Journal of Shanghai University (English Edition), 2006, **10**(1): 33 - 43
Article ID: 1007-6417(2006)01-0033-11

Undercover communication using image and text as disguise and countermeasures

WANG Shuo-zhong(王朔中), *CHEN Chao*(陈超), *ZHANG Xin-peng*(张新鹏)
School of Communication and Information Engineering, Shanghai University, Shanghai 200072, *P. R. China*

Abstract A brief survey of some representative techniques of steganography and steganalysis is presented. Various methods developed in the authors' laboratory are introduced, including symmetric LSB embedding, secure steganography in JPEG, palette, and uncompressed color images, histogram-based analysis and least histogram abnormality steganography, multiple-base notational system based embedding, stego-encoding integrated with error correction, *etc*. Some of the proposed approaches provide overall improvement, while others offer alternatives to existing techniques with advantage in certain aspects. Data hiding in text using the typesetting tool TeX is also introduced, with a brief description of a recently developed technique. Current research topics and the future plan are outlined. The discussion is focused mainly on steganography/steganalysis in still images.

Key words steganography, steganalysis, information hiding, covert communication, security.

1 Introduction

Since the early 1990s, information hiding has become a hot topic attracting much attention from researchers in various fields including signal processing, cryptography and computer science, developers and suppliers of multimedia contents, and professionals and other personnel who are concerned with information security[1]. Two major areas are of the most interests: digital watermarking and steganography.

The purpose of digital watermarking is to protect intellectual property rights of multimedia products such as image, audio and video. The most important technical specification of digital watermarking is robustness against malicious attacks by copyright violators as well as conventional signal processing operations[2].

Steganography, on the other hand, aims to convey secret message under the cover of apparently innocent host media[3-5]. By carefully embedding the stego-data into a host, the very existence of secret communication is hidden. This is in contrast to cryptography that makes the message unintelligible to any interceptors but makes no attempt to conceal the presence of secret communication. In steganography, the host media merely serves as a disguise, and the most crucial requirement is to make the embedded information undetectable by any perceptual or algorithmic means. Robustness against attacks such as intentional removal and destruction of the hidden data, and general signal processing is, in general, not of primary concern. A comparison between digital watermarking and steganography has been made in Ref. [6] in terms of the essential goals and the degree of importance and stringency in the requirements of various technical specifications such as imperceptibility, statistical invisibility, robustness against attacks, embedding capacity, blind extractability, *etc*.

As steganography can convey secrete messages in an unnoticeable manner, it may be used for either good or evil purposes. Anti-steganography has become an important issue closely related to information security[7]. The predominant countermeasure against steganography to date is steganalysis that reveals the presence of embedded information by exploring statistical abnormality of the suspected media[8]. Another challenge to steganography is active attack[9], *viz*., to introduce indiscernible distortion into digital media indiscriminately to prevent any possible hidden information from being extracted by unknown recipients. Although

Received Sep. 1, 2005
Project supported by National Natural Science Foundation of China (Grant No. 60372090), Key Project of Shanghai Municipality for Basic Research (Grant No. 04JC14037), and Shanghai Leading Academic Discipline Project (Grant No. T0102)
WANG Shuo-zhong, Ph. D., Prof., E-mail: shuowang@staff.shu.edu.cn

this type of attacks does not pose a major threat to most attempts of steganography since it cannot identify the source of hidden information and is unpractical to be used on the huge amount of digital media present in public networks, it is useful in certain local network environments. Ability of surviving active attack is a useful characteristic of a steganographic technique, but is not a major requirement in developing most steganographic algorithms.

In this article, a brief survey of some representative techniques of steganography and steganalysis is made. Various methods developed in the authors' laboratory are introduced. Some of the proposed approaches provide overall improvement, while others offer alternatives to existing techniques with advantages in certain aspects. Current research topics and the future plan are outlined. The discussion is focused mainly on steganography/steganalysis in still images. A brief introduction to text based data hiding techniques is also given. Information hiding in digital audio will be considered later in a separate paper.

2 LSB based steganographic and steganalytic techniques

The term steganography came from Greek meaning covered writing. Ancient stego techniques include writing on the shaved head of a messenger and sending him to the destination after hair grows long enough, using invisible ink to write and showing the contents with chemicals, embedding letters in a seemingly normal text according to certain rules, printing secret words in tiny microdots, and so forth. Modern steganography is realized based on digital signal processing and coding techniques using computers, which is the topic of the present article.

2.1 LSB embedding and steganalysis based on asymmetry of LSB flips

The simplest steganographic technique, termed the LSB method, is to replace all or part of the least significant bit plane of an image with secret data. If the entire LSB plane is replaced and the embedded binary sequence is uniformly distributed, approximately 50% of the original least-significant bits are flipped, leading to slight distortion measured by PSNR = 51.1 dB. Reduced capacity causes even less distortion. Invisibility to human eyes is therefore excellent. Such a basic LSB embedding method, however, is in fact insecure since detectable abnormality is introduced in the embedding. Changes of pixel values occur only between $2i$ and $2i+1$, but not between $2i-1$ and $2i$. This leads to an effective steganalytic technique, the RS method proposed by Fridrich, *et al*.[8] Also, the embedding makes the numbers of pixels with gray values $2i$ and $2i+1$ tend to become close, resulting in pronounced histogram anomaly and providing a clue for the χ^2 analysis[10]. These methods not only can reveal the presence of secret data, but can also estimate the amount of embedded data.

