Data Hiding: Current Status and Key Issues *

Nan-I Wu[†] Chung-Ming Wang [†] Min-Shiang Hwang[‡]

Institute of Computer Science [†]
National Chung Hsing University
250 Kuo Kuang Road, Taichung, Taiwan 402, R.O.C.
Department of Management Information Systems [‡]
National Chung Hsing University
250 Kuo Kuang Road, Taichung, Taiwan 402, R.O.C.
Email:mshwang@nchu.edu.tw
Tel:886-4-22855401
Fax: 886-4-22857173

April 3, 2006

Data Hiding: Current Status and Key Issues

*

[‡]Responsible for correspondence: Prof. Min-Shiang Hwang

Abstract

Image steganography is a covert communication method that uses an image as the cover to hide the truth from potential attackers that some secret message hidden in the image is being transported. When we appreciate the astonishing beauty of a world famous picture in its digital form on the computer, it is hard to imagine that the picture might actually be working as a messenger, carrying some invisible important secret message along with it. In other words, steganography is a collection of cryptographic techniques that provide protection to the secret message by offering it the appearance of an image. In this survey paper, our focus is on the development and current status of steganographic techniques for grayscale images. We shall separately introduce schemes with high hiding capacities and schemes with high imperceptibility. The advantages and disadvantages of those schemes will be closely analyzed, offering directions for our future research efforts.

Keywords: Steganography; data hiding; secure communication; hidden capacity; imperceptible

1 Introduction

1.1 Motivation

Nowadays, thanks to the stunningly fast advancement of the computer and network technology, people can easily send or receive secret information in various forms to or from almost any remotest part of the world through the Internet within seconds. In fact, there might be tons of secret information being transmitted and exchanged on the Internet at this particular point of time. However, important secret messages may run high risks of leaking out while they are being transmitted or exchanged over some public communication channel. Therefore, how to achieve safe secret communication is an important field of research. Traditionally, before it is sent out through the Net, by using a cryptographic technique such as DES or RSA, a private message can be encrypted into some ciphertext that appears totally meaningless.

Though modern cryptographic systems offer quite high a security level to the secret information transmitted and exchanged on the Net, the secret information's appearances as ciphertexts readily draw hackers' attention as though proclaiming that some secret messages of especially high value could be obtained if the ciphertexts could only be in one way or another decrypted. Under such circumstances, even though chances are that the hackers are probably not able to decrypt the ciphertexts due to the strong security the cryptographic system offers, at least the irritated attackers can easily destroy the ciphertexts and make the transmissions fail. As a result, it seems that the best policy of ensuring the security of secret information traveling on the Internet is to avoid any attention and suspicion of the hacker. That is to say, the safest method to keep messages transmitted through open channels from leaking out is to encrypt them into a meaningful content (i.e. plaintext), and this is where steganography/data hiding comes into play.

1.2 History of Steganography

Steganography/Data hiding is a secure communication method that conveys secret messages in the form of plaintexts so that the appearances of the secret messages will not draw eavesdroppers' attention while they are being transmitted through an open channel. The word steganography, which is composed of the two Greek words *steganos* and *graphia*, means "hidden writing" or "covered writing." The earliest study concerning modern steganography was presented by Simmons in 1983 [15]. In [15], the story of $Prisoners'\ Problem$ explains what capabilities and merits steganography has to offer when the public communication channel is insecure. The story is about two prisoners Bob and Alice who are put to different cells in jail and want to escape from prison together. However, any communications between them have to be inspected strictly by Willie the warden. Besides, only plaintexts (i.e. contents that have clear meanings to anyone and everyone) can pass the security inspection, while anything in the form of a ciphertext (i.e. a content that seems totally meaningless to most people) will not be allowed. Under such circumstances, Bob and Alice want to conspire to escape, but they can of course not send a clear message to each other showing the intention of escaping, and neither can they encrypt the secret message about their plan of escape into a ciphertext in an attempt to hide their intention before the message comes to the warden.

To solve this prisoners' problem, many kinds of plaintexts, such as digital images, audios, videos, etc., can be used as the cover to conceal the very existence of the secret message from the inspector. Among the wide variety of plaintext formats, digital images are the most commonly used because they are the most ubiquitous and readily available on the Internet. In addition, the higher degree of distortion tolerance that digital images have over other kinds of plaintext data provides them with a larger hiding capacity. Therefore, in the past decade, many data hiding schemes have been proposed especially for digital images as the cover media. In general, an image before any secret data gets hidden in is called a cover image, and the term stego-image is for an image with the secret message already embedded in.

