Robust Secret Image Sharing Resistant to Noise in Shares

XUEHU YAN, LINTAO LIU, LONGLONG LI, and YULIANG LU, National University of Defense Technology, China

A secret image is split into n shares in the generation phase of secret image sharing (SIS) for a (k, n) threshold. In the recovery phase, the secret image is recovered when any k or more shares are collected, and each collected share is generally assumed to be lossless in conventional SIS during storage and transmission. However, noise will arise during real-world storage and transmission; thus, shares will experience data loss, which will also lead to data loss in the secret image being recovered. Secret image recovery in the case of lossy shares is an important issue that must be addressed in practice, which is the overall subject of this article. An SIS scheme that can recover the secret image from lossy shares is proposed in this article. First, robust SIS and its definition are introduced. Next, a robust SIS scheme for a (k, n) threshold without pixel expansion is proposed based on the Chinese remainder theorem (CRT) and error-correcting codes (ECC). By screening the random numbers, the share generation phase of the proposed robust SIS is designed to implement the error correction capability without increasing the share size. Particularly in the case of collecting noisy shares, our recovery method is to some degree robust to some noise types, such as least significant bit (LSB) noise, JPEG compression, and salt-and-pepper noise. A theoretical proof is presented, and experimental results are examined to evaluate the effectiveness of our proposed method.

CCS Concepts: • **Security and privacy** → **Graphical/visual passwords**; **Access control**; **Key management**; **Digital rights management**;

Additional Key Words and Phrases: Secret image sharing, robust secret image sharing, Chinese remainder theorem, error-correcting codes, JPEG compression

ACM Reference format:

Xuehu Yan, Lintao Liu, Longlong Li, and Yuliang Lu. 2021. Robust Secret Image Sharing Resistant to Noise in Shares. *ACM Trans. Multimedia Comput. Commun. Appl.* 17, 1, Article 24 (April 2021), 22 pages. <https://doi.org/10.1145/3419750>

1 INTRODUCTION

With the widespread development and application of the Internet and multimedia technology, digital multimedia data are easily obtained, transmitted, and manipulated. Therefore, security of digital multimedia is very important for protecting sensitive multimedia data from malicious interference during transmission over public channels. Traditional ways of ensuring a high level of security for multimedia include cryptography and information hiding. Cryptographic techniques transform the multimedia data between incomprehensible and comprehensible forms

This work was supported by the National Natural Science Foundation of China under Grant No. 61602491.

Authors' addresses: X. Yan, L. Liu, L. Li, and Y. Lu, National University of Defense Technology, No.460 HUANGSHAN Road, Hefei, Anhui, 230037, China; emails: publictiger@126.com, {liuta1989, lilongs8636}@163.com, publicLuYL@126.com.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from [permissions@acm.org](https://permissions.acm.org).

© 2021 Copyright held by the owner/author(s). Publication rights licensed to ACM.

1551-6857/2021/04-ART24 \$15.00

<https://doi.org/10.1145/3419750>

by encryption and decryption operations using secret keys. Information hiding [18] embeds multimedia data into digital cover media. However, when the cover media's data are destroyed or lost due to typical causes, the embedded multimedia data will be unavailable. Thus, secret sharing has been proposed to overcome this limitation.

In the generation phase, secret sharing for a (k, n) threshold splits the multimedia data into n shares, called shadow images or shadows, which are subsequently distributed to the corresponding n participants; in the recovery phase, the multimedia data are recovered when any k or more shares are collected. An attacker cannot recover the multimedia data even by using a very computationally powerful device when fewer than k shares are collected. Hence, secret sharing is applicable in many scenarios, such as digital watermarking, key management, identity authentication, access control, password transmission, blockchains, and distributed storage in a cloud [3, 5, 25, 39].

Because digital images are one of the most important media types, secret image sharing (SIS) has been extensively researched. Digital images have a special feature that distinguishes them from general digital data (even though they are a specific form of such data), whereby each binary (grayscale) pixel is represented by 1 bit (8 bits, i.e., 1 Byte); thus, SIS can be easily applied to data sharing. The basic principles of widely studied high-quality SIS techniques include polynomials [26, 40], the Chinese remainder theorem (CRT) [1, 32], and so on [14]. We note that visual cryptography (VC), a.k.a. visual secret sharing (VSS) [10, 17, 29, 34] is also widely studied. (k, n) threshold VC belongs to (k, n) threshold SIS, i.e., VC is one branch of SIS. VC is generally for binary secret images and is lossy by nature, thus, we mainly focus on a secret sharing method with high-quality recovery of the secret image.

For high-quality recovery of the secret image, the first polynomial-based secret sharing method for a (k, n) threshold introduced by Shamir [20] entailed constructing a random $(k - 1)$ -degree polynomial to generate n shares. When any k or more shares are collected, the secret is recovered with high quality according to Lagrange interpolation. Inspired by Shamir's work, several enhanced polynomial-based SIS schemes [2, 16, 23, 35] with more properties have been put forward. The significance of polynomial-based SIS is that the recovered secret image is of high quality and there is no pixel expansion. However, it has the shortcomings that the recovered secret image is either slightly distorted or difficult to obtain, with a high computational complexity of $O(k \log^2 k)$ when obtaining a nondistorted image [1]).

Because the modular approach needs only $O(k)$ operations [1] to recover every secret pixel, Chinese remainder theorem-based SIS (CRTSIS) allows recovery of the nondistorted secret image with fewer calculations and has thus been explored in several other studies. Yan et al. [30] introduced CRT to SIS and achieved small information leakage and loss. Shyu et al. [22] extended Mignotte's scheme using a pseudorandom number generator in an approach that needed auxiliary encryption. Ulutas et al. [24] modified Asmuth Bloom's secret sharing scheme by dividing each grayscale image pixel's value. In their scheme, the random number range may be unsuitable, and thus, the (k, n) threshold may not be achieved. Moreover, image pixel values of double or more the scheme's parameter were not considered. Utilizing a chaotic map, Hu et al. [7] put forward another CRTSIS method with auxiliary encryption. A simple CRTSIS method satisfying the $(3, 5)$ threshold was presented by Chuang et al. [6] for RGB color images. The method either is lossy or requires prestoring the least significant bit (LSB). A CRTSIS method with lossless recovery for a (k, n) threshold has recently been designed by Yan et al. [33], and the explicit parameters have also been illustrated based on image features. Furthermore, Yan et al. [31] and Li et al. [12] developed CRTSIS methods with multiple decryptions and lossless recovery, respectively.

Fig. 1. Our motivation of robust SIS.

In the recovery phase of the above-mentioned SIS for a (k, n) threshold, the secret image can be recovered when any k or more shares are collected, and each collected share is in general assumed to be lossless during storage and transmission.

However, there will be noise [13, 36], such as LSB noise, JPEG compression, and salt-and-pepper noise [4] during real-world storage and transmission. Thus, the shares will be lossy, which will lead to the secret image also being recovered with data loss.

Secret image recovery in the case of lossy shares is important in practice; it is unfortunately seldom considered in the above-mentioned SIS schemes, including CRTSIS schemes, and is the motivation of this article.

SIS for a (k, n) threshold naturally has a loss-tolerance property, i.e., the creator of shares can recover the secret image with at least $n - k$ shares lost. Although several studies [8, 11, 19] have discussed a coalition of participants corrupted by means of the loss-tolerant property, secret recovery in the case of lossy shares has rarely been considered.

Figure 1 illustrates the motivation of robust SIS.

VC [17, 21, 27, 37] is naturally robust, because VC is implemented based on probability theory. A secret image with contrast loss can be recovered by stacking to some degree in the case of lossy shares. The value of the contrast loss is dependent on the noise density added to the shares. However, due to the stacking needed for recovery, the recovered secret image is naturally of low quality, i.e., a significant contrast loss occurs.

An alternative simple idea used to achieve robustness is to embed the shares into n cover images using steganography to output robust steganographic images. A typical approach has been presented by Mohammad and Ali [9]. The researchers proposed polynomial-based SIS to achieve robustness with the help of steganography [38]. In their scheme, a polynomial is first used to generate shares. Afterward, the shares are embedded into the cover images using an existing robust steganography technique to output steganographic images. Thus, the researchers' scheme is robust and produces steganographic images of high visual quality. However, a method of this kind has a high computational complexity and entails pixel expansion. In addition, robustness is achieved based on steganography rather than SIS.

