Journal of Information Hiding and Multimedia Signal Processing ©2014 ISSN 2073-4212
Ubiquitous International Volume **5**, Number **3**, July **2014**

Image Secret Sharing and Hiding with Authentication Based on PSNR Estimation

Peng Li, Qian Kong, Yanpeng Ma

Department of Mathematics and Physics
North China Electric Power University
Baoding, Hebei, 071003 China
lphit@163.com, qiankongkong@126.com, yanpengma@163.com

Received July, 2013; revised January, 2014

Abstract. *In order to increase the security in storage and transmission, the secret image can be shared and hidden in ordinary cover images to form the stego images. Many image secret sharing schemes with steganography and authentication have been proposed. The qualification of the stego images can be verified. Unfortunately, each of these schemes has one or more drawbacks. First, the size of the stego images is large. Second, the visual quality of the stego images evaluated by the peak signal-to-noise ratio (PSNR) is degraded too much. Third, the authentication ability is weak. To overcome such drawbacks, a new scheme based on PSNR estimation is proposed in this paper. The new scheme can optimize both the quality and the size of the stego images. In addition, the piecewise authentication method based on Hash function is introduced to improve the authentication ability. Finally, the effectiveness and efficiency of our scheme are confirmed by the experimental results.*
Keywords: Image secret sharing, Steganography, PSNR estimation, Piecewise authentication

1. **Introduction.** The effective and secure protections of secret images are primary concerns in commercial, medical and military systems. The confidential images must be encrypted from being illegally accessed. However, a common problem is that these encrypted images are maintained in a single information-carrier. For example, the secret image cannot be recovered if the encrypted image is lost or corrupted during the transmission. To solve this security problem, image secret sharing method had been introduced. The secret image is shared among a set of participants. Only the qualified subsets of participants can cooperate to reconstruct the original secret image, unqualified subsets of participants can get no information about the secret image.

The first concept of the (t, n) threshold secret sharing scheme was introduced by Shamir [1]. The secret data is hidden in the constant term of a $(t-1)$-degree polynomial to generate n shadows (also called shares), where any t $(t \leq n)$ or more shadows can be collected to reconstruct the secret data, while any $t-1$ or fewer shadows can get no information about the secret. An important category of secret image sharing is visual cryptography scheme (VCS) proposed by Naor and Shamir [2]. The secret image can be visually decoded through the human visual system without any hardware and computation. However, the visual quality of the recovered secret image in VCS is extremely poor. Some VCS-based schemes were proposed for different application [3-5]. Another category of image secret sharing scheme is based on polynomial. In 2002 Thien and Lin proposed a (t, n)-threshold

polynomial-based image secret sharing scheme [6]. They hide the secret pixels in all coefficients of a $(t-1)$-degree polynomial to split the secret image into n noise-like shares, also called shadow images. The size of each shadow image is only $1/t$ of that of the secret image. Many polynomial-based image secret sharing schemes were proposed for smaller size of shadow images [7, 8].

Since each shadow image is noise-like, it may attract the attention of attackers and is not convenient for management. Some data hiding methods can be utilized to hide the shadow images in some ordinary images. Wu et al. proposed a secret image sharing and hiding method without size expansion [9]. A pre-processing quantization procedure is developed for compressing the secret image. Then the compressed secret image is used to generate shadow images based on polynomial, and finally the shadow images are hidden in the cover images. However, the generated image with the shadow image embedded in, called stego image, has noticeable deterioration of visual quality. Furthermore, their scheme is lossy for secret image, which is not applicable in some situations such as military,medical and fine art image preservation. Some researchers employed the modulus operator to reconstruct the distortion-free cover image [10, 11].

Since multi-participants should cooperate to reveal the secret image, it is unpractical to assume that each participant is honest. The malicious participants may modify their stego images and cause the recovery of a wrong secret image. Some image secret sharing schemes with steganography and authentication were proposed to further protect the qualification of the stego images [12-15]. For example, Lin and Tsai proposed an image secret sharing scheme with steganography and authentication based on parity check policy [12]. Each shadow pixel is embedded in a 4-pixel stego block with a check bit. However, their scheme has three weaknesses pointed out by Yang *et al.* [13]. The first one is weak authentication process which may allow the fake stego image to pass the authentication check. The second one is lossy recovering of the secret image. The third one is the deteriorated quality of the stego images. In 2007, Yang *et al.* proposed an improved scheme based on hash message authentication code to achieve higher authentication ability [13]. Although Yang *et al.*'s scheme overcomes the weaknesses in the scheme of Lin and Tsai, the computational cost of the authentication process is too high, which need to evaluate the hash value for each shadow pixel separately. Recently, Chang *et al.* proposed a secret sharing scheme combining steganography and authentication based on Chinese Remainder Theorem (CRT) [14]. The detecting ratio of a modified stego block is improved to 15/16. Unfortunately, their scheme degrades the visual quality of the stego images by modifying three bits of each stego pixel. Eslami *et al.* improve the quality and authentication of stego images based on cellular automata [15]. However, there scheme can only reveal secret image by consecutive stego images, which restricts the range of application. In these schemes, there is a common problem that the size of the stego images should be expanded to 4 times of that of the shadow images [12-15]. The larger size expansion increases the cost in storage and transmission. Wu *et al.* reduced the size expansion of stego images to 3.5 times of that of the shadow images with acceptable visual quality [16]. There were also some image secret sharing schemes dealing with different problems [17-19], like general access structure and security problem.

