# A Secret Image Sharing with Deep-steganography and Two-stage Authentication Based on Matrix Encoding

Li Liu[1], Anhong Wang[1], Chin-Chen Chang[2] and Zhihong Li[1]

*(Corresponding author: Anhong Wang, Chin-Chen Chang)*

College of Electronic Information and Engineering, Taiyuan University of Science and Technology[1]
No. 66, Waliu Rd., Taiyuan, China
Department of Information Engineering and Computer Science, Feng Chia University[2]
No. 100, Wenhwa Rd., Seatwen, Taichung, Taiwan
(Email: wah_ty@163.com, alan3c@gmail.com)

*(Received Mar. 26, 2016; revised and accepted May 10 & June 5, 2016)*

## Abstract

A secret image sharing with deep-steganography and two-stage authentication based on matrix encoding is proposed. This scheme firstly employed Wang and Su's sharing scheme to share a secret image into $n$ shadows. Then, $n$ shadows were embedded into the pre-selected cover images by using matrix encoding so as to generate $n$ stego images. Different from the common schemes which directly use LSBs replacement, our scheme performs deep-steganography, which hides 3-bit secret data but only modifies at most 1-bit via matrix encoding. Benefiting from the comparatively slight modification to the cover image, our scheme obtains enhancement in both the security of secret data and the visual quality of the stego image. As far as the authentication ability is concerned, our scheme explores a two-stage authentication: the first uses a sub-key to pass identity authentication, and the second performs tamper authentication. The experimental results show that our scheme achieves better authentication ability than the referenced schemes.

*Keywords: Deep-steganography, matrix encoding, secret sharing, two-stage authentication*

## 1 Introduction

With the rapid development and wide application of Internet, information hiding technology has come to play an important role in the field of information security. As a new information hiding technology, steganography hides the secret information into the cover image and generates a stego image [15]. Since the secret information is invisible in the stego image, this ensures that any third party (i.e., aside from the communication parties) is not aware of the existence of secret information.

Compared with traditional encryption, steganography provides a new solution to avoid any suspicion of attackers when the data is transmitted. Many steganographic methods [1, 3, 9, 11, 19] have been proposed to produce meaningful stego image which hides secret information. However, this stego image is usually held by only one person without extra copies. Thus, if the stego image is lost accidentally or modified intentionally, the secret information will be destroyed. Hence, it is necessary to share certain secret information among several people [5]. The concept of $(k, n)$-threshold secret sharing proposed by Shamir [14] can solve this problem. This sharing scheme divides a secret message into $n$ shadows. The secret can be restored if $k(k \leq n)$ of the $n$ shadows are obtained, but any $k-1$ or fewer of them will obtain no information about the secret image.

In 1995, Naor and Shamir [13] introduced this sharing idea into image field, and later Thien and Lin [17] used this idea to generate $n$ noise-like images (so called 'shadows') with size $1/k$ of the secret image. Because smaller shadows were needed for easy transmission, storage and hiding, Wang and Su [18] proposed an improved scheme using Huffman coding to compress the difference image of the secret image, with each generated shadow image being about 40% smaller than that of the method in [17]. However, these noise-like images tended to make attacker suspicious.

In order to further improve the security of secret image, steganography based on secret image sharing schemes [2, 6, 12, 16, 20, 21] have been proposed to hide the noise-like shadows inside pre-selected meaningful images (called 'cover images'), and consequently generate the meaningful stego images to represent shadows so that no one can detect the existence of the secret information. Here, the challenge is to create high-quality stego im-

ages so that the modifications are not visually perceptible. Moreover, it will be useful to check in advance the fidelity of all stego images before they are used to reconstruct the secret images. Since fake stego images that were accidentally or intentionally submitted by the participant will lead to unsuccessful secret reconstruction. The scheme of steganography and authentication based on secret image sharing was firstly proposed by Lin and Tsai [12] in 2004. However, this scheme has a lossy reconstructed secret image and a weak authentication mechanism. Afterwards, Yang et al. proposed a scheme [20] that overcomes the weakness of that proposed by Lin et al. and enhances the authentication to some degree. However, this scheme reduces the visual quality of the stego images because the lowest 4-bit of the pixel value in each block is modified.

In Chang et al.'s scheme [2], the Chinese remainder theorem (CRT) is used to generate four authentication bits in order to obtain better authentication ability. Meanwhile, they claimed that their scheme enhances the visual quality of stego images. In [6], the concept of linear cellular automata was employed instead of Shamir's $(k, n)$ threshold image sharing scheme, and this scheme not only obtains better visual quality but also improves the ability of tamper detection. Nevertheless, this scheme needs to offer at least $k$ consecutive shadows to reveal the secret image, and cannot accurately locate the tampered blocks.