Secret image recovery in the case of lossy shares without pixel expansion is an important issue and poses difficulty that must be dealt with in practice, which is the overall focus of this article. The recovery method generally entails using mathematical functions, such as interpolation and modulo, which are sensitive to low-level noise; thus, based on SIS itself and under the condition of no pixel expansion, achieving robust SIS for a (k, n) threshold is a key challenge. The research objective investigated in this article is to propose an SIS scheme without pixel expansion that can recover the secret image despite lossy shares.

In this article, robust SIS and its definition are first introduced. Next, a robust SIS scheme for a (k, n) threshold without pixel expansion is proposed based on CRT and error-correcting codes (ECC). By screening the random numbers, the share generation phase of the proposed robust SIS is designed to attain an error-correcting capability without increasing the share size; in this way, in the case of collecting a noisy share, our recovery method is to some degree robust to some noise types, such as LSB noise, JPEG compression, and salt-and-pepper noise. The characteristics of the

Table 1. Key Notations Used in This Article

Notation	Description
(k, n)	Threshold parameters
S	The original secret image
$W \times H$	The size of the original secret image
S'	The recovered secret image
SC_i	The i th share
SC'_i	The i th noisy share
t	The number of shares collected in the recovery phase
$S'_{i_1, i_2, \dots, i_t}$	The secret image recovered from shares $SC_{i_1}, SC_{i_2}, \dots, SC_{i_t}$
k_0, n_0 , and t_0	The length of each message, codeword length, and error-correcting capability in ECC
(HL, WL)	Block size parameters in ECC
N_A	The number of available values of A satisfying the equations in Step 8 of our method
D and R	The bits of a message and the corresponding check bits

proposed scheme are its robustness, lack of pixel expansion, lossless recovery, and use of the SIS principle. A theoretical proof is provided, and experimental results are examined to demonstrate the effectiveness of our proposed method.

The remaining sections are organized as follows: Section 2 introduces CRT. In Section 3, we discuss the introduced robust SIS definition and our proposed robust SIS algorithm in detail. Section 4 presents the proof of the security and performance analysis of the algorithm. Section 5 discusses the experimental results and comparisons. Section 6 presents the conclusions.

2 PRELIMINARIES

In this section, we introduce some preliminaries for our study. In (k, n) threshold SIS, n shares, denoted by $SC_1, SC_2, \dots, SC_n$, are generated for an original secret image S , and the secret image S' can be recovered from any t ($k \leq t \leq n, t \in \mathbb{Z}^+$) shares.

The key notations used in this article are shown in Table 1.

2.1 Chinese Remainder Theorem (CRT)

CRT, formally introduced in the southern and northern Chinese dynasties, can be used to solve a set of linear congruence equations.

First, a set of integers denoted by $m_i (i = 1, 2, \dots, k)$ is chosen subject to $\gcd(m_i, m_j) = 1, i \neq j$; then, according to CRT, Equation (1) has a unique solution

$$\begin{aligned}
 y &\equiv (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + \dots + a_k M_k M_k^{-1}) \pmod{M}, y \in [0, M - 1], \\
 y &\equiv a_1 \pmod{m_1} \\
 &\dots \\
 y &\equiv a_k \pmod{m_k},
 \end{aligned} \tag{1}$$

where $M = \prod_{i=1}^k m_i$, $M_i = M/m_i$ and $M_i M_i^{-1} \equiv 1 \pmod{m_i}$.

Both polynomial-based SIS and CRTSIS [1] have been widely researched. The reasons for using CRT in our scheme are stated as follows:

- (1) CRTSIS can achieve lossless recovery, while most polynomial-based SIS schemes are lossy.
- (2) The recovery method of polynomial-based SIS is Lagrange interpolation with a computational complexity of $O(k \log^2 k)$, while that in CRTSIS entails only modular operations with a complexity of $O(k)$; hence, CRTSIS needs fewer computations than polynomial-based SIS to recover the secret image.

2.2 Bose-Chaudhuri-Hocquenghem (BCH) Codes

Block code [15] is one widely applied kind of ECC that operates on fixed-size packets (blocks) of symbols or bits of predetermined size and can in general be hard-decoded in polynomial time with respect to the block length. In $ECC(k_0, n_0, t_0)$ block codes, k_0 , n_0 , and t_0 represent the size of each message, codeword length, and error-correcting capability, respectively. The error-correcting capability of a block code is t_0 if and only if $2t_0 + 1 \leq d \leq 2t_0 + 2$, where d denotes the minimum Hamming distance of the block code.

BCH is a typical type of classic block code and is usually used to correct some arbitrary number of errors per code block. It utilizes the theory of the generator polynomial defined by a cyclic code to achieve precise mathematical relations of message values and check values. One key feature of BCH codes is that there is strict control over the number of bit errors correctable by the code during code design. In particular, it is possible to design binary BCH codes for correcting multiple bit errors. Another feature of BCH codes is that we can easily decode them via syndrome decoding, a.k.a. an algebraic method, which will simplify the design of the decoder for the codes. Therefore, BCH is selected in our experiments to achieve the error-correcting capability.

Consider an example of BCH (7,4,1) codes. D denotes the bits of a message, and its corresponding check bits are denoted by R . If $D = (1001)$, then we use BCH (7,4,1) to encode D to obtain codeword $(D, R) = (1001110)$, where $R = (110)$. If we receive a noisy codeword (1001111), we can use BCH (7,4,1) to decode it to obtain the original $D = (1001)$, where one bit error has been corrected.

In extended BCH codes, one additional check bit pair equal to the result of XORing (D, R) , which can be used to check for an error, is added to the end of the codeword. In the example of extended BCH (8,4,1) codes, the extended codeword will be (10011100). Extended BCH codes will be used in our experiments.

3 INTRODUCTION OF ROBUST SIS DEFINITION AND THE PROPOSED ROBUST SIS SCHEME

3.1 Robust SIS Definition

Definition 3.1 (Robust Secret Image Sharing). In the generation phase of SIS for a (k, n) threshold, a secret image denoted by S is split into n original shares denoted by $SC_1, SC_2, \dots, SC_n$. In the recovery phase, the secret image is recovered from $SC_{i_1}, SC_{i_2}, \dots, SC_{i_t}$ by the traditional original method, where $\{i_1, i_2, \dots, i_t\}$ denotes any subset of t elements of $\{1, 2, \dots, n\}$, and the recovered secret image is denoted by S' . The n noisy shares denoted by $SC'_1, SC'_2, \dots, SC'_n$ result from adding noise to $SC_1, SC_2, \dots, SC_n$, respectively. We call an SIS scheme robust to noise for a (k, n) threshold if the following conditions are satisfied:

- (1) **Security condition:** the secret image will not be recovered from $SC'_{i_1}, SC'_{i_2}, \dots, SC'_{i_t}$ when $t < k$.
- (2) **Secret recovery condition:** the secret image can be recovered from $SC'_{i_1}, SC'_{i_2}, \dots, SC'_{i_t}$ when $t \geq k$.
- (3) **Robustness condition:** $IQR(SC'_{i_1}, SC'_{i_2}, \dots, SC'_{i_t}) > IQT(SC'_{i_1}, SC'_{i_2}, \dots, SC'_{i_t})$ when $t \geq k$,

where

- (1) $IQR(SC'_{i_1}, SC'_{i_2}, \dots, SC'_{i_t})$ denotes the image quality of the secret image denoted by $S'_{SC'_{i_1}, SC'_{i_2}, \dots, SC'_{i_t}}$ recovered from $SC'_{i_1}, SC'_{i_2}, \dots, SC'_{i_t}$ by the robust recovery method, and $IQT(SC'_{i_1}, SC'_{i_2}, \dots, SC'_{i_t})$ denotes the image quality of the secret image recovered from $SC'_{i_1}, SC'_{i_2}, \dots, SC'_{i_t}$ by the traditional recovery method;
- (2) the image quality means the similarity between S' and S , which can be evaluated by conventional metrics, such as the signal-to-noise-ratio (PSNR), the structural similarity index measure (SSIM) [28], and the contrast in VC; and
- (3) the greater the improvement in the image quality is, the stronger the robustness achieved.

If $IQR(SC'_{i_1}, SC'_{i_2}, \dots, SC'_{i_t}) = IQT(SC_{i_1}, SC_{i_2}, \dots, SC_{i_t})$, then we say that the robust SIS is fully robust to the noise; otherwise, we say that the robust SIS is partially robust to the noise.

