An Adaptive Technique for the Steganography in Spatial Domain

Der-Chyuan Lou and Jiang-Lung Liu

Department of Electrical Engineering
Chung Cheng Institute of Technology
Tahsi, Taoyuan 33509, Taiwan, R.O.C.
E-mail: dclou@ccit.edu.tw

Abstract

With the increasing computational capability of computer, the security of data transmission in computer network has been threatened. To meet the requirement of computational security, traditional cryptosystems have to keep lengthening the key-size. By applying the data hiding technique, this problem can be tackled. Secret hiding, one of the applications of data hiding, is a technique to hide the encrypted data, called secret, into a cover image to avoid passive cryptanalysis. The challenge of this kind of technique is how to hide as much secret as possible in the cover image while the embedded image, called stego-image, is visually acceptable. In this paper, we propose an n-LSB based secret hiding system (SHS). In the SHS, an enhanced n-LSB hiding method, called dynamic n-LSB, is used to improve the quality of stego-images. An important transformation function has derived from the Gaussian noise model. It provides a theoretical method to obtain the optimum value of n that leads to a better quality of stego-images for the dynamic n-LSB method. With the transformation function, the capacity of secret hiding is also concluded.

Keywords: *Image processing, information hiding, Gaussian noise, cryptography, steganography.*

1 Introduction

Computer network has improved our communication quality but has also incurred some problems. One of the bothering problems is the security of transmission. Many cryptosystems such as DES and RSA [8] have been proposed to protect the security of data through the encryption/decryption process. The characteristic of these schemes is that the encrypted data are presented as a bunch of messy and meaningless ones. When these data are transmitted through the network, they may pique the interest of illegal users and invite active cryptanalysis. With the increasing computational capability of computer, these cryptosystems have to lengthen the key-size to maintain their so-called computational security [8]. Recently, this situation is improved via data hiding technique [1].

Data hiding, a form of *steganography*, embeds data into digital media for different purposes such as copyright protection and tamper proofing [5]. An application of data hiding is *secret hiding*. In this application, a desired data is hidden in a *cover image* [5] to form another meaningful image (called *stego-image* [5]). The stego-image is then transmitted on the computer network. Since the stego-image is a meaningful image, once it is intercepted it must be ignored if it is visually irrelevant to the illegal users. Recently, Cheng and Chang had proposed a VQ-based data hiding scheme [3] for image hiding. In [3], a forged image is first divided into several equal-sized image blocks to form a codebook. With the codebook, the desired image is coded to the distorted forged image. This idea is novel, while the performance and overhead are need to be dealt with. Besides, this method is dedicated to an image file. In fact, any LSB method [5,10], which simply hides the data in the least significant bits of an image's pixels, can be applied to this kind of applications. There are enough reasons for us to construct the LSB-based data hiding system, called *secret hiding system* (SHS), for secret communication:

- All kinds of data can be the input of the SHS.
- In the SHS, the cover image can be "thrown" away after the embedded data had been extracted. This implies that we can use not only the least significant bits but also the lower significant bits (called n-LSB) to hide data although this may leads to more distortions.
- The embedded data is supposed to be an encrypted one. That is, if the encrypted data is detected, it reveals nothing about the secrets.
- LSB method is easy to be implemented by hardware. This makes it possible to cooperate with the existing encryption/decryption chip to form another powerful chip for secret communication.

The most important thing in constructing a secret hiding system is to decide how many lower significant bits can be used for data hiding. To answer this question, the PSNR [4] value can be taken as a performance metric. In general, it is said visually acceptable if the PSNR of a stego-image is greater than 30 dB, otherwise it is unacceptable. Based on this measure, if we insert data directly into n-LSB, called direct n-LSB, in the worst case (i.e. we have maximum 2^n-1 error in n-LSB), the PSNRs of the stego-images are 31.23 dB, 24.61 dB, and 18.30 dB corresponding to n=3, 4, and 5. Clearly, the direct 3-LSB method works in the SHS. In the SHS, we want to hide as much secret as possible in the n-LSB. With this desire, a major problem arises: what is the capacity limitation of n-LSB in the SHS? In this paper, we solve this problem in an elegant way.