In all of the aforementioned schemes, the cover images are first divided into fixed-size blocks (of size 2×2) and then the pixels of shadows are hidden orderly into the LSBs of each block. Note that there are two problems.

Firstly, it is possible that only a part of a cover image will be used to hide secret data, so the statistical property of stego images shows a great difference between the two parts of non-embedded and embedded data; secondly, the RS steganalysis [8, 10] can easily detect the existence of secret data that has been embedded by LSBs and can predict its length. Hence, if an attacker wanted to steal the embedding positions of secret data, he could obtain the secret data easily. In this paper, we propose a deep-steganography method using matrix encoding. Firstly, Wang and Su's sharing scheme was employed to share secret image into $n$ shadows.

Secondly, $n$ shadows were embedded into the preselected cover images by using matrix encoding to generate the $n$ stego images. Note that, in order to reduce the change in the statistical property of cover images, the full capacity of the cover images was used to realize the process of randomly embedded data. Since secret data does not directly appear in the pixels of the cover image, we call it 'deep-steganography'. Benefiting from the comparatively slight modification to the cover image, our scheme obtains enhancement in both the security of secret data and the visual quality of stego image. Furthermore, the authentication ability of our scheme can be well expressed by using two-stage authentication.

# 2 Related Works

## 2.1 Wang and Su's Image Sharing Scheme

Wang and Su [18] used a Huffman coding for a $(k, n)$-threshold secret image sharing scheme in order to generate smaller shadows and reconstruct the secret image completely.

The difference image DIFF=$\{diff_{ij}\}$ is calculated using Equation (1) and then encoded using the Huffman coding scheme.

$$diff_{ij} = \begin{cases} se_{ij}, & if \;\; i = 0 \;\; and \;\; j = 0 \\ se_{ij} - se_{(i-1)j}, & if \;\; i \neq 0 \;\; and \;\; j = 0 \\ se_{ij} - se_{i(j-1)}, & otherwise \end{cases} \quad (1)$$

where $se_{ij}$ is the pixel value of the original secret image (sized $m \times n$) in the $i$-th row and $j$-th column, $1 \leq i \leq m, 1 \leq j \leq n$. Every $t$ bits that obtained from the Huffman output stream are converted into the decimal sharing coefficient $(a_0, a_1, \ldots, a_{k-1})$, and every $k$ coefficients are used to generate the $(k-1)$ degree polynomial sharing function.

$$f_l(x) = (a_0 + a_1 x + a_2 x^2 + \cdots + a_{k-1} x^{k-1}) \mod 2^t. \quad (2)$$

Each shadow $S_i$ can be derived as

$$S_1 = f_l(1), \ldots, S_i = f_l(i), \ldots, S_n = f_l(n). \quad (3)$$

where the number of $l$ depends on the number of decimal sharing coefficients. Obviously, if fewer than $k$ shadows are received, the original secret image cannot be revealed.

In the revealing phase, the sharing coefficients $a_0, a_1, \ldots, a_{k-1}$ of $f_l(x)$ can be calculated using Lagrange's interpolation when giving any $k$ of $n$ shadows, and then all of the sharing coefficients are transformed into binary bit stream. This bit stream was decoded by using the Huffman codes table to reveal the difference image, and then the inverse-differencing process was used to reveal the whole secret image.

## 2.2 Matrix Encoding

Matrix encoding, which was introduced by Crandall [4], reduces the number of changes required and improves the embedding efficiency to a great extent in comparison with the classic LSB replacement methods. Assume the embedding cell is expressed in the form of vector $m = \{m_1, m_2, \ldots, m_q\}$ with the length of $q$. The coding implemented on each embedding cell is denoted by an ordered triple $(d_{max}, q, t)$, where $q$ is the number of modifiable bit positions in an embedding cell, and $t$ is the bit length of secret information $s = \{s_1, s_2, \ldots, s_t\}$. Usually, we set $d_{max} = 1$, namely, an embedding cell with $q$ positions will be changed in no more than $d_{max}$ positions to embed $t$ bits of secret information [7].