1.3 Requirements That Steganographic Schemes should satisfy

Generally speaking, a steganographic technique is usually evaluated in two aspects:

- Imperceptibility/Stego-image quality: How to preserve the details of the cover image when the secret message is being embedded in so that the differences between the stego-image and the cover image can be perfectly imperceptible to the human eye is the very first problem an ideal steganographic scheme has to face. As we all know, the higher the stego-image quality, the more invisible the hidden message. Therefore, the stego-image quality is a very important criterion to use when we evaluate the performance of a steganograpnic technique. We can judge whether the stego-image quality is acceptable to the human eye by using the Peak Signal-to-Noise Ratio (PSNR), whose formula is as follows:

  $$PSNR = 10\ log_{10}\ \frac{255^2}{MSE}\ dB$$

  and

  $$MSE = (\frac{1}{M \times N}) \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} (P(x,y) - P'(x,y))^2$$

  where M and N represent the image size. In the formula, $P(x,y)$ stands for the original pixel value, and $P'(x,y)$ represents the pixel value in position (x,y) with the secret data already hidden in. A greater PSNR value means a lower degree of image distortion after the hiding of the secret data. For example, given a grayscale image as the cover image to hide secret data in, it is hard for any human being to perceive any difference between the cover image and the stego-image if the PNSR value of the stego-image goes beyond 36 dB.

- Payload/Hiding capacity: The payload indicates the maximum number of bits that can be hidden with an acceptable resultant stego-image quality. Because the scheme would be of no value if the stego-image turned out seriously distorted despite the fact that it can hold a large amount of secret data, the hiding capacity does have its limit, especially when it comes to the binary image. We can say that a scheme does have its contribution to this field of research if it proves to either increase the payload while maintaining an acceptable stego-image quality or improve the stego-image quality while keeping the hiding capacity at the same level, or better if it can get both promoted.

1.4 Related Works

Many different steganographic schemes have been come up with for various kinds of images. We can classify the existing schemes according to the format of the cover image as follows:

- Steganography for grayscale images/spatial domain [1, 3, 4, 10, 11, 12, 16, 23, 25, 26, 29, 30]: These schemes typically directly insert a small piece of the secret message into the least-significant-bit of each image pixel in the spatial domain. There are some advantages to using the spatial domain to hide data: (1) it is simpler and faster to implement the technique; (2) it can more easily offer a high hiding capacity; (3) the stego-image quality can be more easily controlled. As a result, the grayscale image has become a popular kind of image when it comes to secret data hiding. As a matter of fact, we can further classify these grayscale image steganographic schemes into two types: (1) high hiding capacity methods [16, 23, 24]: schemes whose embedding algorithms function in a pixel-by-pixel manner, resulting in the hiding capacity of half the cover image size, taking no human visual sensitivity into consideration with a just acceptable stego-image quality, and (2) high imperceptibility methods [4, 25, 30]: schemes whose embedding algorithms are human-visual-sensitivity-related, resulting in a different payload value for each individual pixel. The latter kind tends to preserve more image details, offering a higher degree of imperceptibility; however, this is done at the sacrifice of the hiding capacity.

- Steganography for JPEG images/frequency domain [2, 8, 14, 17]: The JPEG image is currently the most popular image compression file format available on the Internet. Therefore, it is more convenient to use JPEG images to convey secret data than grayscale images. However, the image distortion is usually very serious when the DCT coefficients are modified for the hiding of the secret data, and therefore the poorly limited, hardly increasable hiding capacity is a major problem.

- Steganography for binary images [18, 19, 20, 28]: It is also more challenging to hide secret data in binary images because there are only two alternatives to the color of a binary image. The modifications done to the image due to the embedding of the secret data can be easily observable by the human eye, which gives a strict limit to the hiding capacity of the binary image in comparison with the grayscale image. Among the currently available steganographic techniques for binary image, Wu and Liu's method [28] is a very good choice if the quality of the stego-image is the major concern. However, the hidden capacity is on top of the priority list, then Tseng *et al.*'s [18] method is the most highly recommended.

- Steganography for palette images (i.e., Gif images) [21, 22, 27]: Palette images, just like JPEG images, are widely used over the Internet. Palette images are composed of a color palette and some image data (i.e., index data). When embedding secret data, if it is the color palette that is modified, then major distortions can take place even when only a small part of the color palette is altered. That is to say, modifying the image data would be the better choice if the stego-image quality is the major concern. However, whether the secret message is embedded on the color palette side or the image data side, palette image steganographic schemes do not seem very likely to be capable of providing a high payload.