In this paper, we propose an n-LSB based secret hiding system. In the SHS, an enhanced n-LSB hiding method, called dynamic n-LSB, is developed to improve the quality of stego-images. An important transformation function is derived from the *Gaussian noise* model. It provides a theoretical method to obtain the optimum value of n that leads to a better quality of stego-images for the dynamic n-LSB method. With the transformation function, the capacity of secret hiding is also concluded.

The rest of this paper is organized as follows. In Section 2, the secret hiding system and several parameters used in this paper are defined. A dynamic and *lossless* n-LSB method is proposed in Section 3. In Section 4, the capacity issue is addressed based on the dynamic n-LSB method. The security analyses of the secret hiding system are discussed in Section 4. Section 5 concludes this work.

2 The System Model

2.1 Secret Hiding System

The block diagram of the secret hiding system is shown in Fig. 1. It includes a hiding stage and an extraction stage, both can be divided respectively into two steps: data-encryption and secret-insertion in hiding stage, secret-extraction and secret-decryption in extraction stage.

In the data-encryption step of the hiding stage, any secure cryptosystem such as DES, RSA etc. can be used to encrypt the original data for preventing the active cryptanalysis. Many cryptosystems for text (e.g. [8]) or image (e.g. [2]) can be applied to ensure that the encrypted data (i.e. secret) is computationally secure (further security analysis is discussed in Section 4). In a trusted cryptosystem, the secret is distributed uniformly so that it can resist statistic attack. Hence, in this paper, the secret is treated as a random variable with uniform distribution hereafter.

In the secret-insertion step of the hiding stage, the secret is considered as a bit stream which is transformed (see Subsection 2.5) into an array of n-bit elements. The secret array is then, if necessarily, expanded (see Subsection 2.5) and inserted into a cover image. The transformation function is used to transform the "unnatural" stego-image into a reasonable one, which has better quality (visually or theoretically) than the "unnatural" one. The transformation function is the kernel of our dynamic n-LSB method (see Section 3).

The transformed stego-image must be lossless in the transmission for the integrity of embedded secret. Thus, the secret-extraction process is only to separate the secret from the n-LSBs of the stego-image. Then, the secret array is converted to a bit stream so that the original data can be decrypted by the used cryptosystem.

2.2 Pixel Array

An image of size $M \times N$ can be represented as an array I_P of size $M \times N$:

$$I_P = \{P_i : P_i \in \{0,1,\Lambda\ ,2^{b_P}-1\},\ i = 1,2,\Lambda\ ,M \times N\}, \quad (1)$$

where P_i is the light intensity of pixel i with b_P bits. The space for storing P_i varied from image to image. Except the true-color image, P_i is usually encoded as the index of the color plate to save the space of storage. A "color" in a color plate can be represented with 3 bytes. Each byte represents one of the blue, red, and green components of light intensity. For an 8-bit gray-level image, there are 256 "colors" in the color plate with continuous gray levels between black (index 0) and white (index 255). With the continuous color plate, the indices of 8-bit gray-level image can be altered and still visually acceptable. For this reason, images, except the 8-bit gray-level ones, are not recommended as cover images unless continuous color plates are used. In this paper, the cover image is referred to as an 8-bit gray-level image.

