.940
S_1, S_4	27.43	27.46	27.41	27.71	8.084	7.909	8.084
S_2, S_3	28.12	27.57	27.53	27.57	7.939	7.844	7.939
S_2, S_4	27.57	27.53	27.42	27.75	7.951	7.852	7.951
S_2, S_4	27.34	27.48	27.48	27.61	8.083	7.916	8.083
Average	27.60	27.49	27.45	27.66	7.994	7.870	7.994

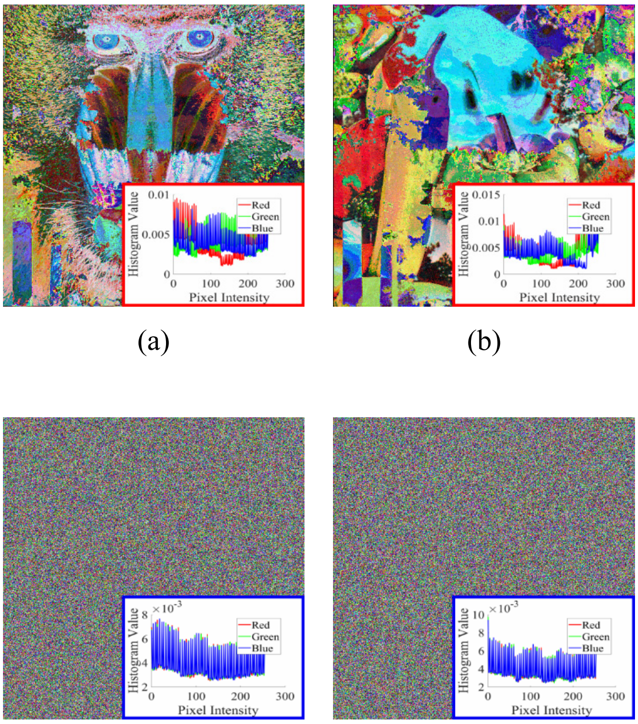
Table 5 compares the methodology and algorithm aspect between the proposed method and the others [1-7]. The proposed method achieves the highest randomness level. It is caused by incorporating the image encryption before performing the shared images generation. For implementing the secure MSS system, it can be highly considered compared to the other schemes.

Table 5. Comparisons in terms of algorithm aspects

Parameters	Proposed	[7]	[6]	[5]	[4]	[3]	[2]	[1]
Image Type	Color	Color	Binary	Binary	Binary	Binary	Grayscale	Grayscale
Secret Sharing Scheme	(n, n) with n is even/odd number	(n, n)while n is even number	(t, n)	(t, n)	(t, n)	(t, n)	(n, n)	$(n, n+1)$
Multi-Threshold	No	No	Yes	Yes	Yes	Yes	No	No
Pixel Expansion	No	No	No	No	No	No	No	No
Information Reveal	No	No	Partial	Partial	Partial	Partial	Partial	Partial
Combination of Secrets	Yes	Yes	No	No	No	No	No	No
Randomness	Very High	High	Average	Average	Average	Average	Average	Low
Recovery Strategy	CRT	CRT	Lagranges	CRT	Boolean	Boolean	XOR	XOR
Sharing Capacity	n/n	n/n	$1/n$	$1/n$	$1/n$	$1/n$	n/n	$n/(+1)$
Recovery of Secrets	Lossless	Lossless	Lossless	Lossless	Lossless	Lossless	Lossless	Lossless

4.5 Overlying Two Shared Images

This experiment validates the benefit of proposed method in terms of information visibility. It investigates the effect of image encryption in the secure MSS system. Herein, two shared images are overlaid together to obtain the visual recognition of image content**.** The former scheme [7] and proposed method generate four shared images $\{S_1, S_2, S_3, S_4\}$, while all images in Figure 2 are turned as secret images. Figure 10(a) to Figure 10(b) are the overlaid results of two shared images $S_1 \oplus S_2$ and $S_2 \oplus S_3$, respectively, while $\{S_1, S_2, S_3\}$ are from [7]. This overlying operation with XOR operator indicates $S_1 \oplus S_2 = \{I_1 \oplus M\} \oplus \{I_2 \oplus M\} = I_1 \oplus I_2$. As shown in these figures, the visual content of overlaid images becomes very hard to be perceived and recognized as Baboon and Peppers images. It causes unpleasant condition since a malicious attacker can recognize the meaningful image content. However, the proposed method can suffer the aforementioned problem. Figure 10(c) to Figure 10(d) are overlaid results of $S_1 \oplus S_2$ and $S_2 \oplus S_3$, respectively, while $\{S_1, S_2, S_3\}$ are from the proposed method. Again, one cannot easily recognize the visual content of overlaid images. The image encryption gives high impact on improving security level of MSS as indicated with good performance of proposed method.



(a) (b)

(c) (d)

Figure 10. The results of (a, c) $S_1 \oplus S_2$ and (b, d) $S_2 \oplus S_3$. Images in (a)-(b) and (c)-(d) are from [7] and the proposed method with double masking coefficients, respectively.

5 Conclusions

This paper presents some techniques for solving the problem on former MSS scheme while n is odd. We introduce the usage of random image, converting n secret images into nk encrypted secret images, and utilizing double masking coefficients. The fusion of encryption and MSS increase the stability and security required for good MSS design. The proposed MSS method can be effectively implemented for achieving the correctness issue and high randomness of shared images.

References

[1] T.-H. Chen, C.-S. Wu, Efficient Multi-secret Image Sharing Based On Boolean Operations, *Signal Processing*, Vol. 91, No. 1, pp. 90-97, January, 2011.