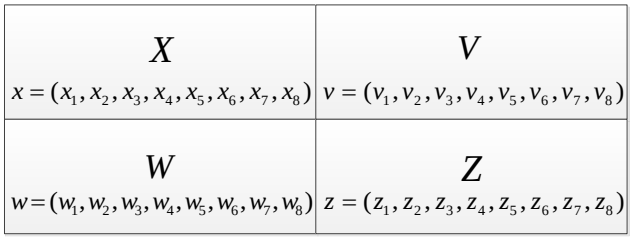


Figure 1: Structure of the four-pixel block in the cover image

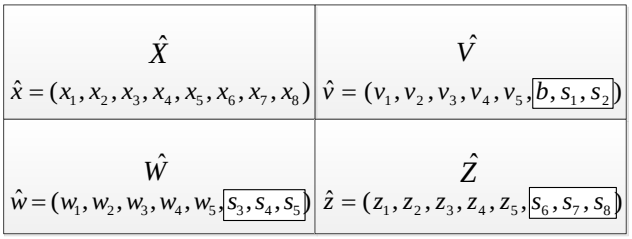


Figure 2: Block structure of the stego image in Lin and Tsai's scheme

A hash function $f(\cdot)$ is defined as Equation (4) to map $q$ bits embedding cell $m$ into $t$ bits binary string.

$$f(m) = \bigoplus_{i=1}^{q} m_i \cdot i. \tag{4}$$

Subsequently, XOR operation is implemented on the value of the hash function and secret information $s$ to find the position $P$ of the changes required.

$$P = s \oplus f(m). \tag{5}$$

Finally, an embedded stego data $m'$ is generated by the following rule:

$$m' = \begin{cases} m, & P = 0 \\ m_1, \cdots, \bar{m}_i, \cdots, m_q & P = i \end{cases}, \tag{6}$$

where $\bar{m}_i$ is the negation of $m_i$. In the secret extraction phase, the receiver would retrieve the secret information $s$ by directly putting the stego data $m'$ into the same hash function, i.e., $s = f(m')$.

## 2.3 Review of Existing Schemes

The scheme of the steganography and authentication based on secret image sharing was first proposed by Lin and Tsai [12] in 2004 as follows. Firstly, select $n$ meaningful images as the cover images and divide them into non-overlapping 4-pixel blocks. Secondly, use each pixel of the secret image as sharing coefficient $a_0$ and choose $(k-1)$ random numbers as sharing coefficients $a_1, a_2, \ldots, a_{k-1}$ in Equation (2) to generate $n$ shadows. Note that there is modulo 251 in this scheme instead of modulo $2^t$ and the top-left pixel value $x$ of each cover image block in Figure 1 is used as the value in Equation (2) for computing all of the shared pixels $f(x)$. Thirdly, convert each shared pixel into a binary representation $s_1, s_2, \ldots, s_8$, and meanwhile, one parity bit $b$ is generated as an authentication bit by the secret key $K$. Finally, embed the nine bits $(s_1, s_2, \ldots, s_8, b)$ into the cover image block as in Figure 2 to form the stego-block. However, the calculation of modulo 251 damages the quality of the reconstructed secret image, and the authentication ability of 1 bit is very weak.

Later, Yang et al.'s scheme [20] overcame the weakness of Lin and Tsai's scheme. The main improvements were as follows: (1) The modulus value is set to $2^8$, so there is no loss of data when the secret image is reconstructed; and (2) One authentication bit $b$, which is calculated by a hash function, offers higher authentication ability than that of Lin and Tsai's scheme. The embedding strategy of this scheme is shown in Figure 3. However, because the bits $x_7, x_8$ of pixel $X$ need to be recorded in the pixel $W$ as shown in Figure 3, the visual quality of the stego images may be greatly reduced.

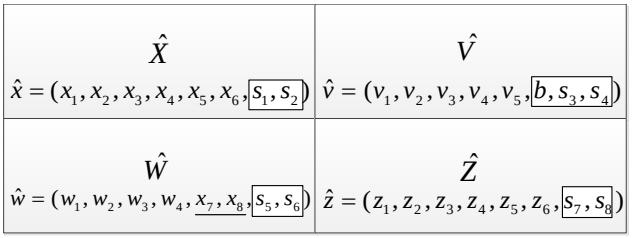


Figure 3: Block structure of the stego image in Yang et al.'s scheme

Chang et al.'s scheme [2] has better stego image quality and authentication ability than previous schemes. This scheme uses $k$ consecutive pixels of the secret image as sharing coefficients $a_0, a_1, \ldots, a_{k-1}$ in Equation (2) to generate smaller shadows, so the visual quality of the stego image is clearly improved. Meanwhile, the use of four authentication bits $(b_1, b_2, b_3, b_4)$ in each stego-block, which is calculated by CRT, also decrease the possibility of successful tampering. The embedding strategy of this scheme is shown in Figure 4.