We further analyze and discuss Definition 3.1 as follows:

- (1) The **security condition** and the **secret recovery condition** are inspired by SIS for a (k, n) threshold.
- (2) As the traditional secret sharing principle is in general based on mathematical theory, the recovery method is sensitive to the pixel values of shares. Accordingly, the errors due to noise will be propagated to the secret image recovered by the traditional recovery method.

3.2 Our Robust SIS Algorithm

The design idea of the proposed robust SIS algorithm is illustrated in Figure 2, and the pixels' processing order is shown in Figure 3. The algorithm is shown in detail in **Algorithm 1**; for an original secret image of size $W \times H$, threshold (k, n) , $BCH(k_0, n_0, t_0)$, and block size parameters (HL, WL) , the output comprises n shares $SC_1, SC_2, \dots, SC_n$ also of size $W \times H$, where $HL \times WL = n_0$ and $\frac{HL}{2} \times WL = k_0$ for the ECC codeword length, $HL \geq 2$ denotes the number of LSBs processed for each block, and $WL \geq 1$ denotes the number of secret pixels processed every time for each block, which will be clearly shown in Figure 3.

The recovery steps are illustrated in **Algorithm 2**.

Regarding Algorithm 1, we note the following:

- (1) To clearly understand Algorithm 1, please refer to Figure 2 and Figure 3.
- (2) Available parameters will be further analyzed in Section 4 and specified in Section 5.2.
- (3) The objective of Step 1 is to select a set of integers that satisfy CRT conditions. In general, we suggest choosing m_i to be as large as possible so the shares' pixel values will be distributed over a large range and suggest choosing p to be as small as possible for security. The available parameters will be further analyzed in Section 4 and specified in Section 5.2.
- (4) The objective of Steps 2 and 4 is to achieve the (k, n) threshold and lossless recovery, which will be analyzed in Section 4.
- (5) For a clear understanding, we take S and $HL = 8, WL = 4$ as an example to illustrate our idea of pixel selection order and construction of D^i and R^i , as shown in Figure 3, where we intend to obtain a maximally separated distribution of share pixels to resist burst noise to some degree. More importantly, in Steps 4.1 and 8, D^i are equal to $HL/2$ LSBs of the share pixel values, and, since the LSBs of the share pixel values in the current block have good randomness, the selection of bits of the message has good randomness. Thus, the output of check bits has good randomness as well, which results in acceptable randomness of the share pixel values in the next block even if D^i is screened.

ALGORITHM 1: Proposed (k, n) -threshold robust secret image sharing method.

Input: Secret image S of size $W \times H$, threshold (k, n) , block size parameters (HL, WL) , and extended $ECC(k_0, n_0, t_0)$.

Output: Share SC_i and its private corresponding integer m_i for $i = 1, 2, \dots, n$.

Step 1: Select a set of integers $\{128 \leq p < m_1 < m_2 \dots < m_n \leq 256\}$ that satisfy

- (1) $\gcd(m_i, m_j) = 1, i \neq j$,
- (2) $\gcd(m_i, p) = 1$ for $i = 1, 2, \dots, n$, and
- (3) $M > pN$,

where $M = \prod_{i=1}^k m_i$, $N = \prod_{i=1}^{k-1} m_{n-i+1}$ and p can be public among all n participants.

Step 2: Compute $T = \left\lceil \frac{\frac{M}{p} - 1}{2} \right\rceil$, which can be public.

Step 3: Let $B_{wl,b}^i$ denote the b th bit plane value of the w th pixel in the current block for the i th share, where $1 \leq b \leq 8$, $1 \leq wl \leq WL$, and $1 \leq i \leq n$.

D^i denotes the bits of the message in ECC for the i th share, and its corresponding check bits are denoted by R^i for $i = 1, 2, \dots, n$.

Follow the order shown in Figure 3 to select unprocessed secret pixels to construct the first block. Repeat Step 4.1 to process the secret pixels in the block one-by-one.

Step 4.1: Let $x = S(w, h)$, where (w, h) denotes the position in S of the secret pixel currently being processed.

If $0 \leq x < p$, then randomly select an integer A in $[T + 1, \left\lfloor \frac{M}{p} - 1 \right\rfloor]$, and calculate $y = x + Ap$; otherwise, randomly select an integer A in $[0, T)$, and calculate $y = x - p + Ap$.

Compute $a_i \equiv y \pmod{m_i}$, and set $SC_i(w, h) = a_i$ for $i = 1, 2, \dots, n$.

Step 4.2: Set $D^i = (B_{1, \frac{HL}{2}}^i, B_{1, \frac{HL}{2}-1}^i, \dots, B_{1,1}^i, B_{2, \frac{HL}{2}}^i, B_{2, \frac{HL}{2}-1}^i, \dots, B_{2,1}^i, \dots, B_{WL, \frac{HL}{2}}^i, B_{WL, \frac{HL}{2}-1}^i, \dots, B_{WL,1}^i)$ for $i = 1, 2, \dots, n$. Utilize $ECC(k_0, n_0)$ to encode bits of message D^i to obtain R^i for $i = 1, 2, \dots, n$, where $HL \times WL = n_0$ and $\frac{HL}{2} \times WL = k_0$.

Step 5: Repeat Steps 6–9 until all the secret pixels have been processed.

Step 6: Follow the order shown in Figure 3 to select unprocessed secret pixels to construct the current block.

Step 7.1: Repeat Step 7.2 to process the secret pixels in the current block one-by-one.

Step 7.2: Set $x = S(w, h)$, where (w, h) denotes the position in S of the secret pixel currently being processed. If $0 \leq x < p$, then randomly select an integer A in $[T + 1, \left\lfloor \frac{M}{p} - 1 \right\rfloor]$, and calculate $y = x + Ap$; otherwise, randomly select an integer A in $[0, T)$, and calculate $y = x - p + Ap$. Compute $a_i \equiv y \pmod{m_i}$, and set $SC_i(w, h) = a_i$ for $i = 1, 2, \dots, n$.

Step 8: If

$$B_{1,HL}^i = R^i(1), B_{1,HL-1}^i = R^i(2), \dots, B_{1, \frac{HL}{2}+1}^i = R^i(\frac{HL}{2}),$$

$$B_{2,HL}^i = R^i(\frac{HL}{2} + 1), B_{2,HL-1}^i = R^i(\frac{HL}{2} + 2), \dots, B_{2, \frac{HL}{2}+1}^i = R^i(HL),$$

$\dots$,

$$B_{WL,HL}^i = R^i(\frac{HL}{2} \times (WL - 1) + 1), B_{WL,HL-1}^i = R^i(\frac{HL}{2} \times (WL - 1) + 2), \dots, B_{WL, \frac{HL}{2}+1}^i = R^i(\frac{HL}{2} \times WL)$$

for $i = 1, 2, \dots, n$,

go to the next block; otherwise, go to Step 7.1.

Step 9: Set $D^i = (B_{1, \frac{HL}{2}}^i, B_{1, \frac{HL}{2}-1}^i, \dots, B_{1,1}^i, B_{2, \frac{HL}{2}}^i, B_{2, \frac{HL}{2}-1}^i, \dots, B_{2,1}^i, \dots, B_{WL, \frac{HL}{2}}^i, B_{WL, \frac{HL}{2}-1}^i, \dots,$

$B_{WL,1}^i)$ for $i = 1, 2, \dots, n$. Utilize $ECC(k_0, n_0)$ to encode bits of message D^i to obtain R^i , for $i = 1, 2, \dots, n$.

Step 10: Output n grayscale shares $SC_1, SC_2, \dots, SC_n$.

Fig. 2. Design idea of the proposed robust secret image sharing algorithm.

- (6) The first block with WL secret pixels is processed separately without screening in Steps 3–4 to output R^i to screen A , thus obtaining satisfactory share pixel values in the next block.
- (7) Because A is randomly selected in Step 7.2, when $N_A \geq 8$, we can search for a value of A that satisfies the equations in Step 8, where N_A denotes the number of available values of A satisfying the equations in Step 8, and $N_A = T \times \prod_{i=1}^n \left(\frac{2^{8-\frac{HL}{2}}}{m_i} \right)$, which will be analyzed

Fig. 3. Idea of the pixel selection order and construction of D^i and R^i .

in Section 4. As a result, the mathematical relation in ECC between bits of the message D^i and check bits R^i , a.k.a. the share bits' relation between adjacent blocks, will be constructed for the i th share for $i = 1, 2, \dots, n$; thus, robustness will be achieved. Robustness in the case of no pixel expansion based on SIS is the significant advantage between the proposed method and other related methods.