In this paper, we shall focus only on grayscale image steganography. The rest of this paper is organized as follows. In Section 2, we shall introduce some related works, including high hiding capacity methods [16] and high stego-image quality schemes [25, 30]. Then, in Section 3, we shall systematically compare and analyze the schemes introduced in Section 2, so that we can come to some critical, constructive ideas, which will serve as our directions for future research discussed in Section 4, followed by a brief conclusion given in Section 5.

2 Steganography for Grayscale Images

In this section, we shall introduce several methods that hide secret data in the spatial domain. In general, a grayscale image pixel value includes eight bits, and the last three bits of each pixel can be used to hide secret data without causing any distortion that is perceptible to the human eye. For this reason, grayscale images are widely used for hiding data because of their greater hiding capacities over other image formats. One of the most famous techniques in this category is the LSBs (Least-Significant-Bits) method, which directly embeds the secret data into the least significant bits of the pixel value. The earliest algorithm is called the simple LSBs method, and its embedding algorithm is as follows.

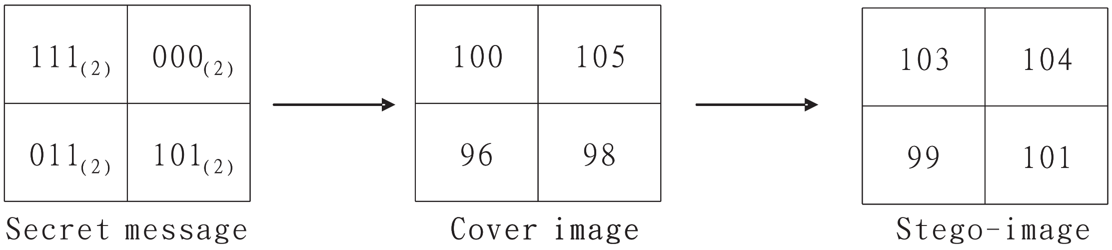

Figure 1: Simple 3-LSBs method

2.1 Steganography by the Simple LSBs Method

Suppose P_i is some pixel value of an image. The pixel value of P_i, expressed in its binary form, is as follows:

$$P_i = (b_7 b_6 b_5 b_4 b_3 b_2 b_1 b_0)_2 = \sum_{n=0}^{7} b_n \times 2^n. \tag{1}$$

where b_7 is the most significant bit, and b_0 is the least significant bit. Usually, the last three bits b_2, b_1 and b_0 can be used to hide secret data, and that is what we call the 3-LSBs scheme. The stego-image quality the 3-LSBs scheme can offer is merely acceptable. The embedding procedure of the simple LSBs scheme runs in a pixel-by-pixel fashion; namely, the payload of each pixel is identical. Assume the task here is to hide these three bits of secret data $(s_2 s_1 s_0)_{(2)}$ into P_i; in other words, the three bits $(s_2 s_1 s_0)_{(2)}$ are to be inserted into the last three bits $b_2 b_1 b_0$. Fig. 1 is an illustration showing how the 3-LSBs scheme can have the job done. As Fig. 1 suggests, each pixel of the cover image winds up holding 3 bits of secret data. The first pixel value is P_i=$100_{(10)}$, and its binary value is $01100100_{(2)}$. We can directly insert three bits of secret data $111_{(2)}$ into its last three bits $100_{(2)}$. This way, the binary value $01100100_{(2)}$ is now changed into $01100111_{(2)}$, and the stego-image P_i'=103 can be obtained by transforming $01100111_{(2)}$ into its decimal value.

2.2 Steganography by the Optimal LSBs Method

The simple LSBs method can be modified so that the stego-image quality gets improved [16, 23, 24]. The embedding algorithms of such improved schemes are still based on that of the simple LSBs method. In this section, we introduce one of the improved methods called the optimal LSBs method [1]. The scheme can greatly improve the stego-image quality by applying an optimal pixel adjustment process. In Ref. [1], three candidates are picked out from the pixels and compared to see which one can have the best result (closest to the original pixel value) with the secret data embedded in. The best candidate is then called the optimal pixel and is used to conceal the secret data. Their embedding algorithm goes as follows:

Step1 Assume P_i is the original pixel value and k bit(s) of secret data is to be embedded.

Step2 Embed k bit(s) of secret data into P_i by using the LSBs method. (Please refer to Section 2.1 for the embedding algorithm of the LSBs method.) The stego-image P_i' can then be obtained.