2.3 Hiding Capacity

Let a cover image I_Q having q pixels. Each of these pixels has a gray value represented by b_Q bits, which can be defined as

$$I_Q = \{Q_i : Q_i \in \{0,1,\Lambda\ ,2^{b_Q}-1\},\ i = 1,2,\Lambda\ ,q\}. \quad (2)$$

A data array I_R with r elements. Each of these elements is represented with b_R bits, which can be expressed as

$$I_R = \{R_j : R_j \in \{0,1,\Lambda\ ,2^{b_R}-1\},\ j = 1,2,\Lambda\ ,r\}. \quad (3)$$

Let I_R be the secret and $r \le q$, the hiding ratio of I_R and I_Q is defined as follows,

$$HR = \begin{cases} \dfrac{r \times b_R}{q \times b_Q}, & \text{if } r < q; \\ \dfrac{b_R}{b_Q}, & \text{if } r = q. \end{cases} \quad (4)$$

Note that if $r = q$, the hiding ratio is said to be *static*. On the other hand, the hiding ratio is said to be *dynamic* if $r < q$. The hiding factor β is specifically used to denote the static hiding ratio instead of *HR* in the SHS. In this case, the *hiding capacity* is equivalent to the hiding factor.

2.4 n-LSB Insertion

A t-bit data X^t can be divided into two parts: m higher bits X^{m+} and n lower bits X^{n-}, i.e.,

$$X^t = X^{m+} + X^{n-}, \quad (5)$$

where $X^{m+} \in \{2^n, 2^n+1, \Lambda\ ,2^t-1\}$, $X^{n-} \in \{0,1,\Lambda\ ,2^n-1\}$, and $m+n=t$. Given an n-bit data Y^n, the process inserting Y^n into X^t is defined as

$$X^* = X^{m+} + Y^n, \quad (6)$$

where X^* is the result of the insertion.

2.5 Secret insertion

By Eqs. (1) and (5), the 8-bit gray-level cover image I_C of size $M \times N$ can be represented as

$$I_C = \{C_i : C_i = C_i^{m+} + C_i^{n-},\ i = 1,2,\Lambda\ ,M \times N\}, \quad (7)$$

where $C_i^{m+} \in \{2^n, 2^n+1, \Lambda\ ,255\}$ and $C_i^{n-} \in \{0,1,\Lambda\ ,2^n-1\}$. Here, $m+n=8$, C_i^{m+} and C_i^{n-} denote the m higher bits and n lower bits of C_i, respectively. In the SHS, the secret S can be considered as a bit stream of length L_S. To be hidden in the $M \times N$ cover image I_C, the secret S is first converted into an array with k elements of n bits as

$$I_S = \{S_i : S_i \in \{0,1,\Lambda\ ,2^n-1\},\ i = 1,2,\Lambda\ ,k\}, \quad (8)$$

where $n \le t$, $k = L_S / n$, and $k \le M \times N$. Then, an expansion function f_E is applied to insert the I_S into a cover image I_C. This process is formulated as follows:

$$I_O = \{O_j : O_j = C_j - C_j^{n-} + S_i,\ j = f_E(i), i = 1,2,\Lambda\ ,k\}, \quad (9)$$

where I_O is the stego-image. The purpose of applying expansion function is to spread the elements of I_S randomly and uniformly in the n-LSB of elements of I_C. This measure can equalize the visual distortion of a whole image when the size of I_S is smaller than that of I_C (i.e. $k < M \times N$). Of course, if $k = M \times N$, the expansion process can be neglected and the elements of I_S is directly insert in the n-LSB of the elements of I_C. Thus, the embedding process can be formulated according to the definition of Eq. (7) as:

$$I_O = \{O_i : O_i = C_i - C_i^{n-} + S_i, i = 1,2,\Lambda\ ,M \times N\}. \quad (10)$$

Many useful methods can be used to construct the expansion function. A simple one is the look-up table method, which builds up a look-up table in the SHS to allocate the positions of I_C in the expansion process. Although this method is quick, it is space consuming. Another useful expansion function is the *toral automorphism* [9].