An alternative steganalytic technique, the gray-plane crossing (GPC) method, has been proposed in Ref. [11]. We consider an image a 3D terrain in which the height z represents pixel gray values, and define two families of parallel planes P_0: [$z = 1.5$, $z = 3.5$, $z = 5.5$, $\cdots$, $z = 235.5$], and P_1: [$z = 0.5$, $z = 2.5$, $z = 4.5$, $\cdots$, $z = 254.5$]. The total numbers with which the terrain passes through planes in P_0 and P_1 are N_0 and N_1 respectively. Generally speaking, a natural image without inserted data has $N_0 \approx N_1$. Since LSB embedding does not affect N_0 but causes N_1 to increase, the ratio $R = N_1/N_0$ can be used as a metric for steganalysis. When R exceeds a given threshold, the image is suspected as to contain secret data. It has been shown that, by choosing an appropriate threshold, probabilities of both missing and false alarm can be made small if the embedding rate is sufficiently high.

It is obvious that the simple LSB embedding has already been defeated by several analytic methods. To combat steganalysis, a modified LSB stego method has been devised in which changes of gray values between $2i$ and $2i-1$, and between $2i+1$ and $2i+2$ are also allowed[12]. Assume a pixel at (i, j) has a gray value $x(i, j)$. If the LSB of $x(i, j)$ is the same as the bit to be embedded, $x(i, j)$ is not changed, otherwise calculate

$$T = \sum_{u=i-1}^{i+1} \sum_{v=j-1}^{j+1} x(u, v) - 9x(i, j) \tag{1}$$

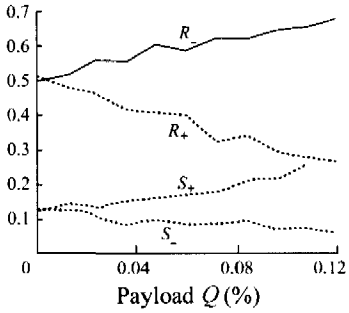
and modify $x(i, j)$ as follows:

$$x'(i,j) = \begin{cases} x(i,j) - 1, & T \leqslant 0,\ 0 < x(i,j) < 255, \\ x(i,j) + 1, & T > 0,\ 0 < x(i,j) < 255, \\ x(i,j) - 1, & x(i,j) = 255, \\ x(i,j) + 1, & x(i,j) = 0. \end{cases} \tag{2}$$

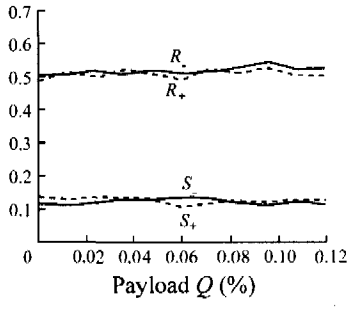
In this way, although higher bit planes may also be affected, changes in pixel gray values are still kept to 1, therefore distortion is the same as the plain LSB method. Extraction is easy as the least significant bits are simply the embedded data.

The modified LSB embedding is no longer vulnerable to the RS, χ^2 and GPC analyses since the undesirable asymmetry in the LSB flipping is avoided. Therefore we may call this method symmetrical LSB embedding.

Fig. 1 gives typical results of the RS analysis on the plain LSB and the symmetrical LSB embedding in the test image Lena. Fig. 1(a) shows that, for the plain LSB method, with the embedded data increased, the parameter pairs $[R_+, R_-]$ and $[S_+, S_+]$, as defined in Ref. [8], go progressively apart. In Fig. 1(b) for the symmetrical LSB, parameter values in the two pairs stay basically undetached, indicating inability of the RS analysis in detecting the embedded information.



(a) Plain LSB method



(b) Symmetrical LSB method

Fig. 1 RS analysis on the stego-Lena

In a recent publication[13], Ker proposed a new method for detecting the symmetrical LSB embedding (Ker referred it as the LSB matching steganography) in grayscale images. He used the histogram characteristic function (HCF)[14] previously proposed for palette images, and applied it in two ways: calibrating the output using a down-sampled image and computing the adjacency histogram. Experimental results show that the methods are remarkably effective. Further studies are needed in this area on, for example, generalization of the method to cover color images, and possible modification to the symmetrical LSB technique for withstanding Ker's analysis.

2.2 Vulnerability of LSB embedding in true color images and anti-RQP technique

For RGB color images, LSB embedding can be performed on each color component leading to a three-fold payload. The above described symmetrical LSB embedding can also be used to resist the RS, χ^2 and GPC analyses. Additional vulnerability, however, originates from the significantly increased number of colors due to LSB embedding. When the total number of colors in an image is not much more than 50% of the total pixel number, increase of color varities can be used for analysis. For example, a color image sized 284×213 has 36 570 different colors, which is 60% of the pixel number. After LSB embedding, the number of colors is increased to 46 948, 78% of the total pixel number. All the newly created colors are neighbors of the originally existing colors since LSB embedding only changes the pixel values by 1. By analyzing the number of connecting color pairs, a raw-quick-pair (RQP) method can be used to detect the presence of embedded data[15].