Different from the above mentioned three schemes, Es-

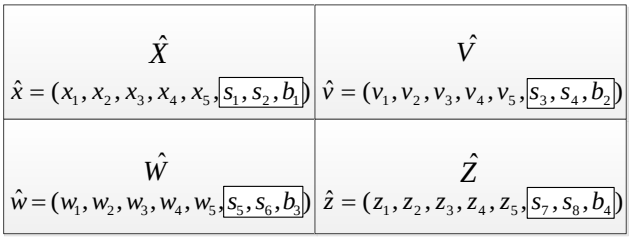


Figure 4: Block structure of the stego image in Chang et al.'s scheme

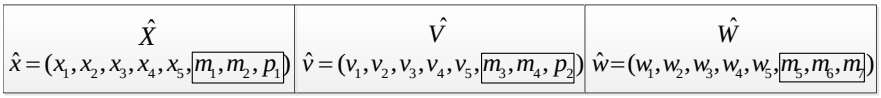


Figure 5: Block structure of the stego image in the proposed scheme

lami et al. [6] employ the concept of linear cellular automata instead of Shamir's $(k,n)$ threshold image sharing scheme. Although this scheme also achieves good visual quality and authentication ability, it needs to offer at least $k$ consecutive shadows to reveal the secret image, and cannot accurately locate the tampered blocks.

# 3 Proposed Scheme

The proposed scheme includes the following two phases: (1) the sharing and embedding phase; and (2) the authentication and revealing phase.

## 3.1 Sharing and Embedding Phase

Based on the details described in previous sections, we can now describe a complete algorithm to implement the proposed sharing and embedding procedure. Assume that the secret image $SE$ is a $m \times m$ gray-scale image. Select $n$ meaningful images like photographs of famous people or beautiful landscapes as cover images with a size of $w \times w$.

Wang and Su's scheme [18] as described in Sub-section 2.1 was first adopted to generate $n$ shadows. Notice that the sharing function in our scheme is slightly different from that in Wang and Su's scheme. In order to meet the needs of the matrix encoding, we use the parameter $t = 3$ instead of $t = 8$ in Equation (2); that is, every 3 bits that are obtained from the Huffman output stream are converted into the decimal sharing coefficient, and the generation polynomial used in GF($2^3$) is $x^3 + x + 1$, as shown in Equation (7). Apparently, all pixel values in each shadow are limited to the range from 0 to 7.

$$f_l(x) = (a_0 + a_1 x + a_2 x^2 + \cdots + a_{k-1} x^{k-1}) \mod 2^3. \quad (7)$$

To achieve a high embedding efficiency which indicates the average bit number of embedded secret data per change, the ordered triple (1,7,3) is used in our scheme as an example of matrix encoding. Accordingly, the structure of the four-pixel block in the cover image of previous schemes also needs to be changed. In the proposed scheme, as shown in Figure 5, every three pixels form a block so as to implement the matrix encoding. Suppose that we choose $m_1, m_2, m_3, m_4, m_5, m_6, m_7$ from the three pixels $\hat{X}, \hat{V}, \hat{W}$ in each block as an embedding cell. And each shadow pixel is converted into binary bits $s_1, s_2, s_3$ as secret data to be embedded. The following is a basic algorithm that reveals the principle of the proposed scheme for embedding.

**Embedding algorithm.**

**Input.** $n$ shadow images $S^{(j)}$, $n$ cover images $C^{(j)}, j \in [1,n]$, and a secret key $K$.

**Output.** $n$ stego images $\hat{C}^{(j)}, j \in [1,n]$, and $n$ sub-keys $K_1, \ldots, K_j, \ldots, K_n$.

**Steps.**

**Step 1.** Split the secret key $K$ into $n$ sub-keys $K_1, \ldots, K_j, \ldots, K_n$ by using the polynomial sharing function (Note that here we do not need the modulo operator).

**Step 2.** Divide each cover image $C^{(j)}$ into non-overlapping blocks with size $1 \times 3$.

**Step 3.** Select random location for the embedded block through the following steps:

- Assume that the length of the $j$-th shadow is $l$, and the number of all blocks in the $j$-th cover image is $L$, then calculate

$$t = \lfloor \frac{L}{l} \rfloor, \quad (8)$$

where $t$ means that at least one block during $t$ continuous blocks can be used to embed a shadow pixel.

- Use the secret sub-key $K_j$ to generate the random sequence $\{r_1^{(j)}, r_2^{(j)}, \ldots, r_l^{(j)}\}$.
- The $i^{(j)}$-th location of the embedded block is calculated by Equation (9).

$$Loc(i^{(j)}) = i^{(j)} \times t + r_i^{(j)} \bmod t, \quad 1 \le i^{(j)} \le l. \quad (9)$$

Here, we randomly select one block to embed secret data during $t$ continuous blocks, which can realize uniform random embedding.