[2] C.-C. Chen, W.-J. Wu, A Secure Boolean-based Multi-secret Image Sharing Scheme, *Journal of System and Software*, Vol. 92, pp. 107-114, June, 2014.

[3] C.-N. Yang, C.-H. Chen, S.-R. Cai, Enhanced Boolean-based Multi Secret Image Sharing Scheme, *Journal of System and Software*, Vol. 116, pp. 22-34, June, 2016.

[4] J.-B. Feng, H.-C. Wu, C.-S. Tsai, Y.-P. Chu, A New Multi-secret Images Sharing Scheme Using Lagrange's Interpolation, *Journal of System and Software*, Vol. 76, No. 3, pp. 327-339, June, 2005.

[5] C. Guo, C.-C. Chang, C. Qin, A Multi-threshold Secret Image Sharing Scheme Based on MSP, *Pattern Recognition Letters*, Vol. 33, No. 12, pp. 1594-1600, September, 2012.

[6] C. Guo, H. Zhang, Q. Song, M. Li, A Multi-threshold Secret Image Sharing Scheme Based on the Generalized Chinese Reminder Theorem, *Multimedia Tools and Applications*, Vol. 75, No. 18, pp. 11577-11594, September, 2016.

[7] M. Deshmukh, N. Nain, M. Ahmed, A Novel Approach for Sharing Multiple Color Images by Employing Chinese Remainder Theorem, *Journal of Visual Communication and Image Representation*, Vol. 49, pp. 291-302, November, 2017.

[8] J.-M. Guo, H. Prasetyo, False-positive-free SVD-based Image Watermarking, *Journal of Visual Communication and Image Representation*, Vol. 25, No. 5, pp. 1149-1163, July, 2014.

[9] X. Wu, J. Weng, W. Yan, Adopting Secret Sharing for Reversible Data Hiding in Encrypted Images, *Signal Processing*, Vol. 143, pp. 269-281, February, 2018.

[10] Z. L. Liu, C. M. Pun, Reversible Data-hiding in Encrypted Images by Redundant Space Transfer, *Information Sciences*, Vol. 433-434, pp. 188-203, April, 2018.

[11] F. Khelifi, On the Security of a Stream Cipher in Reversible Data Hiding Schemes Operating in the Encrypted Domain, *Signal Processing*, Vol. 143, pp. 336-345, February, 2018.

[12] H. Prasetyo, A New Image Encryption Technique Using Simple Chaotic Maps, *International Symposium on Electronics and Smart Devices 2018 (ISESD 2018)*, Bandung, Indonesia, 2018, pp. 1-4.

[13] Image Database, http://sipi.usc.edu/database.

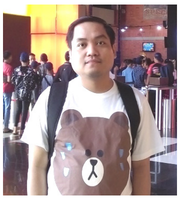
[14] J.-C. Liu, C.-H. Lin, K.-Y. Lee, Cloud-based Personal Data Protection System and Its Performance Evaluation, *Journal of Internet Technology*, Vol. 20, No. 6, pp. 1721-1727, November, 2019.

[15] Q. Wang, D. Gao, W. Zhu, Cloud-enabled Software-defined

Vehicular Networks: Architecture, Applications, and Challenges, *Journal of Internet Technology*, Vol. 20, No. 6, pp. 1819-1828, November, 2019.

[16] X. Sun, Y. Liu, W. Wei, W. Jing, C. Zhao, Based on QoS and Energy Efficiency Virtual Machines Consolidation Techniques in Cloud, *Journal of Internet Technology*, Vol. 20, No. 6, pp. 1849-1859, November, 2019.

Biographies



Heri Prasetyo received the bachelor degree from Department of Informatics Engineering, Institut Teknologi Sepuluh Nopember (ITS), Indonesia in 2006. He received master and doctoral degrees from Department of Computer Science and Information Engineering, and Department of Electrical Engineering, respectively, both from National Taiwan University of Science and Technology (NTUST), Taiwan, in 2009 and 2015. He received the Best Dissertation Award from the Taiwan Association for Consumer Electronics (TACE) in 2015, the Best Paper Awards from the International Symposium on Electronics and Smart Devices 2017 (ISESD 2017), ISESD 2019, International Conference on Science in Information Technology (ICSITech 2019), and the Outstanding Faculty Award 2019 from his current affiliation. His research interest includes multimedia signal processing, computational intelligence, pattern recognition, and machine learning.

Chih-Hsien Hsia was born in Taipei city, Taiwan, in 1979. He received the Ph.D. degree from Tamkang University, Taiwan, in 2010. In 2007, he was a Visiting Scholar with Iowa State University, Ames, IA, USA. From 2010 to 2013, he was a Postdoctoral Research Fellow with the Department of Electrical Engineering, National Taiwan University of Science and Technology, Taipei, Taiwan. From 2013 to 2015, he was an Assistant Professor with the Department of Electrical Engineering at Chinese Culture University, Taiwan. He was an Associate Professor with the Department of Electrical Engineering, Chinese Culture University, Taiwan, from 2015 to 2017. He currently is an Associate Professor with the Department of Computer Science and Information Engineering, National Ilan University, Taiwan. His research interests include DSP IC Design, Multimedia Signal Processing, and Cognitive Learning.He has served as a Guest Editor of three special issues of the Journal of Imaging Science and Technology, the Sensors and Materials, the Journal of Internet Technology, the Journal of Applied Science and Engineering and the Journal of Computers. He has serves on Associate Editor of the Journal of Imaging Science and Technology and the Journal of Computers.

Jing-Yi Deng was born in Taoyuan, Taiwan, in 1996. He received the Computer Science and Information Engineering, National Ilan University in 2018. Currently, he is a master's student of Computer Science and Information Engineering, National Ilan University, Taiwan. His research interests include Image Processing and Virtual Reality.