Two stego-images (see Figs. 2(b) and 2(c)) are created by applying two hiding factors $\beta = 0.5$ (i.e. 4/8) and $\beta = 0.625$ (i.e. 5/8) to illustrate the effects of the secret insertion process. In these figures, the expansion process is omitted since I_C and I_S have the same size. Two arrays of size 65536 with 4-bit and 5-bit elements in them are first randomly generated to simulate the random secret. The two secrets are then inserted into the same gray-level image (shown in Fig. 2(a)) of size 256×256 to create the two stego-images, as Figs. 2(b) and 2(c). Note that a kind of low-quantization-like distortion is perceptible in both stego-images. This kind of distortion can be observed from the discontinue portion of an image, and becomes more obvious as β increase. For an 8-bit gray-level image, this kind distortion is considered being "unnatural" and referred to as "suspected" (i.e. the cover image is invalid). In the next section, a noise-based secret hiding method called dynamic *n*-LSB is proposed to improve this problem.

3 Dynamic *n*-LSB (A Noise-based Method)

3.1 Noise model

In the SHS, a stego-image I_O can be considered as a mixture of a cover image I_C and an unpredictable noise

$$I_N = \{N_i : N_i \in \{0,1,\Lambda\ ,2^n - 1\},\ i = 1,2,\Lambda\ ,M \times N\}, \quad (11)$$

i.e.,

$$I_O = \{O_i : O_i = C_i + N_i, i = 1,2,\Lambda\ ,M \times N\}. \quad (12)$$

Let I_E be the set of *n*-LSB of elements of I_O, the Eqs. (9) and (10) can be normalized as

$$I_O = \{O_i : O_i = C_i - C_i^{n-} + E_i, i = 1,2,\Lambda\ ,M \times N\}. \quad (13)$$

From Eqs. (12) and (13), the additional noise can be derived as:

$$I_N = \{N_i : N_i = E_i - C_i^{n-},\ i = 1,2,\Lambda\ ,M \times N\}. \quad (14)$$

According to Eq. (14), the additional noise can be derived; and its histogram is shown in Fig. 3(a). The distribution of this additional noise, called *direct n*-LSB noise which is malapportioned as compared with the *Gaussian noise* [6]. For comparison, a Gaussian noise with standard deviation σ = 16/3 is generated and its histogram is shown in Fig. 3(b). Clearly, the distribution of Gaussian noise is more concentrated inside [-σ, σ] and sparser outside [-2σ, 2σ] than the *n*-LSB noise (numerical comparasions are shown in Table 1). According to Figs. 3(a) and 3(b), it is clear that the stego-image with Gaussian noise has higher PSNR [4] than the one with *n*-LSB noise. The comparison of PSNR of these two kinds of noise is shown in Table 2. In the next subsection, the transformation function is proposed to adjust the distribution of the *n*-LSB noise so that the transformed distribution is similar to that of Gussian noise. With this adjustment, the visual and theoretical quality of the stego-image can be improved.

3.2 Transformation Function

A ***Gaussian noise*** [6] is a random variable having normal distribution and zero mean. According to the *probability density function* of Gaussian noise, no more than 5% of elements fall outside the range of [-2σ, 2σ] and at least 68% of elements fall inside the range of [-σ, σ]. Here σ is the *standard deviation*. According to Table 1, we found that for the direct *n*-LSB noise, most elements fall outside [-2σ, 2σ] and not many in [-σ, σ]. To adjust the distribution of the direct *n*-LSB noise so that it has the similar distribution of the Gaussian noise, a transformation function is defined as follows

$$I_O = T_\delta(I_O) = \begin{cases} O_i - 2^n, & \text{if } N_i \geq \delta \text{ and } O_i \geq 2^n; \\ O_i + 2^n, & \text{if } N_i \leq -\delta \text{ and } O_i \leq 255 - 2^n; \\ O_i, & \text{otherwise,} \end{cases} \quad (15)$$

where $i = 1,2,\Lambda\ ,M \times N$, δ is the *transformation factor* and $2^{n-1} < \delta < 2^n$. Note that the transformed stego-image must be lossless in the transmission for the integrity of secret. It guarantees that all the original data can be restored correctly in the decryption process, even if a public-key cryptosystem [8] is used.