In this paper, we propose an enhanced scheme based on PSNR estimation. The secret image is first shared into shadow images by polynomial-based secret sharing scheme. Then, each shadow image is hidden in a cover image by the proposed (s, c) hiding method based on PSNR estimation. The piecewise authentication method based on Hash function

is also proposed to improve the authentication ability. As a result, the proposed scheme can optimize both the visual quality and size expansion of the stego images compared with the schemes of Lin and Tsai [12], Yang *et al.* [13] and Chang *et al.* [14]. It also can achieve acceptable visual quality of the stego images with smaller size expansion. In addition, the qualification of the stego images can be verified efficiently.

The rest of this paper is organized as follows. Section 2 reviews the related works. Section 3 analyzes the PSNR estimation, and the proposed scheme is presented in Section 4. Then, the experimental results and discussion are given in Section 5. Finally, we conclude in Section 6.

2. **Related works.**

In this section, we briefly review the related techniques including the image secret sharing scheme of Thien and Lin [6], and the concept of the optimal least significant bits(OLSBs) substitution method [20].

2.1. **Thien-Lin secret image sharing scheme.**

Thien and Lin [6] developed a (t, n)-threshold image secret sharing scheme to share a secret image into n shadow images by a $(t-1)$-degree polynomial.

$$f(x) = (a_0 + a_1 x + \cdots + a_{t-1} x^{t-1}) \ mod \, p \tag{1}$$

where p is a prime number. All coefficients $a_0, a_1, \ldots, a_{t-1}$ are replaced by secret pixel values. For each time, it can share t secret pixels, and each shadow image receives one shadow pixel. Therefore, the shadow image size is reduced to $1/t$ of that of the secret image. The revealing process can be implemented by Lagrange interpolation using any t shadow images.

2.2. **The OLSBs substitution method.**

In steganography, the visual quality is mostly a concern. The PSNR value is a widely used criterion for evaluating the visual quality of the stego image. The definition of PSNR is as follows.

$$PSNR = 10 \times \log_{10}(255)^2 / MSE \ dB \tag{2}$$

where *MSE* is the mean-square error between the cover image and the stego image. If the size of the cover image is $M \times N$, MSE is defined as

$$MSE = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} (x_{ij} - y_{ij})^2 \tag{3}$$

where x_{ij} and y_{ij} denote the cover and the stego pixel values, respectively.

In the simple least significant bits (LSBs) substitution method, the LSBs of the cover image are replaced by secret bits directly. The simple LSBs substitution can be modified so that the stego image quality gets improved. Chan and Cheng proposed an improved method called the OLSBs substitution [20]. The essential idea is finding the best pixel (closest to the original pixel value) with the secret data embedded. The embedding algorithm goes as follows:

Step1 Assume A_i is the original pixel value and m bits of secret data are to be embedded.
Step2 Embed m secret bits in A_i by simple LSBs substitution. The stego pixel B_i can be obtained.
Step3 Compute the error e_i , where $e_i = A_i - B_i$.

Step4 The optimal stego pixel C_i can be computed by the following formula:

$$C_i = \begin{cases} B_i - 2^m & \text{if } e_i < -2^{m-1} \\ B_i & \text{if } -2^{m-1} \le e_i \le -2^{m-1} \\ B_i + 2^m & \text{if } e_i > 2^{m-1} \end{cases} \tag{4}$$

By OLSBs substitution, the absolute error is reduced from $0 \le e_i \le 2^m - 1$ to $0 \le e_i \le 2^{m-1}$. The distortion of the stego image is also greatly reduced.

3. The PSNR estimation.

In this section, we theoretically analyze the estimated PSNR of the stego image.

3.1. The estimated PSNR of simple LSBs substitution.

To estimate the PSNR value of the stego image, a proper assumption should be given as follows.

Assumption 1: Suppose the $m(m \le 4)$ LSBs of the cover image should be replaced by secret bits. The decimal value of the m LSBs of each cover pixel is uniformly distributed in $\{0, 1, \ldots, 2^m - 1\}$.

This assumption works sense for natural image especially when $m \le 4$. This assumption should also be the selection criteria for the cover image. Indeed, if more than 4 LSBs of the cover image are used to embed secret information, the visual quality of the stego image will be degraded seriously. Therefore, the value of m should be smaller than 5 in practices. In addition, the secret bits to be embedded in cover image are usually encrypted as noise-like bits. With Assumption 1, we get Proposition 3.1 as follows.

Proposition 3.1. *Let A be the cover image. B is the stego image generated by m LSBs substitution. Then the estimated MSE between A and B is*

$$MSE(m) = (2^{2m} - 1)/6 \tag{5}$$

See Appendix A for proof. By equation 2, the estimated PSNR of the stego image is evaluated.

3.2. The estimated PSNR of OLSBs substitution.

The estimated MSE of the stego image with OLSBs substitution is shown in Proposition 3.2 .

Proposition 3.2. *Let A be the cover image. B is the stego image generated by $m(m > 0)$ OLSBs substitution. Then the estimated MSE between A and B is*

$$MSE_{opt}(m) = (2^{2m-1} + 1)/6 \tag{6}$$

The proof of Proposition 3.2 is similar as that of Proposition 3.1 . In order to save space, we omit the proof.

By equation 2, the estimated PSNR of the stego image generated by OLSBs substitution can be computed. Note that, $MSE(0)$ and $MSE_{opt}(0)$ are both equal to zero, which means no difference between the stego image and the cover image. Obviously, $MSE(m)$ is larger than or equal to $MSE_{opt}(m)$. We also get the following proposition by further observation of equation 5 and equation 6.