- (8) We may apply other SIS principles, such as polynomial, in our scheme, as follows: In Steps 1–2 of Algorithm 1, we can construct a polynomial instead of CRT. The random

coefficients of the constructed polynomial will be screened to satisfy the necessary conditions in Algorithm 1. This will be tested in future work.

- (9) VC is implemented based on probability theory, and generally for a binary secret image, the recovered secret image is naturally lossy with low quality. As a result, our method is not suitable for VC.

Regarding Algorithm 2, we further note the following:

- (1) Algorithm 2 actually contains the steps of Algorithm 1 in the reverse order.
- (2) The secret image is recovered when any k or more shares are provided as input.
- (3) To correct errors in each share block, Steps 3–5 are performed, where Step 4 aims to determine if the bits of the message are properly decoded by examining the number of corrected errors. After error correction, the secret pixel's value is recovered directly in Steps 6–9.
- (4) Steps 7–9 can recover $S(w, h) = x$ with any k or more shared pixels, since T divides the interval $[0, \lfloor \frac{M}{p} - 1 \rfloor]$ into two parts corresponding to $0 \leq x < p$ and $p \leq x \leq 255$ in Step 7 of Algorithm 1. As a result, x can be recovered for arbitrary $x \in [0, 255]$.
- (5) The last block with WL secret pixels is processed separately without error correction in Steps 10–13.

4 PROOF OF PERFORMANCE AND SECURITY ANALYSIS

In this section, we will present a proof of the performance and a security analysis of the designed robust SIS by theoretically analyzing the security and other aspects of performance needed to satisfy the conditions in Definition 3.1.

In what follows, we assume that the secret image is a natural image. Without loss of generality, we denote the grayscale pixel values of the currently collected shares by $sc_{i_1}, sc_{i_2}, \dots, sc_{i_t}$, corresponding to $SC_{i_1}(w, h), SC_{i_2}(w, h), \dots, SC_{i_t}(w, h)$ in the recovery phase.

LEMMA 4.1. *Any $k - 1$ or fewer shares are insufficient for recovering the secret image S .*

PROOF. We assume that y is generated in Step 4.1 of Algorithm 1, where $y \in [0, M - 1]$. When $k - 1$ shares' pixels $a_{i_1} = sc_{i_1}, a_{i_2} = sc_{i_2}, \dots, a_{i_{k-1}} = sc_{i_{k-1}}$ have been collected, according to CRT, we can only obtain the solution y_0 modulo $N_2 = \prod_{j=1}^{k-1} m_{i_j}$, where $y_0 \in [0, N_2 - 1]$. The value range of the true y is different from that of the above y_0 . Additionally, $N_2 < M$, and $\gcd(N_2, p) = 1$; hence, in $[N_2, M - 1]$, $y_0 + b \prod_{j=1}^{k-1} m_{i_j}$ are also solutions to the collected shares' $k - 1$ equations in Equation (2) for $b = 1, 2, \dots, m_{i_k} - 1$. Hence, we have a total of m_{i_k} solutions in $[0, M - 1]$ rather than only one. $\square$

LEMMA 4.2. *Any k or more shares without noise are sufficient for recovering the secret image S losslessly.*

PROOF. Since $x = S(w, h)$ in Step 4 of Algorithm 1, we will prove that any k or more shares' pixels are sufficient for recovering x losslessly. To recover x , we have to obtain y , since $x \equiv y \pmod{p}$ or $x \equiv y \pmod{p} + p$. When we have collected $a_{i_1}, a_{i_2}, \dots, a_{i_k}$, based on CRT, we have a unique solution y modulo $N_1 = \prod_{j=1}^k m_{i_j}$, because $N_1 \geq M$. Finally, we have a unique y and hence x in Step 4 of Algorithm 2. $\square$

LEMMA 4.3. $IQR(SC'_{i_1}, SC'_{i_2}, \dots, SC'_{i_t}) > IQT(SC'_{i_1}, SC'_{i_2}, \dots, SC'_{i_t})$ when $t \geq k$.

PROOF. According to Steps 4–5 in our recovery phase, we can correct at least an average of t_0 bit errors in each block for one share. If there is at least an average of t_0 bit errors in each block for one share, then $IQR(SC'_{i_1}, SC'_{i_2}, \dots, SC'_{i_t}) > IQT(SC'_{i_1}, SC'_{i_2}, \dots, SC'_{i_t})$; otherwise, $IQR(SC'_{i_1}, SC'_{i_2}, \dots, SC'_{i_t}) = IQT(SC'_{i_1}, SC'_{i_2}, \dots, SC'_{i_t})$ according to Step 4 of our recovery algorithm.

ALGORITHM 2: Recovery of the proposed robust secret image sharing for a (k, n) threshold.

Input: Any t grayscale shares $SC'_{i_1}, SC'_{i_2}, \dots, SC'_{i_t}$ ($t = k$), their private integers $m_{i_1}, m_{i_2}, \dots, m_{i_t}, p, T$, $ECC(k_0, n_0, t_0)$ and block size parameters (HL, WL) .

Step 1: Repeat Steps 2–9 until all the secret pixels except for the last WL pixels are processed.

Step 2: Follow the order similar to that shown in Figure 3 to select the uncorrected share pixels to construct the current block. Repeat Steps 3–5 to process the WL uncorrected share pixels in the current block.

Step 3: Set $D^{i'} = (B_{1, \frac{HL}{2}}^i, B_{1, \frac{HL}{2}-1}^i, \dots, B_{1,1}^i, B_{2, \frac{HL}{2}}^i, B_{2, \frac{HL}{2}-1}^i, \dots, B_{2,1}^i, \dots, B_{WL, \frac{HL}{2}}^i, B_{WL, \frac{HL}{2}-1}^i, \dots, B_{WL,1}^i)$ for $i = 1, 2, \dots, n$ in the current block.

In the next block set $R^{i'}(1) = B_{1,HL}^i, R^{i'}(2) = B_{1,HL-1}^i, \dots, R^{i'}(\frac{HL}{2}) = B_{1, \frac{HL}{2}+1}^i,$

$R^{i'}(\frac{HL}{2} + 1) = B_{2,HL}^i, R^{i'}(\frac{HL}{2} + 2) = B_{2,HL-1}^i, \dots, R^{i'}(HL) = B_{2, \frac{HL}{2}+1}^i,$

$\dots,$
 $R^{i'}(\frac{HL}{2} \times (WL - 1) + 1) = B_{WL,HL}^i, R^{i'}(\frac{HL}{2} \times (WL - 1) + 2) = B_{WL,HL-1}^i, \dots, R^{i'}(\frac{HL}{2} \times WL) = B_{WL, \frac{HL}{2}+1}^i$ for $i = 1, 2, \dots, n$.

Step 4: Decode the codeword, i.e., $(D^{i'}, R^{i'})$, to obtain the corrected bits of the message, denoted by $D^{i''}$, and the number of corrected errors. Utilize $ECC(k_0, n_0)$ to encode bits of the message $D^{i''}$ to obtain $R^{i''}$ for $i = 1, 2, \dots, n$.

Determine if the bits of the message have been properly decoded by examining the number of corrected errors. If decoding has failed, then $D^i = D^{i'}$ and $R^i = R^{i'}$; otherwise, $D^i = D^{i''}$ and $R^i = R^{i''}$.

Step 5: $(B_{1, \frac{HL}{2}}^i, B_{1, \frac{HL}{2}-1}^i, \dots, B_{1,1}^i, B_{2, \frac{HL}{2}}^i, B_{2, \frac{HL}{2}-1}^i, \dots, B_{2,1}^i, \dots, B_{WL, \frac{HL}{2}}^i, B_{WL, \frac{HL}{2}-1}^i, \dots, B_{WL,1}^i) = D^i$ for $i = 1, 2, \dots, n$ in the current block.

In the next block set $B_{1,HL}^i = R^i(1), B_{1,HL-1}^i = R^i(2), \dots, B_{1, \frac{HL}{2}+1}^i = R^i(\frac{HL}{2}),$

$B_{2,HL}^i = R^i(\frac{HL}{2} + 1), B_{2,HL-1}^i = R^i(\frac{HL}{2} + 2), \dots, B_{2, \frac{HL}{2}+1}^i = R^i(HL),$

$\dots,$
 $B_{WL,HL}^i = R^i(\frac{HL}{2} \times (WL - 1) + 1), B_{WL,HL-1}^i = R^i(\frac{HL}{2} \times (WL - 1) + 2), \dots, B_{WL, \frac{HL}{2}+1}^i = R^i(\frac{HL}{2} \times WL)$ for $i = 1, 2, \dots, n$.