To overcome this drawback, an improved approach was proposed in which the number of created new colors is reduced to minimum[16]. Instead of modifying LSB of each individual color component, the anti-RQP embedding treats each triplet, [RGB], of the pixel color as an entirety. The triplet is modified to a new value in its close vicinity in the RGB color space, which is a valid color in the palette of the cover image. A new color is created only if such a color is unavailable. The embedding is carried out as follows.

(1) For each candidate pixel, if LSB of the sum of its color triplet is the same as the bit to be embedded, no change is made.

(2) If they are different, set LSB of each color component to 0, resulting in a base color for the pixel. The 8 neighboring colors of a unit cube with the base color at a corner are divided into even and odd groups, depending on LSB of the color triplets.

(3) Modify the host pixel to a corresponding even or

odd color existing in the palette.

(4) If none of the colors in the chosen group is in the palette, randomly set the host pixel to any value in the group. In this case a new color is created, and added to the palette.

Distortion due to the anti-RQP embedding is small since search of matched colors is carried out within unit cubes in the color space, and modifications of colors are confined to the LSB plane. Taking LSBs of R + G + B of the modified pixels, the stego data are easily extracted. To further reduce the number of created colors for better security, the search area can be expanded to a $3 \times 3 \times 3$ cube with increased distortion.

Experiments were performed on two image databases, each containing 100 images. Table 1 gives typical values of PSNR of the stego-images using the LSB and anti-RQP methods. ARQP111 and ARQP333 refers to the anti-RQP algorithms using a unit searching cube and a $3 \times 3 \times 3$ cube respectively.

Table 1 PSNR of stego images with different embedding techniques

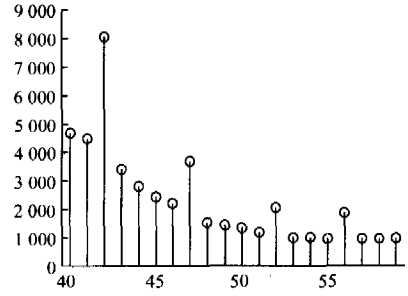
Image database and payload		Typical PSNR after stego embedding (dB)		
Image database	Embedded bits	Plain LSB	ARQP111	ARQP333
People (400 × 300)	17 255	64	62	60
Landscape (267 × 200)	5 299	66	64	62

3 Steganalysis based on histogram abnormality and enhancement of security

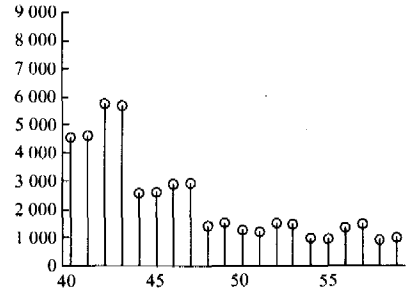
3.1 Histogram abnormality caused by LSB embedding and the remedies

An important type of statistic features frequently used in steganalysis is the changing appearance of histograms, including the basic gray-value histogram and histograms of various derived quantities. A simple example is the χ^2 analysis that reveals the presence of hidden data by exploring the tendency of increased gray-value pairs belonging to roughly the same number of pixels, as shown in Fig.2.

One way of combating histogram analysis is to compensate for the histogram change introduced in the stego embedding such as OutGuess developed by Provos[17]. Also, a least histogram abnormality (LHA) scheme has been proposed to not only maintain balance between the two types of LSB flips, but also preserve the original histogram to the greatest possible extent[18]. In the least square sense, the method optimally assigns the two opposite ways of gray value modifications (+1 and −1) to the pixels whose LSBs differ from the bits to be embedded. This is implemented by solving an over-determined system of linear equations with the Moore-Penrose pseudo-inversion.



(a) The original test image Man



(b) The stego-Man

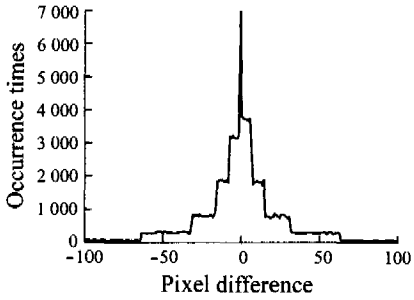
Fig.2 Partial histograms of a test image

3.2 Steganography based on pixel differences

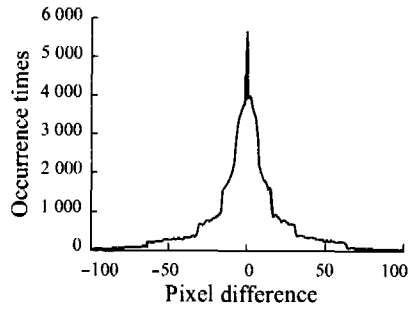
Another category of data embedding is based on pixel pairs or blocks. The pixel-value differencing (PVD) steganography proposed by Wu, *et al.*[19] can hide a large amount of secret bits into a still image by modifying the difference values between pairs of adjacent pixels. In this technique, more data are inserted into areas where fluctuation of pixel-values is large as pixels in these areas can tolerate more changes. This leads to good imperceptibility with a high embedding rate. However, although the PVD method can resist the RS analysis, it is vulnerable to steganalysis based on the histogram of pixel-value differences. The histogram-based analysis can even provide an estimate of the embedded data length. To enhance security, a modified scheme has been proposed.