Proposition 3.3. MSE(m) *and MSE_{opt} represent the* MSE *with simple m LSBs substitution and optimal m LSBs substitution, respectively. Then we have:*

$$MSE(m_1) + MSE(m_2) + \cdots + MSE(m_n) \ge (n - b) \times MSE(a) + b \times MSE(a + 1) \tag{7}$$

$$MSE_{opt}(m_1)+MSE_{opt}(m_2)+\cdots+MSE_{opt}(m_n) \geq (n-b)\times MSE_{opt}(a)+b\times MSE_{opt}(a+1) \tag{8}$$

where m_i *is non-negative integer,*$a = \lfloor Num/n \rfloor$,$b = Num \bmod n$ *, and* $Num = m_1 + m_2 + \cdots + m_n$.

See Appendix B for proof. As shown in Proposition 3.3, if *Num* bits should be embedded in n cover pixels, the optimal solution with the lowest *MSE* value is embedding a bits in each of $n-b$ cover pixels, and $a+1$ bits in each of the other b cover pixels. Since *PSNR* is inversely proportional to *MSE*, minimal *MSE* value means maximal *PSNR* value. This is the advantage of (s, c) hiding method that will be introduced in the next section.

4. **The proposed scheme based on PSNR estimation.** The proposed scheme consists of two procedures. The first one is sharing and hiding procedure, and the second one is authentication and revealing procedure.

4.1. **Sharing and hiding procedure. (A) Secret image sharing**. Before sharing, the secret image should be encrypted using secret key K. The key K is shared into n subkeys to n participants by Shamir's secret sharing scheme [1]. In general, a (t, n)-threshold secret image sharing scheme splits the secret image into n shadow images. Then any t shadow images can reconstruct the original secret image. In order to process the grayscale values for 8-bit pixel directly, the Galois Field GF(2^8) as introduced by Yang *et al.*[13] is also adopted in the proposed scheme. A $(t-1)$-degree polynomial is constructed as

$$f(x) = (a_0 + a_1 x + \cdots + a_{t-1}x^{t-1}) \; mod \; g(x) \tag{9}$$

where $g(x) = (x_8 + x_4 + x_3 + x + 1)$. First, randomly choose n different integers in $\{1, 2, \ldots, 255\}$, $ID_1, ID_2, \ldots, ID_n$ as the ID of n participants. Second, divide the secret pixels into several sections, and each section has t secret pixels. Third, every t pixels from one section are hidden in the coefficients of the polynomial, and use ID_i as the input to generate a pixel of the ith shadow image as shown in Fig.1. n shadow images are generated until all sections are processed. Since all the coefficients of the polynomial are replaced by the secret pixel values, the size of each shadow image is $1/t$ of that of the secret image.

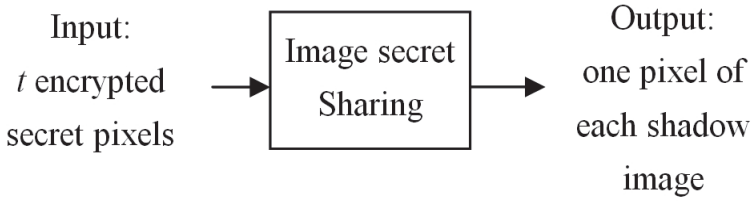

FIGURE 1. The diagram of the sharing procedure

(B) (s, c) **hiding method based on PSNR estimation**. In order to hide each shadow image in a cover image, the (s, c) hiding method is introduced based on *PSNR* estimation, which means that an s-pixel block of the shadow image is embedded in a c-pixel block of the cover image. Also, a check bit should be embedded in each c-pixel block of the cover image for authentication. That is to say, $8s+1$ bits (s shadow pixels and one check bit) are embedded in a c-pixel block of the cover image.

There are several methods to embed $8s+1$ bits in c cover pixels. Based on the theoretic analysis in Proposition 3.3 , $8s+1$ bits evenly embedded in c cover pixels will result in

the smallest *MSE*, which means the largest *PSNR* value of the stego image.

The hiding strategy is set as follows.

First, evaluate a and b by the following equations.

$$a = \lfloor (8s+1)/c \rfloor \tag{10}$$

$$b = (8s+1) \ mod \ c \tag{11}$$

Second, divide all the pixels of the cover block into two subsets, the first subset contains $c-b$ pixels, the second subset contains b pixels.

Third, embed a bit in each pixel of the first subset, including the check bit embedded in the LSB of the first pixel of the first subset; and embed $a+1$ bits in each pixel of the second subset.

Fig. 2 illustrates an example of $(2, 6)$ hiding method based on *PSNR* estimation, where $X_i, W_i, V_i, Z_i, T_i, Y_i$ represent six pixels of the i-th block of the cover image, and $X_i^{'}, W_i^{'}, V_i^{'}, Z_i^{'}, T_i^{'}, Y_i^{'}$ represent the corresponding stego pixels. The 16 secret bits (two secret pixels) are represented as $s_1, s_2, \ldots s_{16}$, and p is the check bit. Evaluating a and b by equations (10)-(11), we have $a = 2$ and $b = 5$. Therefore one cover pixel has 2 bits embedded in (one secret bit and the check bit), and the other five cover pixels each has 3 bits embedded in.