**Step 4.** Embed binary bits $s_1, s_2, s_3$, which are converted from the $i^{(j)}$-th shadow pixel, into the $i^{(j)}$-th embedded block by using the matrix encoding. Here, at most one bit was changed in the $i^{(j)}$-th embedded block.

**Step 5.** Calculate two authentication bits $p_1, p_2$ and embed them into the relevant position in Figure 5.

$$p_1 p_2 = XOR\langle H_{K_j}(TH^{(j)} || B_{ID}^{(j)}) \rangle_2, \quad (10)$$

where $H_{K_j}(\cdot)$ is a hash function with the secret key $K_j$, $TH^{(j)}$ is 15-bit exclusive

the check bits $p_1, p_2$ and an embedding cell $m_1, m_2, m_3, m_4, m_5, m_6, m_7$ from each block of $j$-th cover image, $||$ represents the concatenation operator for strings, $B_{ID}^{(j)}$ is the block ID of $j$-th cover image. Then, the generated output of hash function is executed XOR operation to obtain two authentication bits $p_1, p_2$.

From the description above, we can observe three facts.

1) Secret data was evenly and randomly distributed throughout the whole cover image in order to reduce changes in the visual and statistical properties of the stego images.

2) No more than one bit is changed when embedding the secret data. In other words, no more than three bits were changed in each block of the cover images, so higher visual quality of the stego images can be acquired.

3) Sub-keys $K_j$ used to calculate authentication bits can prevent the other participants from using their own authentication bits to counterfeit.

### 3.2 Authentication and Revealing Phase

Our proposed scheme has two-stage authentication ability.

1) Identity authentication, that is, any $k$ or more participants should provide their sub-keys $K_j$ to the administrator. Afterwards, these sub-keys $K_j$ can be used to recover the secret key $K$ by Lagrange's interpolation. If the recovered secret key $K$ is different from the original secret key $K$, then identity authentication failed; otherwise, further tamper authentication will be implemented.

2) Tamper authentication. Stego images which pass the identity authentication are divided into a set of blocks with three pixels, and then the corresponding sub-keys $K_j$ and the information of block are used to generate the authentication bits. Authentication bits are taken out from the provided stego images, and then compared with the generated authentication bits. If they differ, then the stego image has been tampered with; otherwise, authentication is successful.

After successful authentication, the secret data $s$ can be retrieved by using the inverse processing of data embedding. The basic steps for data extraction are as following:

**Step 1.** Collect any $k$ stego images which have been certified.

**Step 2.** Divide each stego image into non-overlapping blocks with size $1 \times 3$;

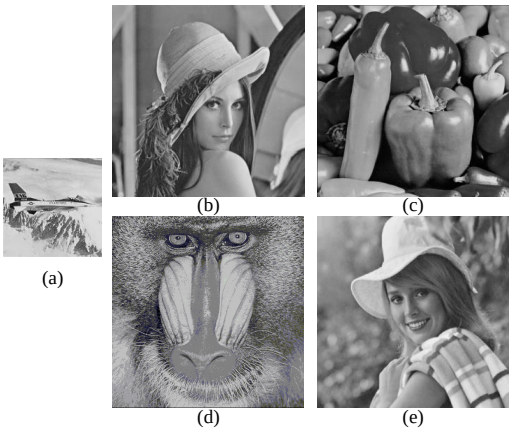


Figure 6: The five test images, (a) Jet-F16, (b) Lena, (c) Peppers, (d) Baboon, (e) Elaine

**Step 3.** Confirm location of the embedded block using Step 3 in the embedding process.

**Step 4.** Extract an embedding cell $m_1, m_2, m_3, m_4, m_5, m_6, m_7$ from every confirmed embedded block. And Use the matrix encoding described in Section 2.2 to retrieve the binary bits $s_1, s_2, s_3$.

**Step 5.** Convert each binary bits $s_1, s_2, s_3$ into the decimal number, and these decimal numbers are rearranged to recover the shadow image.

When all $k$ shadows corresponding to all $k$ stego images are obtained, the secret image can be recovered by using the method as described in Section 2.1. Note that we use Shamir's $(k, n)$-threshold scheme to generate the shadows, so less than $k$ stego images is not enough to recover any information about the secret image.

## 4 Experimental Results and Analysis

Five test images from the USC-SIPI image database as shown in Figure 6 contain a 256×256 secret image Jet-F16 (Figure 6(a)) and four 512×512 cover images Lena (Figure 6(b)), Peppers (Figure 6(c)), Baboon (Figure 6(d)) and Elaine (Figure 6(e)). Three groups of experiments are performed in this section: (1) to estimate the visual quality of the stego images; and (2) to test the authentication ability.