It has been shown that a loophole exists in the PVD method, causing an abnormal appearance of the histo-

gram featured by steps or ruggedness as illustrated in Fig.3, which should otherwise be smooth. The peculiar look of the histogram not only reveals existence of hidden data but also provides a clue for estimating embedded data length. To enhance security, a modified scheme is proposed which avoids occurrence of the unusual ruggedness in the pixel difference histogram while preserving the advantage of low visual distortion of the PVD[20]. A pseudo-random dithering is introduced to the division of ranges of the pixel-value differences, effectively removing the undesirable steps (see Fig.4). In this way, the histogram-based steganalysis is defeated while the advantages of large embedding capacity and high invisibility of the original PVD preserved.



(a) 99.6% of pixel pairs contain stego-data



(b) 50% of pixel pairs contain stego-data

Fig.3 PVD histogram of stego-Baboon

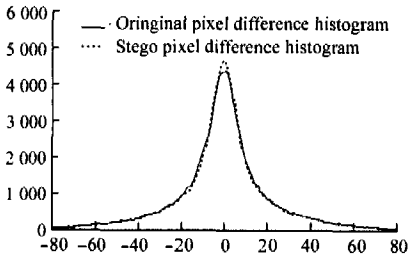


Fig.4 The modified PVD steganography is immune to histogram analysis

Another gray-level difference based method is the side match (SM) steganography[21], in which the pixel difference is defined as

$$d = \frac{g_u + g_l}{2} - g_x, \tag{3}$$

where g_x, g_u, and g_l are gray values of the current pixel, and the pixels on the top and to the left respectively. The difference is modified to let the current pixel carry one or more bits of the secret data. The number of embedded bits is dependent upon d, and the amount of modification made to d is calculated from a modulo operation that takes account of both d and the embedded data.

The SM method has large capacity with small visual distortion since pixels in a busy area can carry more data, while those in a smooth area carry less data. However it suffers from the similar problem of PVD: The rugged histogram of d provides clue for analysis. By first arbitrarily choosing an initial value of embedding rate, an estimated embedding rate may be obtained by iterated curve fitting operations[22]. Therefore the SM embedding is also vulnerable to histogram analysis, and improved techniques are to be developed.

4 Steganography in compressed images

4.1 Using palette image as stego-cover

By using a small number of indices, usually 256, to represent different colors and brightness, palette images can save a great deal of storage space and transmission time compared to the 24 bit true color images, while provide visually acceptable quality. They are good candidates for steganography due to their popularity over the Internet.

Data can be embedded into a palette image by modifying the order of colors in the palette without changing the appearance of the image itself such as implemented in a downloadable stego-tool gifshuffle. For a palette containing 256 colors, there are $(N!)$ different arrangements, meaning that at most $\log_2(N!)$ bits of data can be embedded regardless of the image size. This technique is insecure because the irregularity in the order of palette colors is a clear sign of intentional modification.

Another way of data hiding is to modify the indices within the available colors. Straight modification can sometimes produce isolated pixels that are strikingly different from their immediate neighbors, therefore

arouse suspicion. Improved methods have been proposed, among which the optimal parity assignment (OPA) steganography[23]. OPA assigns all colors into two subsets in an optimal manner, and changes the color of a pixel, if necessary, to the closest available neighboring color so that distortion is reduced compared to other technique such as that used in EZ Stego.

It has been shown that, however, the OPA and similar schemes have loopholes[24]. A palette image, when applying OPA, has some singular colors that can be changed to other colors but no other colors can be changed to them. Data embedding will reduce the numbers of singular colors, making the OPA method insecure for covert communication. In Ref. [24], a new scheme different from the OPA is devised in which all colors are divided into two subsets, representing respectively 0 and 1 in the secret data sequence to be embedded. Division of the colors into subsets is made such that each color has at least two neighbors, and any two neighboring colors belong respectively to the two subsets, as shown in Fig.5. In this way, no singular colors exist and the loophole in OPA is removed. Further improvement has been made by embedding data only in busy areas so that even analysis made by someone who knows the subset division will fail.

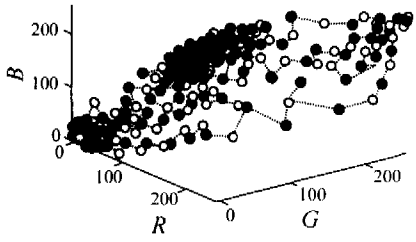


Fig.5 Two color subsets and lines that connect neighboring colors

4.2 Secure steganography in JPEG images

JEPG images are particularly suitable to be used for information hiding since they are very widely used, especially in the Internet environment, for the high compression ratio and good visual quality. Various methods have been proposed, and many tools are made available online.