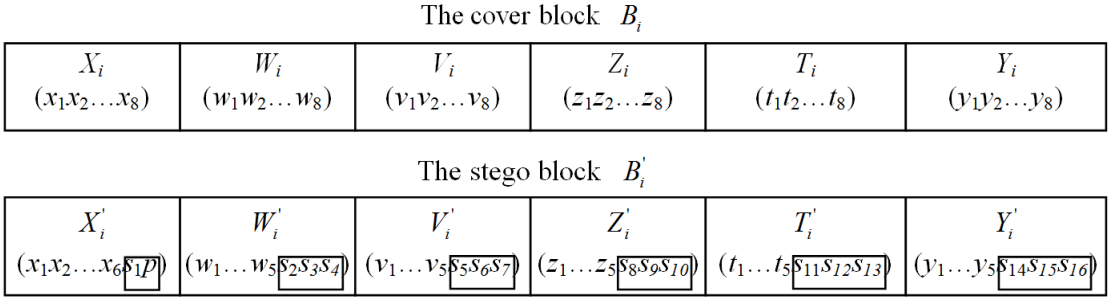

FIGURE 2. An illustration of (2, 6) hiding method

In order to improve the visual quality of the stego images, the OLSBs substitution is adopted in our scheme. Note that the stego pixel with the check bit embedded in should take $a-1$ bits of the shadow pixels embedded in at first by OLSBs substitution, and then the check bit is computed and embedded by simple LSBs substitution. Let $MSE_{check}(m)$ be the estimated *MSE* between the stego pixel with the check bit embedded in and the corresponding cover pixel, where m is the number of bits embedded in the stego pixel. Obviously, we have $MSE_{check}(1) = MSE(1)$. For the case of $m \geq 2$, we have Proposition 4.1 .

Proposition 4.1.

$$MSE_{check}(m) = \begin{cases} 5/2 & m = 2 \\ 13/2 & m = 3 \\ 45/2 & m = 4 \end{cases}$$

The proof is omitted here. Therefore, the estimated MSE of the stego block is

$$MSE = (MSE_{check}(a) + (c-b-1)MSE_{opt}(a) + bMSE_{opt}(a+1))/c \tag{12}$$

Then, the estimated PSNR value of stego image can be evaluated by equation 2.

(C) Piecewise authentication of stego image. To prevent malicious participants from faking the stego images, a piecewise authentication method based on hash function is introduced, by which the check bits of several stego blocks are generated simultaneously. In the proposed scheme, MD5 one-way hash function is used to generate the authentication bits. Then the check bits are generated by XOR the authentication bits and a watermark stream. Fig. 3 shows the generation diagram of the check bits. Since MD5 hash function generates a 128-bit hash value, and each stego block only has one check bit, we can generate 128 check bits at one time by processing 128 stego blocks simultaneously for improving the authentication efficiency. First, each stego image is divided into several sections, and each section contains 128 blocks. The authentication bits of each section are evaluated as follows:

$$(h_1 h_2 \cdots h_{128}) = MD5((B_1^{'} - p_1) \| (B_2^{'} - p_2) \| \cdots \| (B_{128}^{'} - p_{128}) \| K) \tag{13}$$

Where$(B_i^{'} - p_i)$ represents the $8c-1$ bits which come from the ith stego block $B_i^{'}$ of the current section exclusive the check bit p_i, and K is the secret key. $'\|'$ represents the concatenation operation.

In order to increase the security, a watermark steam is randomly generated by the secret key K. Assume that the current 128 watermark bits are denoted as $j_1, j_2, \ldots, j_{128}$. Thus, the 128 check bits of the current section are evaluated by the following equation.

$$(p_1 p_2 \cdots p_{128}) = (h_1 h_2 \cdots h_{128}) \oplus (j_1 j_2 \cdots j_{128}) \tag{14}$$

Where $'\oplus'$ represents the bit-wise XOR operation. Finally, $p_1 p_2 \ldots p_{128}$ are embedded in 128 stego blocks of the current section as check bits, respectively. The generation process of the check bits is repeated until all sections of the stego images are processed. After that, the stego images are generated and transmitted to the authorized participants with the corresponding ID. Since our scheme verify a section of 128 stego blocks as a whole, it cannot precisely localize the modified pixel. However, the proposed scheme can localize the section which has modified pixel with highly probability. f

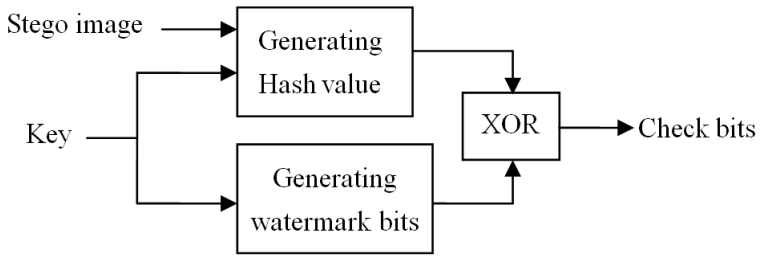

FIGURE 3. The generation diagram of the check bits

4.2. **Authentication and revealing procedure.** Without loss of generality, any t participants can cooperate to reveal the secret image. First, the secret key K is revealed by Lagrange interpolation with t sub-keys. Next, each stego image of these t participants is divided into a set of sections with 128 blocks so as to be authenticated. For each section, the authentication bits are computed by equation (13). With the watermark bits generated by secret key K, the check bits$p_1^{'} p_2^{'} \ldots p_{128}^{'}$ of the current section are computed by equation (14). If the computed check bits $p_1^{'} p_2^{'} \ldots p_{128}^{'}$ are identical to those embedded bits $p_1 p_2 \ldots p_{128}$, the current section is verified successfully, and the shadow pixels are retrieved. Otherwise, the current section is invalid, and the stego image has been changed. The authentication and retrieving process is repeated until t shadow images are retrieved

from t stego images successfully. Then the encrypted secret image is revealed by Lagrange interpolation in $GF(2^8)$. Finally, the secret image is decrypted with the secret key K.