### 4.1 Estimate the Visual Quality of the Stego Images

The objective quality of the stego images is measured by the peak-signal-to-noise ratio (PSNR), which is defined as

$$PSNR = 10\log_{10}(\frac{255^2}{\text{MSE}})\text{dB}, \quad (11)$$

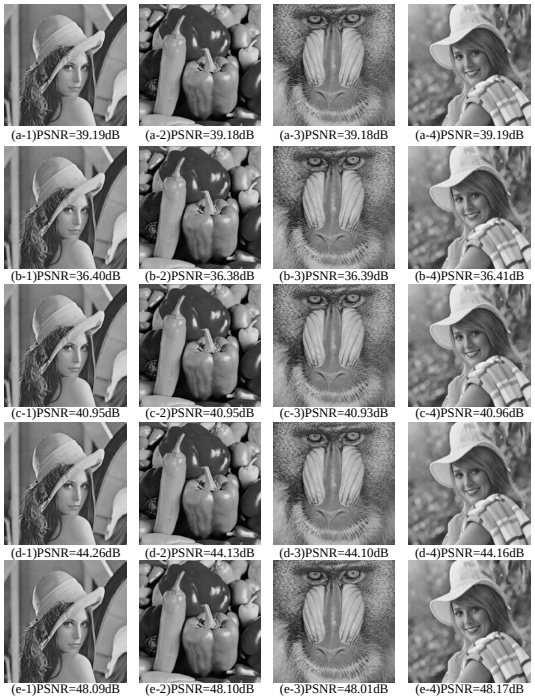


Figure 7: The experimental results of different schemes when (a) stego images in Lin and Tsai 's scheme, (b) stego images in Yang et al.'s scheme, (c) stego images in Chang et al.'s scheme, (d) stego images in Eslami et al.'s scheme, (e) stego images in the proposed scheme

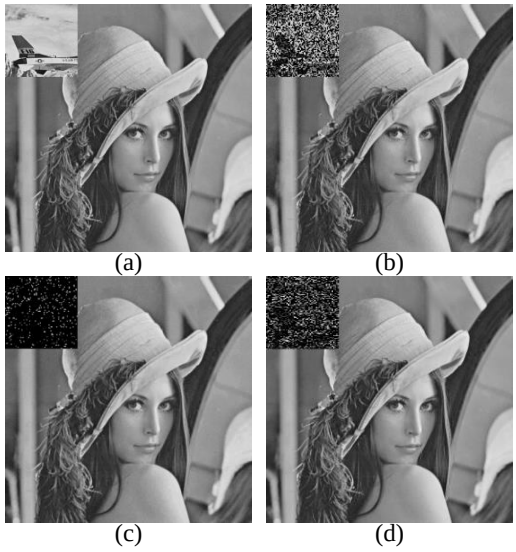


Figure 8: Experimental results for three different schemes, (a) tampered Lena stego image, (b) Yang et al.'s scheme with $DR \approx 1/2$, (c) Chang et al.'s scheme with $DR \approx 15/16$, (d) our scheme with $DR \approx 3/4$

where MSE is the mean square error between the cover images and the stego images. In this experiment, we choose two groups of different threshold parameters: the first group is $k = 2, n = 3$; the second is $k = 3, n = 4$. Figure 7 demonstrates the experimental results of different schemes when $k = 2, n = 3$. As can be seen from Figure 7, the proposed scheme obtains the highest PSNR value among the compared schemes. Note that all of the experiments are conducted under the same conditions, i.e., the same secret image, the same cover image and the same $k, n$.

Table 1 summarizes the experimental results of different schemes when $k = 3, n = 4$. Elaine is used as the fourth cover image in all mentioned schemes. Under the same experimental conditions, the proposed scheme still obtains the highest PSNR value. The reason for this objective quality is that our scheme changes relatively fewer bits, that is to say, not more than one bit in each pixel of the embedding block is modified by hidden secret and authentication bits.

In order to further illustrate the effectiveness of the proposed scheme, we calculated average number of modified bits per pixel in different schemes when different $k$ because fewer modifications can obtain higher quality of the stego images. Table 2 summarizes the results of this comparison. It can be seen from the comparison that, the average number of modified bits per pixel in our scheme is smallest when different $k$, so we also obtain the best visual quality of stego images.