To observe the effects of various δ's, the direct 4-LSB stego-image Fig. 2(c) is transformed by applying various δ's, where $8 < \delta < 15$. The PSNR curve of the transformed stego-image versus δ is shown in Fig. 4. The horizontal curve in Fig. 4 represents the PSNR of the stego-image with Gaussian noise of $\sigma = 16/3$. Note that the closest point of the "Gaussian" and the "transformed 4-LSB" lines occurs in the region between $\delta = 10$ and $\delta = 11$ ($\approx 2\sigma$). It implies that we may have the Gaussian-like distribution if $\delta = 2\sigma$ is taken as the transformation factor. The distributions of the direct 4-LSB noises with various δ's are shown in Table 1. From Table 1, it is clear that when $\delta = 11$ ($\approx 2\sigma$), the transformed 4-LSB noise has the Gaussian-like distribution.

3.3 Dynamic Application

The term "*dynamic n*-LSB" means we can apply various δ's to obtain stego-images of improved quality. From Fig. 4, we can find that for each δ where $2^{n-1} < \delta < 2^n$, the PSNR of the transformed stego-image is better than the direct *n*-LSB stego-image. The proof is trivial and is left to the reader.

For $n < 5$, δ should be selected between $[2^{n-1}, 2\sigma]$ to have a better quality of the transformed stego-image since it has concentrated distribution in [-σ,σ]. If we select $\delta \approx 2\sigma$, we have the Gaussian-like noise. While $n \geq 5$, a static transformation factor $\delta = 2^{n-1}$ is suggested to get the best quality of the stego-image since all the stego-images' PSNRs are lower than 30 dB for any δ. For example, Fig. 2(d) is a transformed 5-LSB stego-image with PSNR=28.82 dB by applying $\delta = 16$. Note that the low-quantization-like distortion, which is prominent in Fig. 2(c), becomes imperceptible and the quality is acceptable as shown in Fig. 2(d) even though the PSNR is lower than 30 dB. For general usage, the transformed 5-LSB is not recommended because of theoretically low PSNR even though visually acceptable.

4 Capacity, Security, and Performance Analyses

4.1 Capacity

The transformation function can be considered as a specific filter in the space domain. By using the dynamic n-LSB method, all the elements of noise outside $[-2^{n-1}, 2^{n-1}]$ can be converted to the ones inside $[-2^{n-1}, 2^{n-1}]$. In the worst case, by applying $\delta = 2^{n-1}$, the PSNRs of the transformed stego-images are 38.59 dB, 31.23 dB, and 24.61 dB corresponding to n=3, 4, and 5, respectively. Clearly, in any case, the transformed 4-LSB is work in the SHS because of the high PSNR of the stego-image. To this, we can conclude that the hiding capacity is 0.5 in the SHS with static hiding ratio. As to the transformed 5-LSB, we won't recommend it in the usage of static hiding ratio.

4.2 Security Analysis

As mentioned in Section 2.1, the n-LSB method cannot avoid active cryptanalysis. It is reasonable that the security of the SHS is equivalent to that of the used cryptosystem. Several existing cryptsystems can be applied to data encryption. In general, the asymmetrical cryptosystems are time consuming comparing to the symmetrical ones [8]. Hence the symmetrical cyrptosystems are recommended if there are a lot of data must be hidden. The stream cipher system [7] encrypts data bit-wise with a key stream is considered as a good cryptosystem in the SHS because of the properties of easy designing and cheap hardwiring. The other reason for preferring stream cipher system to others is that it is more secured than DES in encrypting image data if the image has much redundant data.

4.3 Performance Analysis

The transformation function proposed in Section 2.4 is simple and easy to be implemented by either software or hardware. The performance of the proposed expansion function depends on the method used. An associative look-up table can be used to design a fixed and fast expansion operator. Furthermore, it is possible to hardwire the encryption and the secret hiding simultaneously by using the pipelining technique since all the processes from encryption to transformation are proceeded sequentially.