5. Experimental results and analysis.

5.1. Experimental results.

The effectiveness and efficiency of the proposed scheme are confirmed by the experimental results in this section. All the test images are chosen from the USC-SIPI image database [21]. In the first experiment, we compare the visual quality (i.e., *PSNR* value) of the stego images among the new scheme and schemes of Lin and Tsai [12], Yang *et al.*[13] and Chang *et al.*[14]. Fig. 4 (a) shows the secret image 'House' with 256×256 pixels. Three cover images 'Lena', 'Pepper' and 'Baboon' with 512×512 pixels are shown in Fig. 4 (b)-(d). In order to compare the visual quality of the stego images in a fairly way, only the constant term of the polynomial is replaced by secret pixel when generating shadow images. Three shadow images are generated by (2, 3)-threshold polynomial-based image secret sharing scheme. Therefore, the size of each shadow image is the same as that of the secret image. In the proposed scheme, we use (4, 16) hiding method to hide each shadow image in the corresponding stego image. The experimental results are shown in Fig. 5. We also compare the average *PSNR* value, the estimated *MSE* value and the estimated *PSNR* value of the stego images among the three compared schemes and ours in Table 1. Note that, (4, 16) hiding method means four shadow pixels with a check bit are embedded in 16 stego pixels. By equations (10)-(11), we have $a = 2$ and $b = 1$. Then the estimated *MSE* is calculated by equation (12) as $MSE = (MSE_{check}(2)+14MSE_{opt}(2)+MSE_{opt}(3))/16$, and the *PSNR* value is evaluated by equation (2). In the three compared schemes [12-14], one shadow pixel and a check bit (four check bits in Chang *et al.*'s scheme) are embedded in a four-pixel stego block with simple LSB substitution. The numbers of bits embedded in each pixel of the stego block are (0-3-3-3), (2-3-2-2), and (3-3-3-3) in the three compared schemes, respectively. The estimated *MSE* and *PSNR* values of these schemes are evaluated by equation (5) and equation (2). As shown in Table 1, both the average *PSNR* value in the experiment and the estimated *PSNR* value of the proposed scheme are the largest. Our scheme achieves best visual quality of the stego images.

TABLE 1. The comparison of the *MSE* and *PSNR* values among the schemes of Lin and Tsai,[12] Yang *et al.*,[13] Chang *et al.*[14] and ours.

	Scheme of Lin and Tsai [12]	Scheme of Yang et al.[13]	Scheme of Chang et al.[14]	Our scheme
Average *PSNR*(dB)	39.18	41.61	37.92	45.54
Estimated MSE	7.875	4.5	10.5	1.8125
Estimated *PSNR*(dB)	39.17	41.60	37.92	45.54

To test the feasibility of the proposed scheme with smaller size of the cover images, three cropped images 'Stream', 'Sailboat', and 'Elaine' with 384×256 pixels are taken as the cover images as shown in Fig. 6(a). The secret image 'House' with 256×256 pixels are first shared into three shadow images by (2, 3)-threshold polynomial-based image secret sharing scheme. All coefficients of the polynomial in equation (9) are replaced by secret pixel values. Thus, the size of each shadow image is 256×128 pixels. Then, each shadow image is hidden in the corresponding cover image. (4, 12) hiding method is used in this experiment, which means a 4-pixel shadow block is embedded in a 12-pixel stego block. So $a = 2$ and $b = 9$. Thus, the first pixel of each stego block has 2 bits embedded in, including the check bit. The other 2 stego pixels each have 2 bits embedded in, and the

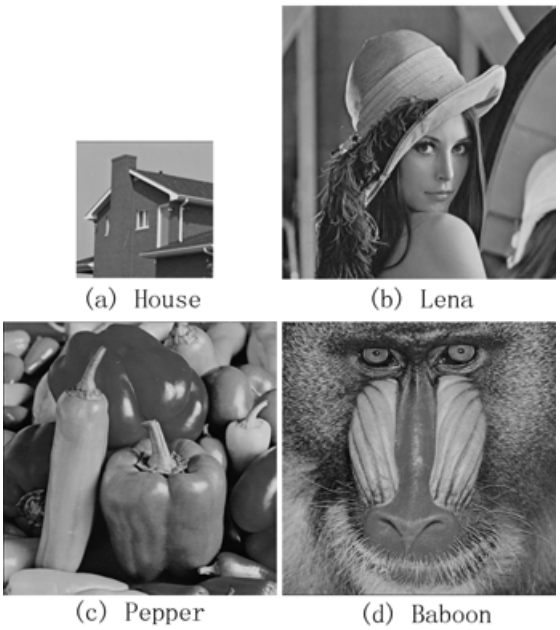

FIGURE 4. The test images. (a) the secret image, (b)-(d) three cover images

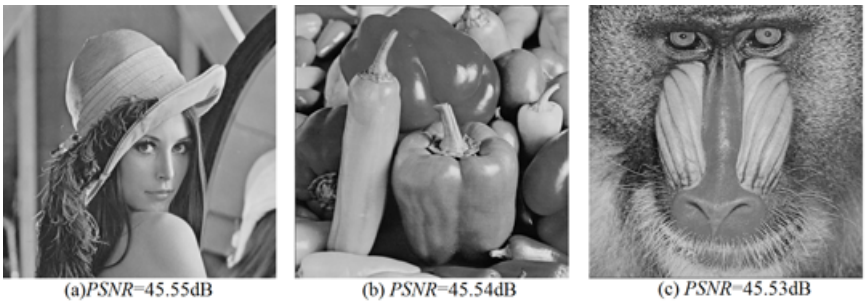

FIGURE 5. The experiment of (2, 3)-threshold sharing and hiding. (a)-(c) The generated stego images with the *PSNR* values 45.55dB, 45.54dB and 45.53dB, respectively

last 9 stego pixels each have 3 bits embedded in. The stego images are shown in Fig. 6(b). We also test various cover images with 384×256 pixels chosen from the USC-SIPI image database [21]. The PSNR values of the stego images are shown in Table 2. As we can see, all PSNR values of the stego images are larger than 41dB. It is clear that our scheme has advantage in achieving acceptable visual quality even with smaller size of the stego image.