Step3 Generate another two pixel values by adjusting the $(k+1)$-th bit of P_i'. Therefore, $P'_{(-)}$ and $P'_{(+)}$ can be calculated as follows:

$$(P'_{(+)}, P'_{(-)}) = \begin{cases} P'_{(+)} = P_i' + 2^k; \\ P'_{(-)} = P_i' - 2^k, \end{cases} \tag{2}$$

Obviously, the hidden data in $P'_{(+)}$ and $P'_{(-)}$ are identical to P_i' because the last k bits of them are the same.

Step4 The most approximate to the original pixel value, P_i'', (i.e. the optimal candidate) can be found by the following formula:

$$P_i'' = \begin{cases} P_i', & \text{if } |P_i - P_i'| \leq |P_i - P'_{(-)}| \leq |P_i - P'_{(+)}|; \\ P'_{(+)}, & \text{if } |P_i - P'_{(+)}| \leq |P_i - P_i'| \leq |P_i - P'_{(-)}|; \\ P'_{(-)}, & \text{if } |P_i - P'_{(-)}| \leq |P_i - P_i'| \leq |P_i - P'_{(+)}|, \end{cases} \tag{3}$$

Finally, all the optimal candidates P_i'' replace the original pixel values P_i, and the embedding algorithm comes to its end. Here is an example that demonstrates the optimal LSBs method can decrease the distortion caused by the simple LSBs method.

Assume P_i=8, k=3, and the three bits of secret data are $111_{(2)}$. Hence, the stego-image P_i'=15 is generated by using the simple 3-LSBs method. We can obtain another two pixel values $P'_{(+)} = 23$ and $P'_{(-)} = 7$ after adjusting the 4-th bit of P_i'. The last three bits of pixel values P_i'=15, $P'_{(+)}$=23 and $P'_{(-)}$=7 are the same. However, the optimal candidate is $P'_{(-)}$=7 because it is the closest to the original pixel value P_i=8. From this example, we can clearly observe that the distortion of the stego-image can be greatly reduced by using the optimal LSBs method.

2.3 Steganography by the PVD Method

In 2003, Wu and Tsai [25] presented an adaptive steganographic scheme based on pixel-value differencing (PVD). With their method, the payload of each individual pixel can be different, and the resultant stego-image quality is extremely fine with perfect modification invisibility. The hiding capacity varies between smooth areas and edge areas, enabling edge areas to hold more secret data than smooth areas. This is because the degree of distortion tolerance of an edge area is naturally higher than that of a smooth area. In addition, the features of the image blocks stay unchanged after Wu and Tsai's scheme is applied, meaning that the embedding of the secret data does not change any smooth area into an edge area or any edge area into a smooth area. Therefore, the stego-image quality the PVD method produces is better than what other LSBs-based methods can offer in terms of human visual perception. The embedding algorithm of the PVD method follows the steps listed below:

Step1 Divide the cover image into a series of non-overlapping sub-blocks, and each sub-block has two consecutive pixels, say P_i and P_{i+1}.

Step2 Let d_i be the difference value between P_i and P_{i+1}, which can be computed by

$$d_i = |P_i - P_{i+1}|. \tag{4}$$

R_1	R_2	R_3	R_4	R_5	R_6
8	8	16	32	64	128

0 7 15 31 63 127 255

Figure 2: All difference values quantized into six ranges

Step3 Quantize the difference values of all the sub-blocks into n contiguous ranges, say R_i where $i = 1, 2, ..., n$. And the size of each sub-range must be selected to be a power of 2. Assume the lower and upper bounds of each R_i are l_i and u_i respectively. Hence, the width w_i of each R_i is $|u_i - l_i|$. Fig. 2 illustrates how all the difference values can get quantized.

Step4 For the difference value d_i of each sub-block, R_i can be searched for its range. The hiding capacity of each sub-block depends on the width w_i of its range. Let k_i be the number of bits that can be hidden into two consecutive pixels P_i and P_{i+1}. The figure k_i can be calculated by

$$k_i = \lfloor (\ log_2 w_i) \rfloor. \tag{5}$$

Step5 Transform k_i bits of secret data into a decimal value k'_i. And compute the new difference value d'_i by adding the lower bound value l_j of its range R_i.