Early techniques caused anomaly in the histogram of DCT coefficients or block properties, therefore were considered insecure[25]. Some simple techniques such as Jsteg apply LSB replacement to the quantized DCT coefficients therefore are vulnerable to the χ^2 test. Other methods modify the quantization tables, making them detectable due to unusual quantization steps. To overcome these drawbacks, F5 does not change the quantization table, and uses a different embedding method on DCT coefficients to preserve the histogram in order to resist the χ^2 test and histogram analysis. In addition, data shuffling and matrix encoding are introduced for better security[26].

However, F5 was soon broken after a sophisticated investigation into the tiny changes in the histogram and block features. This is accomplished using an imitated original image constructed by re-coding with JPEG based on offset blocking of the stego image[27].

In order to improve security of embedded information in a JPEG image, a secure steganographic technique has been proposed, in which non-zero AC DCT coefficients are used to carry the secret bits with DCT coefficient histogram and block features unaltered[28]. Thus the histogram and block-based steganalyses are defeated. This method is secure for JPEG cover images of a quality factor greater than 35.

4.3 Lossless embedding

Information hiding techniques generally cause some insignificant distortions in the host media, which can not be restored after extraction of the embedded message. However, certain applications such as medical imaging require perfect recovery of the carrier media. A lossless embedding scheme has been developed for JPEG images[29]. In this method, certain nonzero DCT coefficients selected with a secret key are used to carry the embedded information, while the original coefficients are coded and stored in the spectral positions that are initially zero. On the extraction side, not only can the hidden message correctly recovered from the coefficients carrying secret data, but also the host image can be completely restored without error. Experimental results show that the lower the compression quality factor, the higher the embedding rate.

The scheme is secure in two senses. First, the presence of embedded message is highly imperceptible to any third party. Second, the embedded data can resist attacks to some extent because the attacker does not know the location of the secret data. Secret message can still be extracted after slight attack whereas modification to a number of coefficients will cause notice-

able distortion that may trigger alarm.

5 Coding techniques in steganography

Security is a paramount requirement of any undercover communication system based on steganography, security in the sense of being undetectable to both human viewer (listener) and statistical analysis. Also, to be of practical significance, a steganographic system must be able to convey sufficient amount of information. This section describes some coding techniques that aim at embedding more data without introducing additional distortion, or embedding the same quantity of data with less modification to the host for reduced distortion. Some of these techniques are independent of specific embedding schemes such as symmetric LSB embedding, histogram preserving algorithms, *etc.*, and are intended to be used in conjunction with these methods in order to further enhance performance.

5.1 Multiple-base notational system (MBNS) based steganography

To suit characteristics of the human visual system (HVS), more data can be inserted into busy areas in an image. In some methods, data embedding is performed in a block-wise fashion, *e.g.*, in the bit-plane complexity segmentation (BPCS) method[30]. Pixels in each block carry the same number of secret bits. It is possible, however, that even two adjacent pixels may tolerate steganographic modifications differently in terms of visual and statistical detectability. This property can be used to accommodate more secret data without introducing additional detectable traces.

A steganographic method has been proposed in which data to be hidden are expressed using a novel multiple-base notational system and then embedded into pixels according to the different degree of pixel value variation in the immediate neighborhood[31]. Embedding strength is varied over the entire host image on a pixel-by-pixel basis, allowing more secret data to be carried in busy areas.

Most stego systems express the stego-data in a binary form, and the amount of information contained in each symbol is exactly one bit. In order to embed more data into busy areas, the message can be expressed using a variable base system. In other words, the message is converted into a series of symbols with different information-carrying capability due to different bases used.

Express an integer number in the following form:

$$x = (d_{n-1}\, d_{n-2} \cdots\ d_2\, d_1\, d_0)_{b_{n-1} b_{n-2} b_2 b_1 b_0},$$
$$0 \leqslant d_i < b_i\ (i = 0, 1, \cdots, n-1), \tag{4}$$

where b_0, b_1, $\cdots$, b_{n+1} denote different bases corresponding respectively to the symbols d_0, d_1, $\cdots$, d_{n-1}. The decimal value of x is calculated as

$$x = d_0 + \sum_{i=1}^{n-1} \left(d_i \cdot \prod_{j=0}^{i-1} b_j \right). \tag{5}$$

Given a decimal number x and the bases, b_0, b_1, $\cdots$, b_{n-1}, a multiple-base expression can be obtained. For example, $49 = (1301)_{3532}$, and $158 = (3142)_{6254}$.

A secret message is embedded into the host by modifying pixels in an order derived from a key. Let each pixel carry one symbol of the message in a multiple base notational system, with the corresponding base being proportional to the degree of variation in the pixel's immediate neighborhood. Thus, pixels in busy areas carry more information and statistically undergo more modification than those in smooth areas. On the extraction side, a receiver can retrieve all the symbols and bases from the stego-image to recover the embedded message.

Performance comparison has been made among stego techniques based on MBNS, PVD and BPCS. All cover images are sized 512×512, and the payload is 4.4×10^5 bits (embedding rate = 0.21). The MBNS method provides the highest PSNR, the lowest Watson metric and the highest Q in all cases as listed in Table 2. PSNR indicates energy of distortion. The Watson metric uses HVS characteristics to measure the total perceptual error. The quality index Q combines correlation loss, luminance distortion and contrast distortion.