Step 6: Repeat Steps 7–9 to process the share pixels in the current block one-by-one.

Step 7: For each share pixel position (w, h) , where (w, h) denotes the position in S' of the share pixel currently being processed, repeat Steps 8–9.

Step 8: Set $a_{ij} = SC'_{ij}(w, h)$ for $j = 1, 2, \dots, k$. Solve Equation (2) to obtain y by CRT.

$$\begin{aligned} y &\equiv a_{i1} \pmod{m_{i1}} \\ &\dots \\ y &\equiv a_{ik} \pmod{m_{ik}} \end{aligned} \tag{2}$$

Step 9: Compute $T^* = \lfloor \frac{y}{p} \rfloor$. If $T^* \geq T$, let $x \equiv y \pmod{p}$; otherwise, set $x = y \pmod{p} + p$. Calculate $S'(w, h) = x$.

Step 10: Repeat Steps 11–13 to process the share pixels in the last block one-by-one.

Step 11: For each share pixel position (w, h) , where (w, h) denotes the position in S' of the share pixel currently being processed, repeat Steps 12–13.

Step 12: Let $a_{ij} = SC'_{ij}(w, h)$ for $j = 1, 2, \dots, k$. Solve Equation (2) to obtain y by CRT.

Step 13: Compute $T^* = \lfloor \frac{y}{p} \rfloor$. If $T^* \geq T$, then let $x \equiv y \pmod{p}$; otherwise, set $x = y \pmod{p} + p$. Calculate $S'(w, h) = x$.

Finally, $IQR(SC'_{i_1}, SC'_{i_2}, \dots, SC'_{i_t}) > IQT(SC'_{i_1}, SC'_{i_2}, \dots, SC'_{i_t})$ when $t \geq k$. $\square$

THEOREM 4.4. *Our scheme is a robust SIS scheme.*

PROOF. According to Definition 3.1, the mentioned conditions are satisfied based on the above Lemmas 4.1–4.3. $\square$

PROPOSITION 1: In our Algorithm 1, $N_A = T \times \prod_{i=1}^n \left(\frac{2^{8-\frac{HL}{2}}}{m_i} \right)$.

PROOF. Generally, A has T possible values in Step 7.2 of Algorithm 1. To satisfy the equations in Step 8, $HL/2$ bit planes are fixed, and thus, N_A will decrease to $N_A = T \times \prod_{i=1}^n \left(\frac{2^{8-\frac{HL}{2}}}{m_i} \right)$.

Using a larger N_A will result in stronger security, since the number of brute force attacks is T^{N_A} . $N_A \geq 2$ is required for the lowest security, because if $N_A = 1$, then we have only one integer A that is being repeatedly applied in Step 7.2 of Algorithm 1, which will be insecure. $\square$

In addition, we suggest $N_A \geq 8$ to achieve an acceptable time for searching the available values of A in the generation phase of our SIS, which is obtained from experiments.

5 EXPERIMENTAL RESULTS AND DISCUSSION

A sketch of the experimental setup is given as follows: First, experimental results are presented to illustrate the effectiveness of our robust SIS scheme. Next, parameters of the proposed robust SIS scheme are discussed. Finally, we compare our scheme with related schemes to demonstrate the advantages of our scheme.

The experiments can adopt any parameter settings listed in Table 2, as will be discussed in detail later. In the following tests, we set $p = 131$, and the input original grayscale secret image is of size 120×120 . The extended BCH code is adopted in our experiments.

5.1 Image Illustration

Figure 4 shows the experimental results of the proposed robust SIS scheme for a (k, n) threshold, where $k = 2, n = 2, m_1 = 253, m_2 = 254, HL = 2, WL = 4$, BCH(8,4,1) is adopted, and the original grayscale secret image is presented in Figure 4(a). Figures 4(b)–(c) display our two generated original shares SC_1 and SC_2 , which are of the same size as the original grayscale secret image. Figures 4(d)–(e) demonstrate the two noisy shares SC'_1 and SC'_2 , where we add LSB-changing (bit-flipping) noise with density $r = 0.0083$ to each of SC_1 and SC_2 . Figures 4(f)–(g) show the difference maps between the original shares and the noisy shares, where a given pixel is shown in white when the pixel's grayscale value in SC_i is different from that in SC'_i and in black when the values are the same, for $i = 1, 2$. Figure 4(h) presents the secret image recovered from the two noisy shares based on CRT by the traditional recovery method, as well as its PSNR and SSIM, where the traditional recovery method means direct application of the traditional CRT recovery method to recover the secret image with noisy shares, and $S'_{i'_1 i'_2 \dots i'_t}$ denotes the secret image S' recovered from $SC'_{i_1}, SC'_{i_2}, \dots, SC'_{i_t}$. Figure 4(i) presents the secret image recovered from the two noisy shares by our recovery method and its PSNR and SSIM. According to Figures 4(h)–(i), the secret image recovered by our method is better than that obtained by the traditional method, which indicates that our method is partially robust to LSB-flipping noise.

In what follows, to save space, we only show the first share and the secret image recovered from the first t shares.

Figure 5 illustrates the experimental results of the proposed robust SIS scheme for a (k, n) threshold, where $k = 4, n = 4, m_1 = 251, m_2 = 253, m_3 = 254, m_4 = 255, HL = 8, WL = 4$, BCH(32,16,3) is adopted, and the original grayscale secret image is shown in Figure 5(a). Figure 5(b) displays an

Fig. 4. Experiments with the proposed robust SIS scheme for a (k, n) threshold, where $k = 2, n = 2, m_1 = 253, m_2 = 254, HL = 2, WL = 4$, BCH(8,4,1) is adopted and LSB-changing (bit-flipping) noise with density $r = 0.0083$ is added to SC_1 and SC_2 .

Fig. 5. Experiments with the proposed robust SIS scheme for a (k, n) threshold, where $k = 4, n = 4, m_1 = 251, m_2 = 253, m_3 = 254, m_4 = 255, HL = 8, WL = 4$, BCH(32,16,3) is adopted and salt-and-pepper noise with a density of $r = 0.002$ is added to SC_i , for $i = 1, 2, 3, 4$.

original share SC_1 generated by our method; this share has the same size as the original secret grayscale image. Figure 5(c) demonstrates the noisy share SC'_1 that results from adding salt-and-pepper noise with a density of $r = 0.002$ to SC_1 . Figure 5(d) shows the difference map between the original share and the noisy share. Figures 5(e)–(g) show the secret images recovered from any two or more noisy shares based on CRT by the traditional recovery method and their PSNR and SSIM. Figures 5(h)–(j) present the secret images recovered from any two or more noisy shares by

our recovery method and their PSNR and SSIM. According to Figures 5(e)–(j), the secret image recovered by our method is better than that recovered by the traditional method from the same noisy shares, which indicates that our method is partially robust to salt-and-pepper noise. According to Figures 5(h)–(j), the secret image recovered from all four shares is recognizable, while no clue about the secret image can be obtained when three or fewer shares are leaked, which indicates that our scheme is a valid SIS design for a (k, n) threshold.

The above examples show the following:

- (1) The shares exhibit neither pixel expansion nor cross-interference for a natural secret image.
- (2) When fewer than k shares have been collected, no secret information is leaked, which indicates the security of our robust SIS scheme.
- (3) When any k or more shares have been collected, the secret image can be recovered to some extent.
- (4) The secret image recovered by our method is better than that recovered by the traditional method from the same noisy shares; hence, our method is partially robust to LSB noise, JPEG compression, and salt-and-pepper noise.
- (5) A robust SIS algorithm without pixel expansion for a (k, n) threshold has finally been implemented, where $n \geq k \geq 2$.

The proper reason for the observed robust behavior of the proposed scheme is analyzed as follows: In **Algorithm 1**, the share generation phase of the proposed robust SIS is specially designed to attain an error-correcting capability without increasing the share size. In such a way, in the case of collecting noisy shares, our recovery method is robust to the noise to some degree.