$$d'_i = k'_i + l_i. \tag{6}$$

Step6 Embed k_i bits of secret data into the sub-block by modifying its P_i and P_{i+1} such that d_i=d'_i. The equation for the modification of P_i and P_{i+1} is as follows:

$$(P'_i, P'_{i+1}) = \begin{cases} (P_i + \lceil m/2 \rceil, P_{i+1} - \lfloor m/2 \rfloor), & if \ P_i \ \geq \ P_{i+1} \ and \ d'_i > d_i; \\ (P_i - \lfloor m/2 \rfloor, P_{i+1} + \lceil m/2 \rceil), & if \ P_i \ < \ P_{i+1} \ and \ d'_i > d_i; \\ (P_i - \lceil m/2 \rceil, P_{i+1} + \lfloor m/2 \rfloor), & if \ P_i \ \geq \ P_{i+1} \ and \ d'_i \leq d_i; \\ (P_i + \lceil m/2 \rceil, P_{i+1} - \lfloor m/2 \rfloor), & if \ P_i \ < \ P_{i+1} \ and \ d'_i \leq d_i, \end{cases} \tag{7}$$

where $m = |d'_i - d_i|$. The new pixel values P'_i and P'_{i+1} can be obtained with the feature value of the secret message already recorded in their difference value d'_i.

Here is an example of how the embedding algorithm of the PVD method works. Assume P_i=100, P_{i+1}=115, and all possible difference values are classified into six ranges as shown in Fig. 2. The difference value between P_i and P_{i+1} is d_i=|100−115|=15, and it belongs to the second range R_2 that has w_i=8, u_2=15, l_2=7 and k_i= $log_2(8)$=3. Assume the 3 bits of secret data to be embedded are $100_{(2)} = 4_{(10)}$. Then, the new difference value is d'_i=$d_i + l_i$=4+7=11. We can use Eq. (7) to modify P_i and P_{i+1} such that d'_i=d_i. Finally, we can obtain P'_i=102 and P'_{i+1}=113 after executing Eq. (7).

Now let's observe how the secret data can be extracted from P'_i and P'_{i+1} by using the PVD method. First, we can compute the difference value d'_i and can search R_i for its sub-range, where $i = 1, 2, \ldots, n$. The hiding capacity k_i of this sub-range can also be found, and so can its lower bound l_i. The secret data in its decimal form can be computed as k'_i=d'_i-l_i, and the exact secret data can be recovered by transforming k'_i into its binary form with the length of k_i bits.

2.4 Steganography by the MBNS Method

In 2005, Zhang and Wang [30] also presented an adaptive steganographic scheme with the multiple-base notational system (MBNS) based on human vision sensitivity (HVS). The hiding capacity of each image pixel is determined by its so-called local variation. The formula for computing the local variation takes into account the factor of human visual sensitivity. A great local variation value indicates the fact that the area where the pixel belongs is a busy/edge area, which means more secret data can be hidden. On the contrary, when the local variation value is small, less secret data will be hidden into the image block because it is in a smooth area. This way, the stego-image quality degradation is very invisible to the human eye. The embedding algorithm of the MBNS method is as follows:

Step1 Assume t_i for $i = 1, 2, \ldots, l$ is a binary stream of secret data whose length is l. Divide l bits of secret data into n segments with the length of each segment being $\frac{l}{n}$ bits. Convert each segment into its decimal value x_i, where $i = 1, 2, \ldots, n$.

Step2 Assume $P(i, j)$ is the pixel in which the secret data is to be embedded. Then, the payload of $P(i, j)$ is determined by the three pixels that surround it, namely $P(i-1, j)$, $P(i-1, j-1)$ and $P(i, j-1)$. Compute the variation $\delta\ (i, j)$ of $P(i, j)$ with $P(i-1, j)$, $P(i-1, j-1)$ and $P(i, j-1)$.

Step3 Determine the base of $P(i, j)$ according to its local variation $\delta\ (i, j)$. Let $b(i, j)$ be the base of $P(i, j)$. It can be calculated by

$$b(i, j) = min(\lceil \frac{\delta\ (i, j)}{\Delta} \rceil, 16). \tag{8}$$

where Δ is a constant, and it controls the hiding capacity of each pixel. A smaller Δ leads to a larger payload, and vice versa. If $b(i, j) \leq 1$, then no secret data will be embedded in $P(i, j)$; namely, this pixel will be skipped. Otherwise, the next step will be taken to hide secret data into $P(i, j)$.

Step4 Compute the remainder and quotient value of x_i by

$$s(i, j) = x_i\ mod\ b(i, j), \tag{9}$$

$$q = \frac{x_i - s(i, j)}{b(i, j)}. \tag{10}$$

Step5 Compute the remainder value $r(i, j)$ for the $P(i, j)$ by modulo calculation.

$$r(i, j) = P(i, j)\ mod\ b(i, j). \tag{11}$$

Step6 Embed secret data $s(i, j)$ into the pixel $P(i, j)$ by using the following algorithm:

If $r(i, j) == s(i, j)$

The task of hiding $s(i, j)$ into $P(i, j)$ is accomplished.