5.2 Matrix encoding

Usually, each designated space, *e.g.*, a pixel in the LSB method, is used to carry 1 bit of stego message. In case the size of data to be embedded is considerably smaller than the available host space, a large portion of the host is left unused. It is possible to make use of this spare host space for reduction of alterations needed for the same amount of stego-data so that the embedded information per change of the host is in effect increased. Or conversely, the amount of alterations made for embedding the same secret information is reduced.

Table 2 Performance comparison between MBNS and other methods

Host image	PSNR (dB)			Watson metric			Q		
	MBNS	PVD	BPCS	MBNS	PVD	BPCS	MBNS	PVD	BPCS
Lena	44.3	41.7	34.6	0.029	0.030	0.059	0.999 4	0.998 9	0.994 7
Baboon	41.4	36.2	26.8	0.028	0.045	0.127	0.999 4	0.996 8	0.971 8
Bridge	42.5	37.8	28.4	0.032	0.040	0.162	0.999 5	0.998 2	0.977 8
Peppers	45.0	41.2	33.5	0.030	0.032	0.073	0.999 6	0.999 0	0.994 1

In F5[26], a technique called matrix encoding is used for this purpose, which changes 1 bit in $(2^k - 1)$ host pixel to embed k bits of the stego-data. For simplicity, let us take $k = 2$ as an example ($k = 1$ corresponds to the simple LSB embedding). We can use the following operation to embed 2 bits, x_1 and x_2, into the LSB of 3 host data, a_1, a_2, and a_3:

$$\begin{cases} a_1, a_2 \text{ and } a_3 \text{ are unchanged} & \text{if } x_1 = a_1 \oplus a_3, x_2 = a_2 \oplus a_3, \\ \text{change LSB of } a_1 & \text{if } x_1 \neq a_1 \oplus a_3, x_2 = a_2 \oplus a_3, \\ \text{change LSB of } a_2 & \text{if } x_1 = a_1 \oplus a_3, x_2 \neq a_2 \oplus a_3, \\ \text{change LSB of } a_3 & \text{if } x_1 \neq a_1 \oplus a_3, x_2 \neq a_2 \oplus a_3, \end{cases} \quad (6)$$

where $\oplus$ is an exclusive-or operator. In extraction, $x_1 = a_1 \oplus a_3$, and $x_2 = a_2 \oplus a_3$. Here the average LSB flips for each embedded bit is 3/8, less than 1/2 of the ordinary LSB embedding. The price paid is that 3 host pixels instead of 2 are designated for embedding 2 bits of secret data. In other words, one bit more than the LSB embedding is consumed. The general form of matrix encoding is referred to the literature.

5.3 Stego-encoding and error correction

Matrix encoding can be viewed as a special case of the cyclic coding[32], which we will refer to as stego-encoding in the following. By designating more host samples, the stego-encoding reduces the number of LSB alterations, hence providing improved security. The drawback, however, is that slight noise can destroy the embedded message since each bit of error introduced by channel noise or active attack will cause more errors in message extraction.

To combat active attacks, a frequently used approach is to introduce error-correction codes, which, however, inevitably increases the required amount of bit alterations so that the probability of the secret data being detected will increase.

For this reason, a novel encoding technique has been proposed, in which the stego-encoding is presented in a suitable way and combined with an error-correction scheme when a substantial amount of the host samples are available (see Ref. [5], pp. 166 – 169). The technique provides error-correction capability so that the embedded data have better chance to survive interferences of channel noise or active attacks while keeping low distortion caused by information hiding. The penalty is, of course, an additional increase of the host data needed for embedding the same quantity of secrete data. Table 3 summarizes the performance of the different encoding techniques, in which the '+/–' symbols represent the merits/drawbacks in each specification. The proposed combination encoding provides the best overall security both in terms of imperceptibility and robustness.

Table 3 Performance of steganographic techniques with different coding schemes

Steganographic techniques	Embedding rate (Payload)	Security	
		Embedding efficiency (Imperceptibility)	Robustness against channel noise
Plain LSB	+ + + + +	+ + +	+
Stego-encoding	+ + + +	+ + + +	–
Cyclic encoding + Plain LSB	+ + + +	+	+ + +
Combination encoding (stego + cyclic)	+ + +	+ + +	+ + +

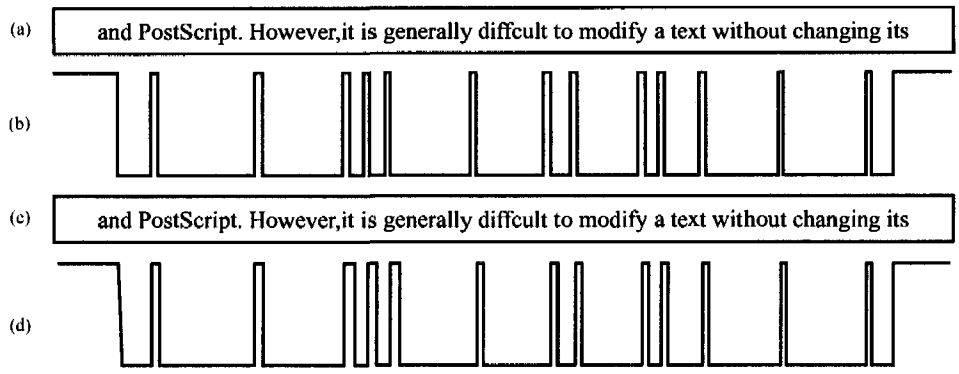
6 Data hiding in text

Since text is by far the most important media for information conveyance over the Internet, it is of interest to use various text files as covers in hidden communications. The candidate media include web pages, email messages, and downloadable files such as pdf and PostScript. However, it is generally difficult to modify a text without changing its contents or appearance because it contains very little redundancy as compared to digital image or audio.