5.2 Available Parameters and Quality Analyses

For the inputs of the proposed **Algorithm 1**, first, we require that $HL \times WL = n_0$ and $\frac{HL}{2} \times WL = k_0$ due to the relation between the message length and codeword length for ECC and the bit plane feature of an image. Second, to generally cover more bit planes of each share pixel in the ECC encoding, when ECC is available, HL is chosen to be as large as possible, with the maximum value of 8. According to Figure 3, when ECC is available, a small WL is suitable for the random noise with a high density experienced by the low bit planes of a share, while a high WL is suitable for the burst noise with a low density experienced by more bit planes of a share. Obviously, a high WL results in higher generation and recovery efficiencies than a low WL due to the latter needing more rounds of ECC encoding and decoding. We will utilize the following two examples to clearly indicate the effects of various values of WL for the same HL , where $k = 3$, $n = 3$, $m_1 = 253$, $m_2 = 254$, $m_3 = 255$, and $HL = 8$.

In the first example, to compare the effects of $WL = 1$ and $WL = 4$, we add the LSB-changing (bit-flipping) noise with the same density of $r = 0.208$ to SC_i for $i = 1, 2, 3$. Figures 6(a)–(e) illustrate the experimental results obtained when $WL = 1$ and BCH(8,4,1) is adopted. Figures 6(f)–(j) illustrate the experimental results obtained when $WL = 4$ and BCH(32,16,3) is adopted. According to Figure 6(e), the secret image is losslessly recovered in the case of collecting all three noisy shares, since $t_0 = 1$ and one bit-flipping error can be corrected for each pixel position when $WL = 1$; hence, our scheme for the $(3, 3)$ threshold is fully robust to LSB-changing (bit-flipping) noise when $WL = 1$ and BCH(8,4,1) is adopted. According to Figures 6(e) and (j), the quality of the secret image recovered when $WL = 1$ is better than that when $WL = 4$, since $t_0 = 3$ and three bit-flipping errors can be corrected for each block with 4 pixels when $WL = 4$. In other words, if there are 4 bit-flipping errors at some 4-pixel positions in one block, then the decoding fails.

Fig. 6. Experiments with the proposed robust SIS scheme for a (k, n) threshold performed to show the effects of various values of WL , where $k = 3, n = 3, m_1 = 253, m_2 = 254, m_3 = 255, HL = 8$, and LSB-changing (bit-flipping) noise with density $r = 0.208$ is added to SC_i for $i = 1, 2, 3$.

Fig. 7. Experiments with the proposed robust SIS scheme for a (k, n) threshold performed to show the effects of various values of WL , where $k = 3, n = 3, m_1 = 253, m_2 = 254, m_3 = 255, HL = 8$, and JPEG compression with the same quality of 100 is performed on SC_i for $i = 1, 2, 3$.

Finally, when ECC is available, a small WL is more suitable than a large WL under the condition of random noise with a high density being experienced by the low bit planes of shares.

In the next example, to compare the effects of $WL = 1$ and $WL = 4$, we perform JPEG compression on SC_i for $i = 1, 2, 3$, with the same quality of the JPEG-compressed file of 100. Figures 7(a)–(e) illustrate the experimental results obtained when $WL = 1$ and BCH(8,4,1) is adopted.

Table 2. Available Parameters $p, m_1, m_2, \dots, m_n, HL$, and WL

(k, n)	p	$m_1, m_2, \dots, m_n$	HL, WL	$ECC(k_0, n_0, t_0)$
(2,2)	131	253,254	2,4	(8,4,1)
(2,2)	128	253,255	2,4	(8,4,1)
(2,3)	131	253,254,255	2,4	(8,4,1)
(2,3)	128	251,253,255	2,4	(8,4,1)
(3,3)	131	253,254,255	8,4/4,8;2,4/8,1	(32,16,3);(8,4,1)
(3,3)	128	251,253,255	8,4/4,8;2,4/8,1	(32,16,3);(8,4,1)
(3,4)	131	251,253,254,255	4,8/2,4	(32,16,3)/(8,4,1)
(3,4)	128	247,251,253,255	4,8/2,4	(32,16,3)/(8,4,1)
(4,4)	131	251,253,254,255	8,4/4,8;2,4/8,1	(32,16,3);(8,4,1)
(4,4)	128	247,251,253,255	8,4/4,8;2,4/8,1	(32,16,3);(8,4,1)

Figures 7(f)–(j) illustrate the experimental results obtained when $WL = 4$ and BCH(32,16,3) is adopted. According to Figures 7(e) and (j), the image quality of the secret image recovered when $WL = 4$ is better than that obtained when $WL = 1$, since $t_0 = 1$, one bit-flipping error can be corrected for every one-pixel position when $WL = 1$, and JPEG compression may lead to more than one bit-flipping error in each block. Finally, when ECC is available, a large WL is more suitable than a small WL under the condition of burst noise with a low density being experienced by more bit planes of shares.

In addition to parameters HL and WL , in step 1 of the proposed **Algorithm 1**, we select a set of integers $\{128 \leq p < m_1 < m_2 < \dots < m_n \leq 256\}$ that satisfy three equations, aiming to achieve CRT-based SIS for a (k, n) threshold. The condition $\{128 \leq p < m_1 < m_2 < \dots < m_n \leq 256\}$ is required because of the image pixel value range and $pN < M$. In our **Algorithm 1**, to achieve a random distribution of the share pixel values over a large range to improve security, m_i should be as large as possible, and p should be as small as possible for security of the secret image recovery while ensuring that the secret pixel values can be divided into two intervals. Due to image pixel values being in the range of $[0, 255]$, we can choose $p = 128$; moreover, in cryptography, a prime number in general has significance; thus, we can also select $p = 131$, which is the smallest prime number greater than 128.

Considering the above analysis, we list several available parameters $p, m_1, m_2, \dots, m_n, HL$, and WL for a (k, n) threshold in Table 2. The user can further select other suitable parameters in addition to the available parameters in Table 2 according to the specific applications.

5.3 Robustness Analyses

To test the robustness of the proposed algorithm, when the type of noise added to the share is fixed, the noise density plays an important role in the quality of the recovered secret image and thus our robustness. Therefore, herein, we intend to study the robustness of the proposed algorithm to certain types of noise as the noise density changes. The parameters are set to $k = 3, n = 3, m_1 = 253, m_2 = 254, m_3 = 255, HL = 8$, and $WL = 4$; BCH(32,16,3) is adopted, and the same secret image of Lena is used as in the above experiments. 100 corresponds to lossless recovery and a better visual appearance, and the result based on CRT obtained by the traditional recovery method is shown as well.

Figure 8 shows the curves of the quality evaluation metrics versus noise density for the recovered secret image in the scenario of LSB-flipping noise being added to all three shares. The figure demonstrates the following:

Fig. 8. PSNR and SSIM curves of secret images recovered by the traditional method and our method when LSB-flipping noise is added to all three shares.

Fig. 9. PSNR and SSIM curves of secret images recovered by the traditional method and our method when compression noise is added to all three shares.

- (1) When $0 \leq \text{density} \leq 0.07$, the PSNR of our method is close to 100, and the SSIM is close to 1, i.e., the secret image is recovered losslessly, and our robust SIS scheme is fully robust to LSB-flipping noise; deviations from perfect results are caused by noise randomness.
- (2) When $\text{density} > 0.07$, both the PSNR and SSIM of our method are nearly monotonically decreasing functions of density, and our robust SIS scheme is partially robust to LSB-flipping noise.
- (3) Both the PSNR and SSIM of the traditional method are monotonically decreasing functions of density.
- (4) Highest robustness is analyzed from two perspectives: (1) the highest quality of the recovered secret image in the case of lossy shares; and (2) the highest improved rate of the quality compared with the traditional method. The highest quality of the recovered secret image in the case of lossy shares is lossless, i.e., PSNR=100, SSIM=1 when $\text{density} = 0.05$. Compared with the traditional method, our highest improved rate of the quality is 624.39% for PSNR when $\text{density} = 0.083$ or 946.74% for SSIM when $\text{density} = 0.208$.
- (5) The quality of the secret image recovered by our method exceeds that by the traditional method in the case of collecting shares affected by LSB-flipping noise.

Figure 9 shows the curves of the quality evaluation metrics versus the quality of JPEG compression used in the creation of shares from which the secret image was recovered. The figure demonstrates the following:

Fig. 10. PSNR and SSIM curves of secret images recovered by the traditional method and our method when salt-and-pepper noise is added to all three shares.