To evaluate the authentication ability of the proposed scheme, two modified stego images are verified. Fig. 7(a) shows an obviously modified stego image 'Elaine' with an image 'pepper' added in, and the authentication result is shown in Fig. 7(b). The black square means the stego block does not pass the authentication process, which indicates the corresponding section of stego blocks was modified. The modification can be detected well. Fig. 7(c) is the authentication result of the stego image 'Sailboat' with the pixel value at position (113, 1) changed from 172 to 173. There are 64 stego blocks don't pass the authentication, which indicates the corresponding section was modified. Obviously, one pixel modified will cause many more stego blocks fail to pass the authentication check. Although our scheme does not pinpoint the area where the modification has occurred, it

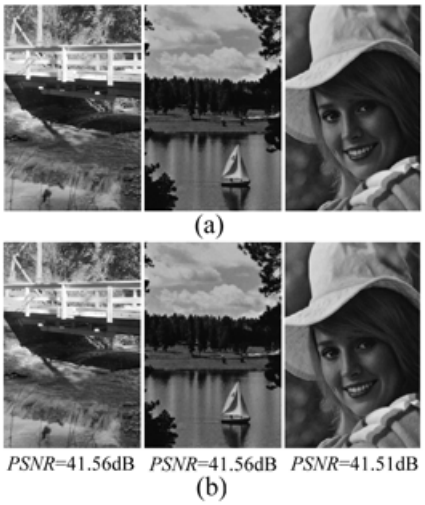

FIGURE 6. The experiment of (2, 3) threshold image secret sharing with (4, 12) hiding method

TABLE 2. The *PSNR* values (dB) of the stego images for common images

Cover image	Stego image 1	Stego image 2	Stego image 3
Aerial	41.50	41.52	41.51
Airplane	41.51	41.51	41.52
Airport	41.52	41.52	41.51
APC	41.48	41.51	41.51
Baboon	41.53	41.51	41.52
Couple	41.45	41.43	41.42
Elaine	41.49	41.53	41.51
Lena	41.52	41.52	41.52
Man	41.11	41.12	41.10
Peppers	41.51	41.50	41.52
Sailboat	41.54	41.56	41.51
Splash	41.51	41.48	41.52
Stream	41.56	41.59	41.57
Tank	41.49	41.50	41.50
Tiffany	41.52	41.50	41.47
Truck	41.53	41.54	41.53
The estimated PSNR value: 41.52dB			

has high probability to detect the modification behavior in stego image. In fact, it is not necessary to verify each pixel to make sure whether the stego image was modified. Suppose the secret image has $M \times N$ pixels. Since the hash bits of a section with 128 stego blocks are evaluated simultaneously, we only need to compute hash function $M \times N/(128 \times t \times s)$ times for each stego image. Although Yang et al.[13] also generate check bit using hash function, it need to compute hash function $M \times N$ times for each stego image. Our scheme has lower computational cost compared with Yang *et al.*'s scheme [13].

5.2. **Discussion.** In our (s, c) hiding method, s shadow pixels with a check bit are embedded in c cover pixels. In order to hide all pixels of shadow image in the cover image, the ratio of c to s should be smaller than or equal to the size ratio of the cover image to the

FIGURE 7. The experiment of the authentication process. (a) The modified stego image 'Lena'; (b) the authentication result of (a); (c) The authentication result of stego image 'Sailboat' with the pixel value at position (113, 1) changed from 172 to 173

shadow image. Based on the observation of the estimated *PSNR* value with fixed ratio, the larger c is, the larger *PSNR* is. However, the number of cover blocks decreases when c is increased. Since each block takes one check bit, the number of check bits is inversely proportional to the value of c. To enhance the authentication security, the number of check bits should be large enough with a proper choice of c. In our first experiment, the size of the cover image is 512×512, and (4, 16) hiding method is adopted. Therefore, there are 128×128 check bits of each stego image. In the second experiment, the size of the cover image is 384×256, and (4, 12) hiding method is adopted. Then, each stego image has 64×128 check bits. Actually, both 128×128 and 64×128 are large enough as the length of the check bits.

In steganography, the visual quality (usually evaluated by *PSNR* value) of the stego image is primarily concerned. The larger *PSNR* value reflects better visual quality of the stego image. In general, if the *PSNR* value is less than 35dB, some of the important characteristics may be lost. When the PSNR value is less than 30dB, the quality is visually unacceptable. In order to prevent attackers from visually distinguishing the difference between the cover image and the stego image, the *PSNR* value should be larger than 35dB. On the other hand, the size expansion of the stego image is secondarily concerned. Smaller size of the stego images is more convenient for storage and transmission. With acceptable visual quality, the size expansion of the stego image should be as small as possible. Let R be the size expansion of the stego image compared with the shadow image. The relationship of the estimated *PSNR* value and the size expansion of our scheme is shown in Fig. 8, where $s = 4$. As we can see, if the *PSNR* value is larger than 35dB, R should be at least 2.25. If we increase the *PSNR* value over 40dB, the size expansion should be larger than or equal to 2.75. Compared with the schemes of Lin and Tsai [12], Yang *et al.* [13] and Chang *et al.* [14], our scheme is better in both size expansion and visual quality of the stego images when $R = 3.25 \sim 3.75$. Note that, the size of each shadow image is $1/t$ of that of the secret image. Therefore, the size of each stego image is R/t of that of the secret image.

Although LSB substitution is vulnerable to resist stego-analysis, it still can get promising security. The threshold property of our scheme ensures that one can reconstruct the secret image from any t stego images. However, any $(t-1)$ or fewer stego images can reveal no information about the secret image.