Nonetheless there are several ways to embed secret data into text as summarized by Bender, *et al.* in their frequently cited paper[1]. These belong to three major categories: open space methods, syntactical methods, and semantic methods. The open space methods insert additional information into a text by changing some format attributes, *e.g.*, adding spaces between words, appending invisible characters to line trails, adjusting line spacings, *etc*. The syntactical methods use sentence patterns or punctuations to carry data. For example, "a, b, and c" and "a, b and c" may represent 0 and 1 respectively. The semantic techniques change words or expressions based on a thesaurus of specially defined synonyms. The word "big" may mean a zero, while its equivalence "large" means one.

Embedding capacity of the syntactical methods is usually small as the number of usable patterns is small. The semantic methods inevitably cause some changes in the meaning or style of the cover text, therefore are prone to arouse suspicion. It is the format-based technique that has received considerable research interests[33,34].

We have developed a method[35] for embedding secret information into text using the typesetting tool TeX, exporting the stego-text in the form of an Acrobat pdf file, and extracting the hidden data from the JPEG image converted from pdf. Spaces between words are altered using TeX functions to encode an encrypted binary sequence. In reception, the embedded data can reliably be extracted by taking the widths of spaces as shown in Fig. 6 where modifications to the inter-word spaces is exaggerated for explanatory purpose. Synchronization is established by locating a wider space after a full stop.



(a) Original carrier text; (b) Output of the image analyzer in which the space after a sentence is slightly larger than those between words; (c) Stego-text; (d) Image analyzer output showing two widened spaces that carry embedded data

Fig.6 Extraction of information embedded in text from a pdf generated image

7 Summary

In this article we have reviewed some of the main techniques in steganography and steganalysis, an important area of research in information security. Although great many researchers are currently involved in various aspects of this challenging topic, leading to a huge amount of publications and applications, the current techniques are far from maturing. On the other hand, the extent of the research area is vast, ranging from basic theory to practical applications, from performance embedding schemes to sophisticated approaches to detection of highly imperceptible hidden information, from data hiding in ordinary multimedia contents to messages inserted in various forms of other media such as the metadata of proprietary software outputs, and in the application aspect, from covert communications to computer forensics inspections. Only some typical techniques and, especially, those having close relations with the work carried out in the authors' laboratory are covered. The emphasis has been laid on the authors' research accomplishments.

Further studies being conducted or under consideration include new embedding algorithms based on arbitrary block/pair division of images, secure steganography in binary images, covert communication through digital speech channels, new stego-encoding methods with enhanced embedding efficiency, combination of stego encoding and other techniques such as histogram preserving techniques, applications of sparse represen-

tation to steganography/steganalysis, steganalysis of symmetric LSB embedding in color images, statistical analysis of hidden data in digital audio, more sophisticated approaches to data hiding in text and countermesures, both format-based and syntactic/semantic, computer forensic inspections based on steganalysis, steganalysis and active attack in the network environment, theoretical studies on security and embedding capacity, development of steganalysis systems, etc.

References

[1] Bender W, Gruhl D, Morimoto N, *et al*. Techniques for data hiding[J]. *IBM System Journal*, 1996, **35**(3, 4): 313 - 336.

[2] Memon N, Wong P W. Protecting digital media content [J]. *Communications of the ACM*, 1998, **41**(7): 34 - 43.

[3] Johnson N F, Jajodia S. Exploring steganography: seeing the unseen[J]. *IEEE Computer*, 1998, **31**(2): 26 - 34.

[4] Provos N, Honeyman P. Hide and seek: an introduction to steganography[J]. *IEEE Security* and *Privacy*, 2003, **1**(3): 32 - 44.

[5] Wang S, Zhang X, Zhang K. *Steganography and Steganalysis: Techniques of Cyber Warfare in the Internet Age*[M]. Tsinghua University Press, Beijing, April 2005 (in Chinese).

[6] Wang H, Wang S. Cyber warfare: steganography *vs*. steganalysis[J]. *Communication of the ACM*, 2004, **47** (10): 76 - 82.

[7] Kovacich G L, Jones A. What infoSec professionals should know about information warfare tactics by terrorists[J]. *Computers and Security*, 2002, **21**(1,2): 35 - 41, 113 - 119.

[8] Fridrich J, Goljan M. Practical steganalysis of digital images - state of the art[A]. *Security and Watermarking of Multimedia Contents* IV, *Proceedings of SPIE* [C]. 2002, **4 675**: 1 - 13.