- (1) When the quality of JPEG compression is less than 97, both the PSNR and SSIM of our method and the traditional method are very low, because neither our method nor the traditional method are robust to JPEG compression noise of high density.
- (2) When the quality of JPEG compression is equal to or greater than 97, both the PSNR and SSIM of our method and the traditional method are monotonically increasing functions of JPEG compression quality. The quality of the secret image recovered by our method is higher than that of the traditional method; thus, our robust SIS scheme is partially robust to JPEG compression noise.
- (3) The highest quality of the recovered secret image in the case of lossy shares is PSNR=19.45, SSIM=0.5767 when the quality of JPEG compression is 100. Compared with the traditional method, our highest improved rate of the quality is 43.02% for PSNR when the quality of JPEG compression is 100 or 178.39% for SSIM when the quality of JPEG compression is 99.
- (4) The quality of the secret image recovered by our method surpasses that of the traditional method in the case of collecting shares affected by JPEG compression noise when high-quality JPEG compression is used.

Figure 10 shows the curves of the quality evaluation metrics versus noise density for the recovered secret image when salt-and-pepper noise is added to all three shares. The figure shows the following:

- (1) Both the PSNR and SSIM of our method and the traditional method are monotonically decreasing functions of density. The quality of secret images recovered by our method is higher than that of the traditional method; thus, our robust SIS scheme is partially robust to salt-and-pepper noise.
- (2) The highest quality of the recovered secret image in the case of lossy shares is lossless, i.e., PSNR=100, SSIM=1 when $density = 0.0001$. Compared with the traditional method, our highest improved rate of the quality is 90.05% for PSNR when $density = 0.0001$ or 6.82% for SSIM when $density = 0.0017$.
- (3) The quality of secret images recovered by our method surpasses that of the traditional method in the case of collecting shares affected by salt-and-pepper noise.

The proper reason for the observed above robust behavior of the proposed scheme is analyzed as follows: When a small amount of noise less than the error-correcting capability is added, our scheme can fully correct it. When a large amount of noise is added, our scheme can partially correct it. Some unusual points are caused by randomness.

Fig. 11. Experimental comparisons of the scheme of Yan et al. and the proposed robust SIS method for a (k, n) threshold, where $k = 2, n = 2, m_1 = 253, m_2 = 255, HL = 2, WL = 4$, and LSB-changing (bit-flipping) noise with density $r = 0.042$ is added to SC_i for $i = 1, 2$.

In summary, our algorithm is to some degree robust to some noise types, including at least LSB-flipping noise, JPEG compression, and salt-and-pepper noise of a certain density.

5.4 Comparisons with Related Schemes

We compare our robust SIS approach with the schemes of Yan et al. [31] and Li et al. [12], using the same secret image as in Figure 11(a), with $p = 131$ and the CRT recovery of Yan et al. and Li et al. The schemes are chosen for comparison, because the researchers' SIS method performs lossless recovery without pixel expansion based on CRT for a (k, n) threshold.

Yan et al. proposed a two-in-one SIS method in which a grayscale secret image was encoded by CRT in the generation phase. The grayscale secret image can be losslessly recovered by solving a set of linear congruence equations with only modular operations. We use the same parameters as in the illustration of Yan et al. to perform the comparisons shown in Figure 11, where $k = 2, n = 2$, the grayscale secret image shown in Figure 11(a) is of size 120×120 , and LSB-changing (bit-flipping) noise with density $r = 0.042$ is added to SC_i for $i = 1, 2$. Figures 11(a)–(e) illustrate the experimental results of the scheme of Yan et al. Figures 11(f)–(j) illustrate the experimental results of our method when $HL = 2, WL = 4$, and BCH(8,4,1) is adopted. According to Figure 11(e), the secret image is not recovered losslessly in the case of collecting both noisy shares in the scheme of Yan et al., since the researchers' method is not robust. According to Figures 11(e) and (j), the image quality of the secret image recovered by our scheme is better than that of the scheme of Yan et al., which shows that our scheme is robust to LSB-changing (bit-flipping) noise. Finally, our scheme is more robust than the scheme of Yan et al.

Li et al. proposed a (k, n) threshold SIS based on CRT by encoding the high 7 bits of the secret pixel and embedding LSB into a random integer. The grayscale secret image can be losslessly recovered by solving a set of linear congruence equations with only modular operations as well. We use the same parameters as in the illustration of Li et al. to perform the comparisons shown in Figure 12, where $k = 3, n = 3$, the grayscale secret image shown in Figure 12(a) is of size 120×120 , and salt-and-pepper noise with a density of $r = 0.001$ is added to SC_i for $i = 1, 2, 3$. Figures 12(a)–(e)

Fig. 12. Experimental comparisons of the scheme of Li et al. and the proposed robust SIS method for a (k, n) threshold, where $k = 3, n = 3, m_1 = 253, m_2 = 254, m_2 = 255, HL = 8, WL = 4$, and salt-and-pepper noise with a density of $r = 0.001$ is added to SC_i for $i = 1, 2, 3$.

illustrate the experimental results of the scheme of Li et al. Figures 12(f)–(j) illustrate the experimental results of our method when $HL = 8, WL = 4$, and BCH(32,16,3) is adopted. According to Figure 12(e), the secret image is not recovered losslessly in the case of collecting both noisy shares in the scheme of Li et al., since the researchers' method is not robust. According to Figures 12(e) and (j), the image quality of the secret image recovered by our scheme is better than that of the scheme of Li et al., which shows that our scheme is robust to salt-and-pepper noise. Finally, our scheme is more robust than the scheme of Li et al. as well as the traditional SIS methods, including polynomial-based SIS and CRT-based SIS.

6 CONCLUSIONS

In this article, we have introduced a formal definition of robust SIS and subsequently proposed a robust SIS algorithm for a (k, n) threshold that utilizes the principle of CRTSIS to achieve the features of no pixel expansion, low complexity of recovery, and robustness to some types of noise, such as least significant bit noise, JPEG compression, and salt-and-pepper noise, to some degree. Our SIS method is even fully robust to some noise of a certain density. The experimental results have proven the effectiveness of the proposed algorithm. Analyses of the available parameters and quality have been presented as well. We have performed experimental comparisons with related schemes to demonstrate the advantages of our algorithm. In our future research, we will study the following topics: First, we will theoretically analyze and test the optical image quality factors HL , WL , and N_A to balance security and image quality. Second, we will improve our method's robustness against more types of noises. Third, we will apply polynomial-based SIS in our scheme.

ACKNOWLEDGMENTS

The authors would like to thank the anonymous reviewers for their valuable comments.