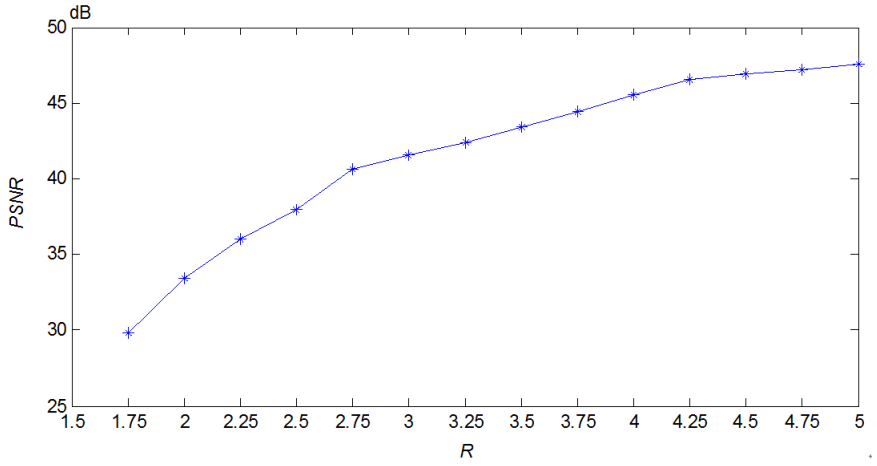

FIGURE 8. The diagram of estimated PSNR values (dB) with different size expansion R

6. **Conclusion.** In this paper, we present an enhanced image secret sharing and hiding scheme with authentication. The secret image is shared and hidden in ordinary cover images so as to be transmitted securely. The (s, c) hiding method based on *PSNR* estimation is introduced to hide each shadow image in a cover image. Compared with the schemes of Lin and Tsai, Yang *et al.* and Chang *et al.*[12-14], the size of the stego images doesn't have to be restricted to four times of the shadow images. The proposed scheme can optimize both the visual quality and the size expansion of the stego images. Furthermore, the authentication ability is enhanced by piecewise authentication method based on Hash function. The qualification of the stego images can be verified effectively.

Appendix A.

Proposition 3.1. Let A be the cover image. B is the corresponding stego image generated by m LSBs substitution. Then the estimated *MSE* between A and B is

$$MSE(m) = (2^{2m} - 1)/6$$

Poof. Let a be the decimal value of m LSBs of a cover pixel, $p_a(i)$ is the probability when $a = i$. By Assumption 1, we have $p_a(i) = 1/2^m, i \in \{0, 1, \ldots, 2^m - 1\}$. Let b be the decimal value of m secret bits, and $p_b(i)$ is the probability when $b = i$. Since secret bits are noise-like random bits, b satisfies uniform distribution, and $p_b(i) = 1/2^m, i \in \{0, 1, \ldots, 2^m - 1\}$. Because the 8-$m$ most significant bits of the cover pixel are not changed, the error between the cover pixel and the stego pixel is equal to the error between a and b. Let $p_{a-b}(x)$ be the probability when $a - b = x$, then we have

$$p_{a-b}(x) = \sum_{i-j=x} p_a(i) p_b(j)$$

Since $p_a(i) = p_b(i) = 1/2^m$, therefore

$$p_{a-b}(x) = (2^m - |x|)/2^{2m}, x \in \{0, \pm 1, \ldots, \pm(2^m - 1)\}$$

Then the probability of the square error is

$$p_{(a-b)^2}(x^2) = \begin{cases} 1/2^m & x = 0 \\ \frac{2^m - x}{2^{2m-1}} & x \in \{1, 2, \ldots, 2^m - 1\} \end{cases}$$

So the estimated mean square error is

$$MSE(m) = \sum_{x=0}^{2^m-1} x^2 p_{(a-b)^2}(x^2) = \sum_{x=1}^{2^m-1} x^2 \frac{2^m - x}{2^{2m-1}}$$

With further reduction, we have the estimated *MSE* value $MSE(m) = (2^{2m} - 1)/6$.

Appendix B

Proposition 3.3. MSE(m) and $MSE_{opt}(m)$ represent the *MSE* of simple m LSBs substitution and optimal m LSBs substitution, respectively. Then we have:

(a):

$$MSE(m_1) + MSE(m_2) + \cdots + MSE(m_n) \geq (n-b)MSE(a) + bMSE(a+1);$$

(b):

$$MSE_{opt}(m_1) + MSE_{opt}(m_2) + \cdots + MSE_{opt}(m_n) \geq (n-b)MSE_{opt}(a) + bMSE_{opt}(a+1);$$

where m_i is non-negative integer,$a = \lfloor Num/n \rfloor$,$b = Num \ mod \ n$, and $Num = m_1 + m_2 + \cdots + m_n$.

Proof. (a). First, let's consider the situation when $b = 0$. Let m be the average value of m_i, then $m = a$. If any $m_i < a$, there must be an $m_j > a$; otherwise, $m < a$. Since m_i and m_j are both integers, $m_j - m_i \geq 2$. It is easy to prove that $MSE(m_i) + MSE(m_j) \geq MSE(m_i + 1) + MSE(m_j - 1)$ by equation (5). Then, we can replace m_i and m_j by $m_i + 1$ and $m_j - 1$ to get smaller *MSE* value. Repeat the above process until no $m_i < a$. Since $m = a$, and $m_i \geq a$, then $m_i = a$, where $i = 1, \ldots, n$. Therefore, the summation of the *MSE* value is the smallest when each $m_i = a$.