## 4.2 Testing the Authentication Ability

The detection ratio is defined as $DR = NTPD/NTP$ to test the authentication ability, where $NTPD$ is the number of tampered pixels that are detected, and $NTP$ is the number of tampered pixels [6].

In this sub-section, we make the tampered Lena stego image by adding a shrunk version of the Jet-F16 in Figure 8(a). Herein, Lin and Tsai's scheme and Eslami et al.'s scheme are not considered to compare the authentication ability because they cannot effectively prevent tampering or locate the tampered position. Figures 8(b), (c) and (d) show the experimental results for three different schemes. Figures 8 (b) and (c) use the same size of stego-block (4 pixels) to achieve tamper detection, but the detection ratio of Yang et al.'s scheme is lower than that of Chang et al. In our scheme, we choose the smaller stego-block (3 pixels) to achieve tamper detection.

Although the detection ratio is slightly lower than that of Chang et al.'s scheme, we adopt a two-stage authentication mechanism, that is to say, the participant firstly must provide the right sub-key $K_j$ to pass identity authentication before tamper detection. It is very difficult to accurately guess the random sub-key $K_j$. Therefore, our scheme has higher authentication ability.

Table 1: Experimental results of different schemes when $k = 3, n = 4$

| Scheme | PSNR | | | |
|---|---|---|---|---|
| | Lena | Pepper | Baboon | Elaine |
| Lin and Tsai's scheme | 39.22 | 39.18 | 39.21 | 39.22 |
| Yang et al.'s scheme | 36.41 | 36.38 | 36.35 | 36.40 |
| Chang et al.'s scheme | 42.70 | 42.77 | 42.73 | 42.69 |
| Eslami et al.'s scheme | 47.12 | 47.16 | 47.10 | 47.15 |
| Our scheme | 49.47 | 49.47 | 49.50 | 49.51 |

Table 2: Comparison of average number of modified bits per pixel with different $k$

| Different $k$ | average number of modified bits per pixel | | | | |
|---|---|---|---|---|---|
| | Lin et al. | Yang et al. | Chang et al. | Eslami et al. | Ours |
| $k$ | – | – | $1 + (2/k)$ | $2/(k-1)$ | – |
| 2 | 2.25 | 2.75 | 2 | 2 | 0.85 |
| 3 | 2.25 | 2.75 | 1.67 | 1 | 0.74 |
| 4 | 2.25 | 2.75 | 1.5 | 0.67 | 0.59 |

# 5 Conclusions

In this paper, a secret image sharing with deep-steganography and two-stage authentication was proposed. This scheme is based on matrix encoding to embed secret shadows into cover images and at most one bit was changed in the embedded block, so secret data does not directly appear in the pixels of the cover image. This ensures the security of secret data and obtains higher visual quality of the stego image. As far as authentication ability is concerned, our scheme increases the process of the identity authentication, that is to say, participants must first provide the right sub-key to pass identity authentication, and then pass tamper authentication. The final experimental results also demonstrate that our scheme achieves better authentication ability than those referenced in the literature review.

# Acknowledgments

This work has been supported in part by National Natural Science Foundation of China (No. 61272262), Program for New Century Excellent Talent in Universities (NCET-12-1037), International Cooperative Program of Shanxi Province (No. 2015081015).

# References

[1] S. Chakraborty and S. K. Bandyopadhyay, "Steganography method based on data embedding by sudoku solution matrix," *International Journal of Engineering Science Invention*, vol. 2, no. 7, pp. 38–42, 2013.

[2] C. C. Chang, Y. P. Hsieh, and C. H. Lin, "Sharing secrets in stego images with authentication," *Pattern Recognition*, vol. 41, no. 10, pp. 3130–3137, 2008.

[3] C. C Chang, N. T. Huynh, and T. F. Chung, "Efficient searching strategy for secret image sharing with meaningful shadows," *International Journal of Machine Learning and Computing*, vol. 3, no. 5, pp. 342–352, 2014.

[4] R. Crandall, "Some notes on steganography," *Posted on Steganography Mailing List*, pp. 1–6, 1998.

[5] X. Dong, "A multi-secret sharing scheme based on the CRT and RSA," *International Journal of Electronics and Information Engineering*, vol. 2, no. 1, pp. 47–51, 2015.

[6] Z. Eslami, S. H. Razzaghi, and J. Z. Ahmadabadi, "Secret image sharing based on cellular automata and steganography," *Pattern Recognition*, vol. 43, no. 1, pp. 397–404, 2010.

[7] L. Fan, T. Gao, Q. Yang, and Y. Cao, "An extended matrix encoding algorithm for steganography of high embedding efficiency," *Computers & Electrical Engineering,*, vol. 37, no. 6, pp. 973–981, 2011.