REFERENCES

- [1] C. Asmuth and J. Bloom. 1983. A modular approach to key safeguarding. *IEEE Trans. Inf. Theor.* 29, 2 (1983), 208–210.
- [2] L. Bao, S. Yi, and Y. Zhou. 2017. Combination of sharing matrix and image encryption for lossless (k, n) —Secret image sharing. *IEEE Trans. Image Proc.* 26, 12 (Dec. 2017), 5618–5631. DOI : <https://doi.org/10.1109/TIP.2017.2738561>
- [3] Akram Belazi and Ahmed A. Abd El-Latif. 2017. A simple yet efficient S-box method based on chaotic sine map. *Optik - Int. J. Light Electron Optics* 130 (2017), 1438–1444.
- [4] Z. Chen, X. Hou, X. Qian, and C. Gong. 2018. Efficient and robust image coding and transmission based on scrambled block compressive sensing. *IEEE Trans. Multimedia* 20, 7 (July 2018), 1610–1621. DOI : <https://doi.org/10.1109/TMM.2017.2774004>
- [5] Yuciao Cheng, Zhengxin Fu, and Bin Yu. 2018. Improved visual secret sharing scheme for QR code applications. *IEEE Trans. Inf. Forens. Secur.* 13, 9 (2018), 2393–2403.
- [6] Ting Wei Chuang, Chaur Chin Chen, and Betty Chien. 2016. Image sharing and recovering based on Chinese remainder theorem. In *International Symposium on Computer, Consumer and Control*. 817–820.
- [7] Hu Chunqiang, Liao Xiaofeng, and Xiao Di. 2012. Secret image sharing based on chaotic map and Chinese remainder theorem. *Int. J. Wavel. Multires. Inf. Proc.* 10, 3 (2012), 1250023 (2012).
- [8] Ronald Cramer, Ivan Bjerre Damgård, Nico Döttling, Serge Fehr, and Gabriele Spini. 2015. Linear secret sharing schemes from error correcting codes and universal hash functions. In *Advances in Cryptology - EUROCRYPT 2015*, Elisabeth Oswald and Marc Fischlin (Eds.). Springer Berlin, 313–336.
- [9] Mohammad Ghebleh and Ali Kalso. 2018. A novel secret image sharing scheme using large primes. *Multimedia Tools Applic.* 77, 10 (01 May 2018), 11903–11923. DOI : <https://doi.org/10.1007/s11042-017-4841-4>
- [10] Xingxing Jia, Daoshun Wang, Qimeng Chu, and Zhenhua Chen. 2019. An efficient XOR-based verifiable visual cryptographic scheme. *Multimedia Tools Applic.* 78, 7 (01 Apr. 2019), 8207–8223. DOI : <https://doi.org/10.1007/s11042-018-6779-6>
- [11] Ilan Komargodski and Anat Paskin-Cherniavsky. 2017. Evolving secret sharing: Dynamic thresholds and robustness. In *Theory of Cryptography*, Yael Kalai and Leonid Reyzin (Eds.). Springer International Publishing, Cham, 379–393.
- [12] L. Li, Y. Lu, X. Yan, L. Liu, and L. Tan. 2019. Lossless (k, n) —Threshold image secret sharing based on the Chinese remainder theorem without auxiliary encryption. *IEEE Access* 7 (2019), 75113–75121. DOI : <https://doi.org/10.1109/ACCESS.2019.2921612>
- [13] Y. Li, Z. Lu, C. Zhu, and X. Niu. 2012. Robust image hashing based on random Gabor filtering and dithered lattice vector quantization. *IEEE Trans. Image Proc.* 21, 4 (Apr. 2012), 1963–1980. DOI : <https://doi.org/10.1109/TIP.2011.2171698>
- [14] Feng Liu and Chuankun Wu. 2011. Embedded extended visual cryptography schemes. *IEEE Trans. Inf. Forens. Secur.* 6, 2 (2011), 307–322.
- [15] Xiaobei Liu, Soo Ngee Koh, Xin Wen Wu, and Chee Cheon Chui. 2012. Reconstructing a linear scrambler with improved detection capability and in the presence of noise. *IEEE Trans. Inf. Forens. Secur.* 7, 1 (2012), 208–218.
- [16] Yanxiao Liu, Chingnung Yang, Yichuan Wang, Lei Zhu, and Wenjiang Ji. 2018. Cheating identifiable secret sharing scheme using symmetric bivariate polynomial. *Inf. Sci.* 453 (2018), 21–29.
- [17] Moni Naor and Adi Shamir. 1995. Visual cryptography. In *Advances in Cryptology-EUROCRYPT'94 Lecture Notes in Computer Science, Workshop on the Theory and Application of Cryptographic Techniques*. Springer, 1–12.
- [18] Z. Qian, X. Zhang, and S. Wang. 2014. Reversible data hiding in encrypted JPEG bitstream. *IEEE Trans. Multimedia* 16, 5 (Aug. 2014), 1486–1491. DOI : <https://doi.org/10.1109/TMM.2014.2316154>
- [19] V. Rishiwal, M. Yadav, and K. V. Arya. 2008. A robust secret image sharing scheme. In *1st International Conference on Emerging Trends in Engineering and Technology*. 11–14. DOI : <https://doi.org/10.1109/ICETET.2008.109>
- [20] Adi Shamir. 1979. How to share a secret. *Commun. ACM* 22, 11 (1979), 612–613.
- [21] K. Shankar and P. Eswaran. 2016. A new k out of n secret image sharing scheme in visual cryptography. In *10th International Conference on Intelligent Systems and Control (ISCO'16)*. 1–6. DOI : <https://doi.org/10.1109/ISCO.2016.7726969>
- [22] Shyong Jian Shyu and Ying Ru Chen. 2008. Threshold secret image sharing by Chinese remainder theorem. In *IEEE Asia-Pacific Services Computing Conference*. 1332–1337.
- [23] Chih-Ching Thien and Ja-Chen Lin. 2002. Secret image sharing. *Comput. Graph.* 26, 5 (2002), 765–770.
- [24] M. Ulutas, V. V. Nabiyeve, and G. Ulutas. 2009. A new secret image sharing technique based on Asmuth Bloom's scheme. In *International Conference on Application of Information and Communication Technologies (AICT'09)*. 1–5.
- [25] Guangyu Wang, Feng Liu, and Wei Qi Yan. 2016. Basic visual cryptography using braille. *Int. J. Digit. Crime Forens.* 8, 3 (2016), 85–93.
- [26] Ping Wang, Xing He, Yushu Zhang, Wenying Wen, and Ming Li. 2019. A robust and secure image sharing scheme with personal identity information embedded. *Comput. Secur.* 85 (2019), 107–121. DOI : <https://doi.org/10.1016/j.cose.2019.04.010>
- [27] Zhongmin Wang, Gonzalo R. Arce, and Giovanni Di Crescenzo. 2009. Halftone visual cryptography via error diffusion. *IEEE Trans. Inf. Forens. Secur.* 4, 3 (2009), 383–396.

- [28] Zhou Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli. 2004. Image quality assessment: From error visibility to structural similarity. *IEEE Trans. Image Proc.* 13, 4 (Apr. 2004), 600–612. DOI : <https://doi.org/10.1109/TIP.2003.819861>
- [29] Jonathan Weir, Weiqi Yan, and Mohan S. Kankanalli. 2012. Image hatching for visual cryptography. *ACM Trans. Multimedia Comput. Commun. Appl.* 8, 2S (Sept. 2012). DOI : <https://doi.org/10.1145/2344436.2344438>
- [30] Weiqi Yan, Wei Ding, and Qi Dongxu. 2000. Image sharing based on Chinese remainder theorem. *J. North China Univ. of Tech* 12, 1 (2000), 6–9.
- [31] Xuehu Yan, Yuliang Lu, Lintao Liu, Jingju Liu, and Guozheng Yang. 2018. Chinese remainder theorem-based two-in-one image secret sharing with three decoding options. *Digit. Sig. Proc.* 82 (2018), 80–90. DOI : <https://doi.org/10.1016/j.dsp.2018.07.015>
- [32] Xuehu Yan, Yuliang Lu, Lintao Liu, and Xianhua Song. 2020. Reversible image secret sharing. *IEEE Trans. Inf. Forens. Secur.* 15 (2020), 3848–3858. DOI : <https://doi.org/doi: 10.1109/TIFS.2020.3001735>
- [33] Xuehu Yan, Yuliang Lu, Lintao Liu, Song Wan, Wanmeng Ding, and Hanlin Liu. 2017. Chinese remainder theorem-based secret image sharing for (k, n) threshold. *Third International Conference of Cloud Computing and Security (ICCCS'17)* 433–440. DOI : https://doi.org/10.1007/978-3-319-68542-7_36
- [34] C. Yang, C. Wu, and Y. Lin. 2019. k out of n region-based progressive visual cryptography. *IEEE Trans. Circ. Syst. Vid. Technol.* 29, 1 (Jan. 2019), 252–262. DOI : <https://doi.org/10.1109/TCSVT.2017.2771255>
- [35] Ching-Nung Yang and Chuei-Bang Ciou. 2010. Image secret sharing method with two-decoding-options: Lossless recovery and previewing capability. *Image Vis. Comput.* 28, 12 (2010), 1600–1610.
- [36] X. Zhang, F. Peng, and M. Long. 2018. Robust coverless image steganography based on DCT and LDA topic classification. *IEEE Trans. Multimedia* 20, 12 (Dec. 2018), 3223–3238. DOI : <https://doi.org/10.1109/TMM.2018.2838334>
- [37] Zhi Zhou, Gonzalo R. Arce, and Giovanni Di Crescenzo. 2006. Halftone visual cryptography. *IEEE Trans. Image Proc.* 15, 8 (2006), 2441–2453.
- [38] Zhili Zhou, Yan Mu, and Q. M. Jonathan Wu. 2019. Coverless image steganography using partial-duplicate image retrieval. *Soft Comput.* 23 (2019), 4927–4938.
- [39] Zhili Zhou, Q. M. Jonathan Wu, Yimin Yang, and Xingming Sun. 2020. Region-level visual consistency verification for large-scale partial-duplicate image search. *ACM Trans. Multimedia Comput., Commun., Applic.* 16, 2 (2020).
- [40] Z. Zhou, C. Yang, Y. Cao, and X. Sun. 2018. Secret image sharing based on encrypted pixels. *IEEE Access* 6 (2018), 15021–15025. DOI : <https://doi.org/10.1109/ACCESS.2018.2811722>

Received January 2020; revised June 2020; accepted August 2020