5 Conclusions

In this paper, an n-LSB based secret hiding system has been proposed. A transformation function in dynamic n-LSB has been derived based on Gaussian noise model. By selecting the transformation factor, a direct n-LSB stego-image can be transformed to get a better quality. Theoretically and experimentally, the proposed dynamic n-LSB can improve the quality of the direct n-LSB stego-image by applying proper transformation factor. Based on the transformation function, the hiding capacity is derived and concluded to 0.5 in the SHS with static hiding ratio. Future work may include the designs and implementations of dynamic secret hiding and secret hiding techniques for color images.

Acknowledgments

This research was supported in part by the National Science Council of the Republic of China under grant NSC 88-2213-E-014-002.

References

[1] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding," *IBM Systems Journal*, vol. 35, nos. 3 and 4, pp. 313-336, 1996.

[2] H. K.-C. Chang and J.-L. Liu, "A linear quadtree compression scheme for image encryption," *Signal Processing: Image Communication*, vol. 10, pp. 279-290, 1997.

[3] T.-S. Chen and C.-C. Chang, and M.-S. Hwang, "Virtual image cryptosystem based upon vector quantization," *IEEE Transactions on Image Processing*, vol. 7, no. 10, pp. 1485-1488, Oct. 1998.

[4] R. C. Gonzalez and R. E. Woods, *Digital Image Processing*, Addison-Wesley, New York, 1992.

[5] N. F. Johnson and S. Jajodia, "Exploring steganography: seeing the unseen," *IEEE Computer Magazine*, vol. 31, no. 2, pp. 26-34, Feb. 1998.

[6] E. A. Lee and D. G. Messerschmitt, *Digital Communication*, Kluwer Academic, Boston, 1988.

[7] M. Y. Rhee, *Cryptography and Secure Communications*, McGraw-Hill, Singapore, 1994.

[8] J. Seberry and J. Pieprzyk, *CRYPTOGRAPHY: An Introduction to Computer Security*, Prentice-Hall, New York, 1989.

[9] G. Voyatzis and I. Pitas, "Applications of toral automorphisms in image watermarking," *Proceedings of the 1996 IEEE International Conference on Image Processing*, vol. 2, Sep. 1996, pp. 237-240.

[10] S. Walton, "Image authentication for a slippery new age," *Dr. Dobb's Journal*, vol. 20, no. 4, pp. 18-26, Apr. 1995.

Table 1 Distribution of various noises with standard deviation $\sigma = 16/3$.

	Guassian	Direct 4-LSB	4-LSB (δ=9)	4-LSB (δ=10)	4-LSB (δ=11)	4-LSB (δ=12)	4-LSB (δ=13)	4-LSB (δ=14)
$\|I_O\| \le \sigma$	69.90%	56.46%	68.61%	68.42%	64.53%	61.27%	58.88%	57.21%
$\|I_O\| > 2\sigma$	4.84%	11.96%	-	-	3.89%	7.14%	9.54%	11.21%

Table 2 Comparisons of PSNR in various conditions.

n	Direct n-LSB	Gussian	Transformated n-LSB ($\delta \approx 2\sigma$)
3	37.9161	39.5389	38.5816
4	31.7933	33.5808	33.3389
5	25.4843	27.5283	27.4007