[8] J. Fridrich, M. Goljan, and R. Du, "Reliable detection of lsb steganography in color and grayscale images," *Proceedings of The International Conference on Multimedia and Security: New Challenges*, pp. 27–30, 2001.

[9] H. Gupta, A. P. R. Kumar, and S. Changlani, "Steganography using lsb bit substitution for data hiding," *International Journal of Advanced Research in Computer Science and Electronics Engineering*, vol. 2, no. 10, pp. 676–680, 2013.

[10] C. Jianping and U. Jauhari, "Analysis on regular-singular steganalysis algorithm for multimedia,"

*Journal of Network & Information Security*, vol. 4, no. 4, pp. 395–403, 2013.

[11] L. Li, A. El-Latif, X. Yan, S. Wang, and X. Niu, "A lossless secret image sharing scheme based on steganography," in *Proceedings of The International Conference on Instrumentation, Measurement, Computer, Communication and Control (IMCCC'12)*, pp. 1247–1250, Beijing, China, Dec. 2012.

[12] C. C. Lin and W. H. Tsai, "Secret image sharing with steganography and authentication," *Journal of Systems and Software*, vol. 73, no. 3, pp. 405–414, 2004.

[13] M. Naor and A. Shamir, "Visual cryptography," *Advances in Cryptology (EUROCRYPT'94)*, pp. 1–12, Springer, 1995.

[14] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[15] M. Shobana, "Efficient X-box mapping in stego-image using four-bit concatenation," *International Journal of Electronics and Information Engineering*, vol. 1, no. 1, pp. 29–33, 2014.

[16] A. Singh and U. Jauhari, "A symmetric steganography with secret sharing and psnr analysis for image steganography," *International Journal of Scientific & Engineering Research*, vol. 3, no. 6, pp. 2–8, 2012.

[17] C. C. Thien and J. C. Lin, "Secret image sharing," *Computers & Graphics*, vol. 26, no. 1, pp. 765–770, 2002.

[18] R. Z. Wang and C. H. Su, "Secret image sharing with smaller shadow images," *Pattern Recognition Letters*, vol. 27, no. 6, pp. 551–555, 2006.

[19] D. C. Wu and W. H. Tsai, "A steganographic method for images by pixel-value differencing," *Pattern Recognition Letters*, vol. 24, no. 9, pp. 1613–1626, 2003.

[20] C. N. Yang, T. S. Chen, K. H. Yu, and C. C. Wang, "Improvements of image sharing with steganography and authentication," *Journal of Systems and Software*, vol. 80, no. 7, pp. 1070–1076, 2007.

[21] C. N. Yang, J. F. Ouyang, and L. Harn, "Steganography and authentication in image sharing without parity bits," *Optics Communications*, vol. 285, no. 7, pp. 1725–1735, 2012.

**Li Liu** received her B.E. degree in communication engineering in 2002, from Lanzhou Railway University and M.E. degree in communication and information system in 2006, from Lanzhou Jiaotong University. Now, she is a Ph. D student in Northwestern Polytechnical University. Her current research interests include information hiding and secret sharing. She has published more than 10 papers.

**Anhong Wang** was born in Shanxi Province in 1972. She received B.E and M.E. degrees from Taiyuan University of Science and Technology (TYUST) respectively in 1994 and 2002, and PHD degree in Institute of Information Science, Beijing Jiaotong University in 2009. She became an associate professor with TYUST in 2005 and became a professor in 2009. She is now the director of Institute of Digital Media and Communication, Taiyuan University of Science and Technology. Her research interest includes image/video coding, compressed sensing, and secret image sharing. She has published more than 40 papers. Now she is leading two national research projects from National Science Foundation of China.

**Chin-Chen Chang** received his B.E. degree in applied mathematics in 1977 and the M.E. degree in computer and decision sciences in 1979, both from the National Tsing Hua University, Hsinchu, Taiwan. He received his Ph. D in computer engineering in 1982 from the National Chiao Tung University, Hsinchu, Taiwan. Since February 2005, he has been a Chair Professor of Feng Chia University. In addition, he has served as a consultant to several research institutes and government departments. His current research interests include database design, computer cryptography, image compression and data structures.

**Zhihong Li** was born in Shanxi Province in 1970. He is currently an associate professor in Taiyuan University of Science and Technology (TYUST). He received the B.Eng. degrees in electronic information engineering from Taiyuan University of Science and Technology (TYUST) in 1994. His research interest includes compressed sensing and secret image sharing. He has participated in the projects on distributed video coding and now is leading one research project on image secret from Shanxi Natural Science Foundation.