Else

Modify $P(i, j)$ until its remainder $r(i, j)$ is equal to $s(i, j)$.

After Step 6, if $q \neq 0$, then we must update x_i by $x_i = q$ and read the second pixel $P(i, j) = P(i + 1, j)$ to hide the secret data by re-executing Step 2∼Step 6. If $q = 0$, it means the first segment of secret data has already been embedded. In that case, we can go on and read the next segment of secret data and re-execute Step 2∼Step 6 until the whole secret data is finished.

3 Comparisons and Analyses

In this section, we shall first compare performances of the simple LSBs method and the optimal LSBs method in terms of stego-image quality, and then we shall analyze the efficacies of the PVD method and the MBNS method. To begin with, some experimental results will be given to demonstrate that the optimal LSBs method can greatly improve the stego-image quality provided by the simple LSBs method. From Table 1, we observe that the PSNR value of the optimal LSBs scheme is greater than that of the simple LSBs method by about 2.22∼3.03 dB. Please pay special attention to the fact that the steog-image quality of 4-LSBs by using the optimal scheme is still acceptable to the human eye. However, the PSNR value drops sharply down to 28 dB even when 5-LSBs is used to embed secret data. Moreover, the embedding effect in the smooth areas is conspicuous to the eye when the 4-LSBs scheme is used. However, the optimal LSBs method can still meet the high hiding capacity requirement because no high quality scheme [4, 25, 30] can conceal data over half the size of the cover image. Therefore, the optimal LSBs method is a more ideal scheme when a high payload is required. By contrast, the PVD method

Table 1: Comparisons between the optimal LSBs method and the simple LSBs method

Cover-Images (512 × 512)	Optimal Method [1]		Simple Method		Increased PSNR (dB)
	Capacity (bits)	PSNR (dB)	Capacity (bits)	PSNR (dB)	
Lena (2-LSBs)	524288	46.37	524288	44.15	2.22
Lena (3-LSBs)	786432	40.73	786432	37.92	2.81
Lena (4-LSBs)	1048576	34.81	1048576	31.78	3.03
Baboon (2-LSBs)	524288	46.37	524288	44.15	2.22
Baboon (3-LSBs)	786432	40.73	786432	37.92	2.81
Baboon (4-LSBs)	1048576	34.80	1048576	31.86	2.97
Jet (2-LSBs)	524288	46.37	524288	44.11	2.26
Jet (3-LSBs)	786432	40.73	786432	37.96	2.77
Jet (4-LSBs)	1048576	34.81	1048576	31.85	2.96

and the MBNS method are more suitable for low hiding capacity applications because they are better at preserving image details after the embedding of the secret data. Suppose there are two consecutive pixels from a smooth area. The two smooth area pixels will remain smooth after the processing of the PVD method, while the property of the two pixels might change if it is a LSBs-based scheme that is used to hide the secret data. From the viewpoint of human vision sensitivity, the MBNS scheme is better than the PVD scheme, and the reason is that the former has more parameters than the latter. In the MBNS scheme, the local variation of each pixel is determined by three surrounding pixels, whereas the PVD scheme refers to only two. Therefore, with the MBNS method, the image local property can be more objectively and precisely measured.

Ideally, with the MBNS method, the perceptual change of each pixel after hiding data is slighter. However, critical accumulative distortion could happen because the Δ value is smaller. As the embedding algorithm introduced earlier in Section 2.4 goes, suppose the pixels $P(i-1,j)$, $P(i-1,j-1)$ and $P(i,j-1)$

are the stego-pixels that have been modified with secret data embedded in. This way, the local variation of $P(i,j)$ derived from its three surrounding pixels $P(i-1,j)$, $P(i-1,j-1)$ and $P(i,j-1)$ may not be exactly accurate because the pixel values are not the original values but have been changed. Serious distortion of $P(i,j)$ can happen after hiding data. Furthermore, $P(i,j)$ will be taken as a parameter to process the next pixels $P(i+1,j)$ and $P(i+1,j+1)$ and get their local variation values, which means the distortion accumulates and the problem worsens.