[9] Fisk G, Fisk M, Papadopoulos C, *et al*. Eliminating steganography in internet traffic with active wardens[A]. *Proceedings of the 5th International Workshop on Information Hiding*[C]. 2002, 18 - 35.

[10] Westfeld A, Pfitzmann A. Attacks on steganographic systems[J]. *Lecture Notes in Computer Science*, 1999, **1 768**: 61 - 76.

[11] Zhang X, Wang S, Zhang K. Steganalysis against LSB insertion using statistical method[J]. *Journal of Applied Sciences*, 2004, **22**(1): 16 - 19 (in Chinese).

[12] Zhang X, Wang S, Zhang K. A novel LSB steganography scheme against statistical analysis[J]. *Journal of Image and Graphics*, 2003, **8**(9): 1 055 - 1 060 (in Chinese).

[13] Ker A D. Steganalysis of LSB matching in grayscale images[J]. *IEEE Signal Processing Letters*, 2005, **12**(6): 441 - 444.

[14] Harmsen J, Pearlman W. Higher-order statistical steganalysis of palette images[A]. *Proceedings of SPIE*[C]. 2003, **5 020**: 131 - 142.

[15] Fridrich J, Du R, Long M. Steganalysis of LSB encoding in color images[A]. 2000 *IEEE Int. Conf. on Multimedia and Expo*.[C]. 2000, **3**: 1 279 - 1 282.

[16] Wang S, Zhang X, Zhang K. Steganographic technique capable of withstanding RQP analysis [J]. *Journal of Shanghai University*, 2002, **6**(4): 273 - 277.

[17] Provos N. Defending against statistical steganalysis[A]. *Proc. of 10th USENIX Security Symposium* [C]. Washington D C, 2001, 323 - 335.

[18] Zhang X, Wang S, Zhang K. Steganography with the least histogram abnormality[J], *Lecture Notes in Computer Science*, 2003, **2 776**: 401 - 412.

[19] Wu D C, Tsai W H. A steganographic method for images by pixel-value differencing[J]. *Pattern Recognition Letters*, 2003, **24**: 1 613 - 1 626.

[20] Zhang X, Wang S. Vulnerability of pixel-value differencing steganography to histogram analysis and modification for enhanced security [J]. *Pattern Recognition Letters*, 2004, **25**: 331 - 339.

[21] Chang C C, Tseng H W. A steganographic method for digital images using side match[J]. *Pattern Recognition Letters*, 2004, **25**: 1 431 - 1 437.

[22] Wang W, Zhang X, Wang S. Hidden data detection and payload estimation against side match steganography[A]. *Proc. of the 12th National Conference on Image and Graphics* [C]. *Journal of Image and Graphics*, Oct. 2005, 105 - 108 (in Chinese).

[23] Fridrich J, Rui D. Secure steganographic methods for palette images[J]. *Lecture Notes in Computer Science*, 2000, **1 768**: 47 - 60.

[24] Zhang X, Wang S. Detection of OPA stego-data and secure steganography in palette images[J]. *Acta Electronica Sinica*, 2004, **32**(10): 1 702 - 1 705 (in Chinese).

[25] Fridrich J, Goljan M, Du R. Steganalysis based on JPEG compatibility[A]. *Proceedings of SPIE*[C]. 2001, **4 518**: 275 - 280.

[26] Westfeld A. F5 - a steganographic algorithm[J]. *Lecture Notes in Computer Science*, 2001, **2 137**: 289 - 302.

[27] Fridrich J, Goljan M, Hogea D. Steganalysis of JPEG image: breaking the F5 algorithm [J]. *Lecture Notes in Computer Science*, 2002, **2 578**: 310 - 323.

[28] Zhang X, Wang S. Secure steganographic algorithm in JPEG images[J]. *Journal of Electronics and Information Technology*, 2005, 1 813 - 1 817 (in Chinese).

[29] Zhang X, Wang S. Lossless data hiding in JPEG images [J]. *Journal of Image and Graphics*, 2003, **8**: 563 - 566

(in Chinese).

[30] Noda N, Spaulding J, Shirazi M N, *et al*. Application of bit-plane decomposition steganography to JPEG 2000 encoded images [J]. *IEEE Signal Processing Letters*, 2002, **9**: 410 - 413.

[31] Zhang X, Wang S. Steganography using multiple-base notational system and human vision sensitivity [J]. *IEEE Signal Processing Letters*, 2005, **12**(1): 67 - 70.

[32] Dijk M, Willems F. Embedding information in grayscale images[A]. *Proc. 22nd Symp. Inform. Theory in the Benelux*[C]. The Netherlands, 2001, 147 - 154.

[33] Maxemchuk N F, Low S H. Performance comparison of two text marking method [J]. *IEEE Journal Selected Areas of Communications*, 1998, **16**(4): 561 - 572.

[34] Takizawa Q, Takizawa O, Makino K, *et al*. Method of hiding information in agglutinative language documents using adjustment to new line positions[J]. *LNCS/LNAI*, 2005, **3 683**: 1 039 - 1 048.

[35] Chen C, Wang S, Zhang X. Data hiding in text file using TeX and fxtraction of hidden data from document image [J]. *Journal of Applied Sciences* (to appear, in Chinese).

(*Editor YAO Yue-yuan*)