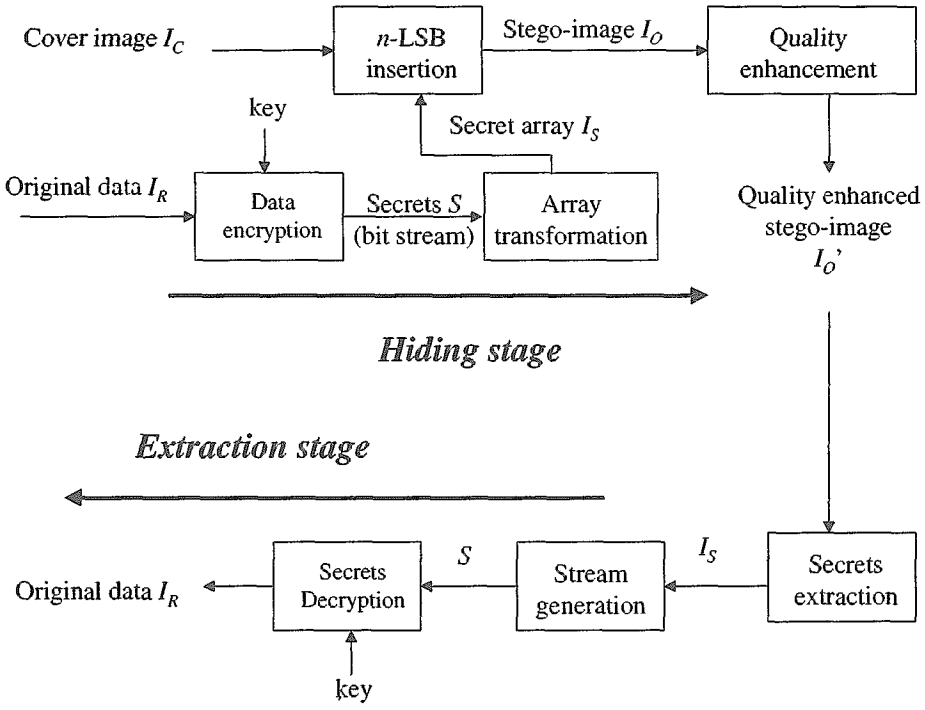
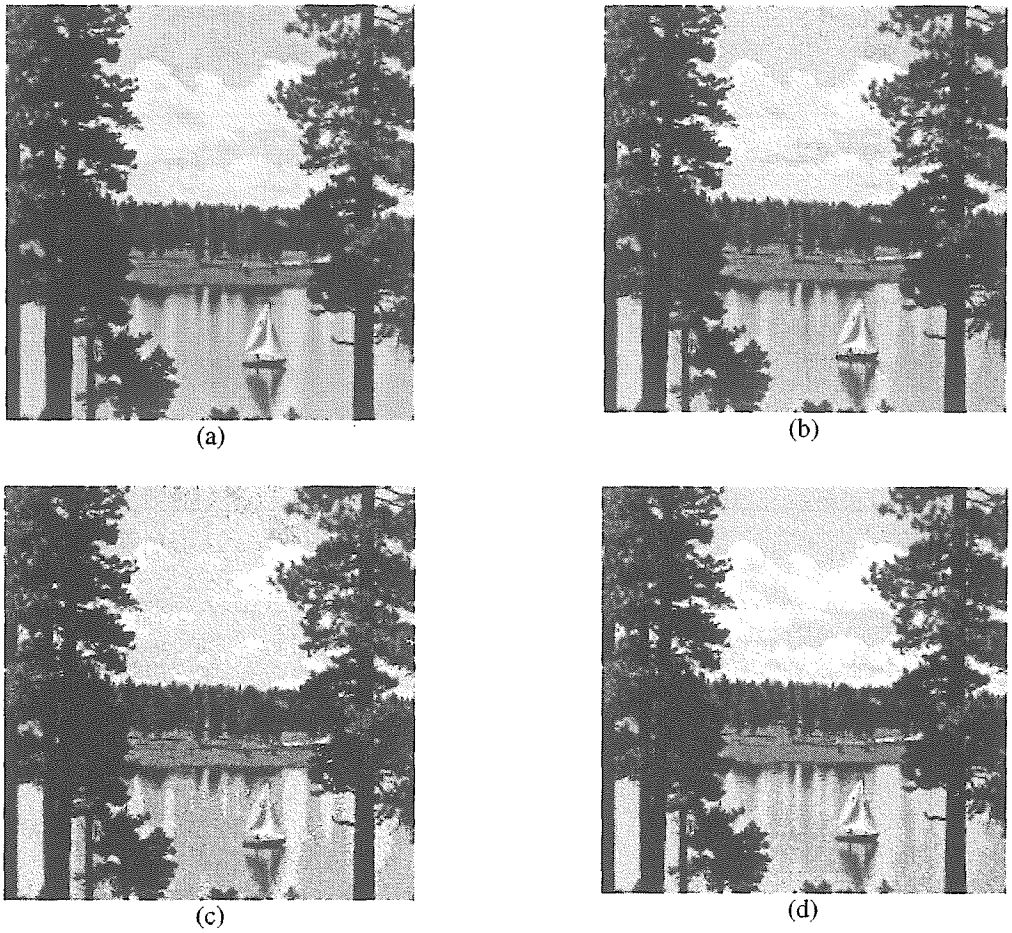
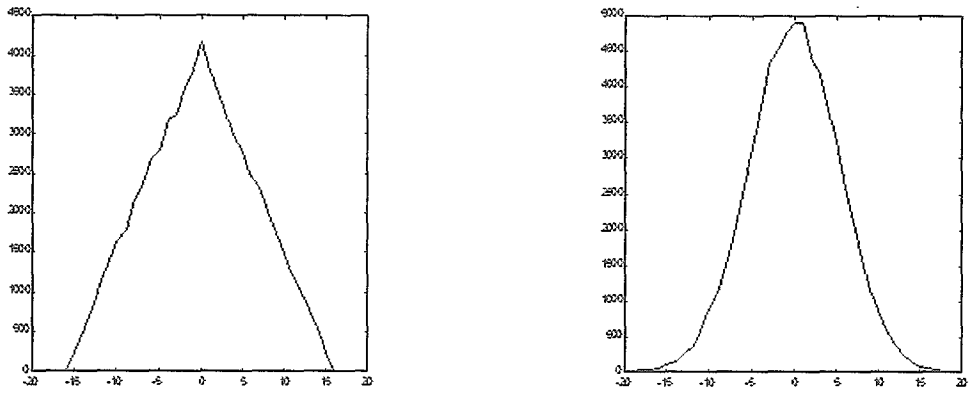