4 Directions for Future Research

Our future research efforts will be focused on putting together a new method that has a greater hiding capacity than the 4-LSBs method and can maintain such stego-image quality as to meet the demand of human visual sensitivity. The following are some directions for future research:

- Make better use of edge areas to hide more data: If 5 bits of secret data were to be hidden in every pixel, then the visual artifacts on the stego-image would be obviously visible. That is to say, not every pixel can afford to hold so many secret data bits without clearly showing the modification. In our opinion, the whole image should at least be broken down to smooth areas and edge areas, and data hiding can then be done to different kinds of areas differently. In smooth areas, for example, we can hide 4 bits of secret data in each pixel; in edge areas, each pixel can afford to hold as many as 5 bits of secret data. However, it is necessary but more challenging to try to maintain the local properties of the pixels, making them stay the same after hiding data, because, say, if some smooth area is changed into a non-smooth area after hiding data, it will result in judging errors in the recovery phase. Therefore, the extracting algorithm must be blind.

- Utilize more surrounding pixels to determine the local complexity of the image pixel: In Wu and Tsai's method [25], the local characteristic of the image is determined by two pixels. In Zhang and Wang's method [30], the local variation of each pixel depends on its three surrounding pixels. In our opinion, within a reasonable limit, more surrounding pixels mean more accurate local variation. For instance, we can compute the local variation based on a 3×3 sub-block design. Nevertheless, if the number of surrounding pixels picked out to determine the local variation gets too big, the sub-block loses its sense of locality, and the local variation derived will make little sense if any. In other words, the problem of how many pixels make the perfect number to take into account when we compute the local variation is a major problem to solve in the future.

- In recent years, many steganalysis schemes have been proposed with the idea of detecting the existence of the hidden data in the stego-image by using statistic steganalysis attacks [5, 6, 7, 9, 13]. Indeed, it is more efficient and accurate to judge whether there is any secret message hidden in a digital image by using steganalysis than by just looking at the picture. To cope with this new trend, new steganographic techniques that we are going to develop in the future should be powerful enough to withstand the attacks of steganalysis detection.

5 Conclusion

Image steganography, the art of conveying secret messages under the cover of digital images, is an interesting field of research. Of all types of digital images, the grayscale image is one of the most suitable kinds of images for steganographic techniques to apply because of the great hiding capacity and high stego-image quality. In this paper, we have reviewed some well-accepted schemes and classified them into two major types: high hiding capacity schemes and high stego-image degradation imperceptibility schemes. If a large amount of data is to be hidden, then the optimal LSBs method is a good choice. On the other hand, both the PVD scheme and the MBNS scheme are superior to LSB-based schemes in terms of stego-image quality. Though the payload of PVD and MBNS is much smaller than that of the LSBs method, the modifications done to the stego-image due to the embedding of the secret message is extremely invisible to the human eye.

In the future, how to increase the payload at the same PNSR level and how to increase the PSNR value under the same payload are among the problems we shall invest research efforts in solving. Of course, an ideal steganographic scheme should be not only capable of providing a high hiding capacity but also able to produce a high qhality stego-image that lives up to the standard of human visual sensitivity. In addition, an ideal steganographic scheme should have the power to resist various steganalysis attacks.

References

[1] C. K. Chan and L. M. Cheng, "Hiding data in images by simple LSB substitution," *Pattern Recognition*, pp. 469–474, Mar. 2004.

[2] C. C. Chang, T. S. Chen, and L. Z. Chung, "A steganographic method based upon JPEG and quantization table modification," *Information Sciences*, vol. 141, pp. 123–138, Mar. 2002.

[3] C. C. Chang, J. Y. Hsiao, and C. S. Chan, "Finding optimal least-significant-bit substitution in image hiding by dynamic programming strategy," *Pattern Recognition*, vol. 36, no. 7, pp. 1583–1595, 2003.

[4] C. C. Chang and H. W. Tseng, "A steganographic method for digital images using side match," *Pattern Recognition Letter*, no. 25, pp. 1431–1437, 2004.

[5] S. Dumitrescu and X. Wu, "A new framework of lsb steganalysis of digital media," *IEEE Transactions on Signal Process*, vol. 53, pp. 3923–3935, Oct. 2005.

[6] S. Dumitrescu, X. Wu, and Z. Wang, "Detection of lsb steganography via sample pair analysis," *IEEE Transactions on Signal Process*, vol. 51, pp. 1995–2007, Jul. 2003.

[7] J. Fridrich, M. Goljan, and R. Du, "Reliable detection of lsb steganography in grayscale and color images," in *Proc. ACM Workshop on Multimedia and Security*, pp. 27–30, 2001.

[8] M. IWATA, K. MIYAKE, and A. SHIOZAKI, "Digital steganography utilizing features of JPEG images," *IEICE Trans. on Fundamentals*, vol. E87-A, pp. 929–936, Apr. 2004.