Now consider the situation when $b \neq 0$. We have $a < m < a + 1$. If any $m_i < a$, there must be an $m_j \geq a + 1$; otherwise, $m < a$. Then we have $m_j - m_i \geq 2$. It is also easy to prove that $MSE(m_i) + MSE(m_j)MSE(m_i + 1) + MSE(m_j - 1)$ by equation (5). Then replace mi and m_j by $m_i + 1$ and $m_j - 1$ to get smaller *MSE* value. If any $m_i > a + 1$, there must be an $m_j \leq a$; otherwise, $m > a + 1$. Then we have $m_i - m_j \geq 2$. It is also easy to prove that $MSE(m_i) + MSE(m_j) \geq MSE(m_i - 1) + MSE(m_j + 1)$. Then replace m_i and m_j by $m_i - 1$ and $m_j + 1$ to get smaller *MSE* value. Repeat the replacing process until no $m_i < a$ and no $m_i > a + 1$. Hence, m_i is equal to a or $a + 1$. Suppose the number of m_i equaled to a is x, then the number of m_i equaled to $a + 1$ is $n - x$. So, we have $a \cdot x + (n - x) \cdot (a + 1) = a \cdot n + b$. By solving this equation, we have $x = n - b$. That is to say, with $n - b$ of mi equaled to a, and the others m_i equaled to $a + 1$, we can get the smallest summation of the *MSE* value.

(b). The proof of (b) is similar to the proof of (a), and omitted here.

Acknowledgment. This work is partially supported by the Fundamental Research Funds for the Central Universities (No.13MS107). The authors also gratefully acknowledge the helpful comments and suggestions of the reviewers, which have improved the presentation.

REFERENCES

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

[2] M. Naor, and A. Shamir, Visual cryptography, *Proc of Advances in Cryptology: Eurpocrypt'94*, LNCS 950, pp. 1-12, 1995.

[3] C. C. Lin, and W. H. Tsai, Visual cryptography for gray-level images by dithering techniques, *Journal of Pattern Recognition Letters*, vol. 24, no. 1-3, pp. 349-358, 2003.

[4] C. N. Yang, and T. S. Chen, Colored visual cryptography scheme based on additive color mixing, *Journal of Pattern Recognition*, vol. 41, no. 10, pp. 3114-3129, 2008.

[5] J. B. Feng, H. C. Wu, C. S. Tsai, Y. F. Chang, and Y. P. Chu, Visual secret sharing for multiple secrets, *Journal of Pattern Recognition*, vol. 41, no. 12, pp. 3572-3581, 2008.
[6] C. C. Thien, and J. C. Lin, Secret image sharing, *Journal of Computer & Graphics*, vol. 26, no. 5, pp. 765-770, 2002.
[7] J. B. Feng, H. C. Wu, C. S. Tsai, and Y. P. Chu, A new multi-secret images sharing scheme using Largrange's interpolation, *Journal of Systems and Software*, vol. 76, no. 3, pp. 327-339, 2005.
[8] R. Z. Wang, and C. H. Su, Secret image sharing with smaller shadow images, *Journal of Pattern Recognition Letters*, vol. 27, no. 6, pp. 551-555, 2006.
[9] Y. S. Wu, C. C. Thien, and J. C. Lin, Sharing and hiding secret images with size constraint, *Pattern Recognition*, vol. 37, no. 7, pp. 1377-1385, 2004.
[10] P. Y. Lin, J. S. Lee, and C. C. Chang, Distortion-free secret image sharing mechanism using modulus operator, *Journal of Pattern Recognition*, vol. 42, no. 5, pp. 886-895, 2009.
[11] P. Y. Lin, and C. S. Chan, Invertible secret image sharing with steganography, *Journal of Pattern Recognition Letters*, vol. 31, no.13, pp. 1887-1893, 2010.
[12] C. C. Lin, and W. H. Tsai, Secret image sharing with steganography and authentication, *The Journal of Systems and Software*, vol. 73, no. 3, pp. 405-414, 2004.
[13] C. N. Yang, T. S. Chen, K. H. Yu, and C. C. Wang, Improvements of image sharing with steganography and authentication, *The Journal of Systems and Software*, vol. 80, no. 7, pp. 1070-1076, 2007.
[14] C. C. Chang, Y. P. Hsieh, and C. H. Lin, Sharing secrets in stego images with authentication, *Journal of Pattern Recognition*, vol. 41, no. 10, pp. 3130-3137, 2008.
[15] Z. Eslami, S. H. Razzaghi, and J. Z. Ahmadabadi, Secret image sharing based on cellular automata and steganography, *Journsl of Pattern Recognition*, vol. 43, no. 1, pp. 397-404, 2010.
[16] C. C. Wu, M. S. Hwang, and S. J. Kao, A new approach to the secret image sharing with steganography and authentication, *Imaging Science Journal*, vol. 57, no. 3, pp. 140-151, 2009.
[17] C. Guo, and C. C. Chang, A construction for secret sharing scheme with general access structure, *Journal of Information Hiding and Multimedia Signal Processing*, vol. 4, no. 1, pp. 1-8, 2013.
[18] Q. Kong, P. Li, and Y. Ma, On the feasibility and security of image secret sharing scheme to identify cheaters, *Journal of Information Hiding and Multimedia Signal Processing*, vol. 4, no. 4, pp. 225-232, 2013.
[19] C. S. Chan, C. C. Chang, and H. P. Vo, A user-friendly image sharing scheme using JPEG-LS median edge predictor, *Journal of Information Hiding and Multimedia Signal Processing*, vol. 3, no. 4, pp. 340-351, 2012.
[20] C. K. Chan and L. M. Cheng, Hiding data in images by simple LSB substitution, *Journal of Pattern Recognition*, vol. 37, no. 3, pp. 469-474, 2004.
[21] A. Weber: 'The USC-SIPI Image Database', University of Southern California, Available at http://sipi.usc.edu/database/, 2010.