Fig. 1. The hiding process and extraction process of the SHS.



(a) (b) (c) (d)

Fig. 2. (a) A 256 gray-level cover image of size 256×256;
(b) a direct 4-LSB stego-image;
(c) a direct 5-LSB stego-image (PSNR=25.48 dB).
(d) an improved stego-image by applying a static transformation factor $\delta = 16$ (PSNR=28.82 dB).



(a) (b)

Fig. 3. (a) The histogram of the direct 4-LSB method's noise;
(b) the histogram of a Gaussian noise with standard deviation $\sigma = 16/3$ and zero mean.

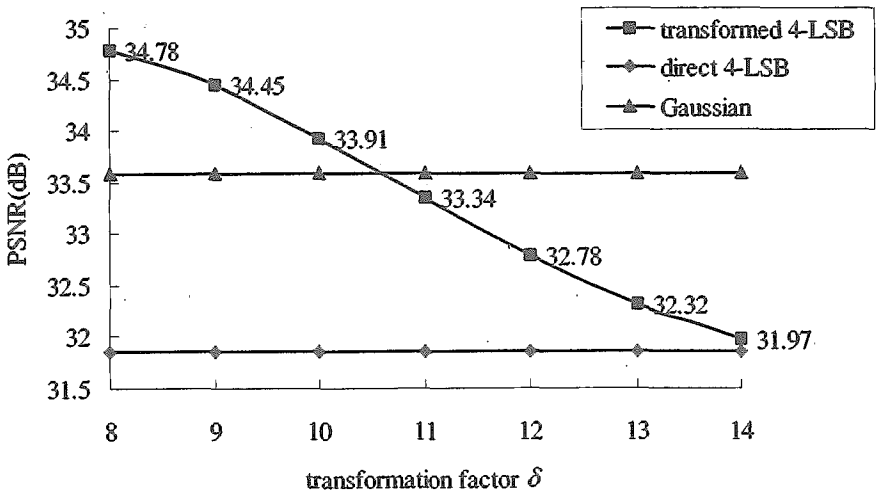


Fig. 4. Comparisons of PSNR in various noise conditions.