[9] A. D. Ker, "Steganalysis of lsb matching in grayscale images," *IEEE Signal Processing Letters*, vol. 12, pp. 441–444, Jun. 2005.

[10] C. C. Lin and W. H. Tsai, "Secret image sharing with steganography and authentication," *Journal of Systems and Software*, vol. 73, pp. 405–414, Nov. 2004.

[11] D. C. Lou and J. L. Liu, "Steganographic method for secure communications," *Computers and Security*, vol. 21, pp. 449–460, Jun. 2002.

[12] L. M. Marvel, C. G. Boncelet, and C. T. Retter, "Spread spectrum image steganography," *IEEE Trans. on Image Processing*, vol. 8, pp. 1075–1083, Aug. 1999.

[13] B. T. Mcbride, G. L. Peterson, and S. C. Gustafson, "A new blind method for detecting novel steganography," *Digital Investigation*, vol. 2, pp. 50–70, 2005.

[14] B. G. Mobasseri and R. J. Berger, "A foundation for watermarking in compressed domain," *IEEE Signal Processing Letters*, vol. 12, pp. 399–402, May 2005.

[15] G. J. Simmons, "The prisoners' problem and the subliminal channel," in *Proceedings of Crypto '83*, pp. 51–67, 1984.

[16] C. C. Thien and J. C. Lin, "A simple and high-hiding capacity method for hiding digit-by-digit data in images based on modulus function," *Pattern Recognition*, vol. 36, no. 12, pp. 2875–2881, 2003.

[17] H. W. Tseng and C. C. Chnag, "High capacity data hiding in jpeg-compressed images," *Informatica*, vol. 15, no. 1, pp. 127–142, 2004.

[18] Y. C. Tseng, Y. Y. Chen, and H. K. Pan, "A secure data hiding scheme for binary images," *IEEE Trans. on Communications*, vol. 50, pp. 1227–1231, Aug. 2002.

[19] Y. C. Tseng and H. K. Pan, "Data hiding in 2-color imgages," *IEEE Trans. on Computers*, vol. 51, pp. 873–878, Jul. 2002.

[20] C. H. Tzeng and W. H. Tsai, "A new approach to authentication of binary image for multimedia communication with distortion reduction and security enhancement," *IEEE Communications Letters*, vol. 7, pp. 443–445, Sept. 2003.

[21] C. H. Tzeng and W. H. Tsai, "A combined approach to integrity protection and verification of palette images using fragile watermarks and digital signatures," *IEICE Trans. on Fundamentals*, vol. E87-A, pp. 1612–1619, June 2004.

[22] C. H. Tzeng, Z. F. Yang, and W. H. Tsai, "Adaptive data hiding in palette images by color ordering and mapping with security protection," *IEEE Trans. on Communications*, vol. 52, pp. 791–800, May 2004.

[23] R. Z. Wang, C. F. Lin, and J. C. Lin, "Image hiding by optimal lsb substitution and genetic algorithm," *Pattern Recognition*, vol. 34, no. 3, pp. 671–683, 2001.

[24] S. J. Wang, "Steganography of capacity required using modulo operator for embedding secret image," *Applied Mathematics and Computation*, vol. 164, pp. 99–116, Jan. 2005.

[25] D. C. Wu and W. H. Tsai, "A steganographic method for images by pixel-value differencing," *Pattern Recognition Letters*, vol. 24, no. 9-10, pp. 1613–1626, 2003.

[26] H. C. Wu, N. I. Wu, C. S. Tsai, and M. S. Hwang, "Image steganographic scheme based on pixel-value differencing and LSB replacement methods," *IEE Proc. -Vis. Image Signal Process*, vol. 152, pp. 611–615, Oct. 2005.

[27] M. Y. Wu, Y. K. Ho, and J. H. Lee, "An iterative method of palette-based image steganography," *Pattern Recognition Letters*, vol. 25, pp. 301–309, 2004.

[28] Min Wu and Bede Liu, "Data hiding in binary image for authentication and annotation," *IEEE Trans. on Multimedia*, vol. 6, pp. 528–538, Aug. 2004.

[29] Y. H. Yu, C. C. Chang, and Y. C. Hu, "Hiding secret data in images via predictive coding," *Pattern Recognition*, vol. 38, pp. 691–705, May 2005.

[30] X. Zhang and S. Wang, "Steganography using multiple-base notational system and human vision sensitivity," *IEEE Signal Processing Letters*, vol. 12, pp. 67–70, Jan. 2005.