A High-Capacity Image Data Hiding Scheme Using Adaptive LSB Substitution

Hengfu YANG [1,2], Xingming SUN [1], Guang SUN [1,3]

[1]School of Computer and Communication, Hunan University, no. 252, Lushan South Road, Changsha, 410082, China
[2]Dept. of Information Science & Engg., Hunan First Normal Univ., no. 1015, Fenglin 3rd Road, Changsha, 410205, China
[3]Information Management Dept., Hunan Financial and Economic Coll., 139, Fenglin 2nd Road, Changsha, 410205, China

sunnudt@163.com, hengfuyang@hotmail.com, hengfuyang@163.com

Abstract. *Many existing steganographic methods hide more secret data into edged areas than smooth areas in the host image, which does not differentiate textures from edges and causes serious degradation in actual edge areas. To avoid abrupt changes in image edge areas, as well as to achieve better quality of the stego-image, a novel image data hiding technique by adaptive Least Significant Bits (LSBs) substitution is proposed in this paper. The scheme exploits the brightness, edges, and texture masking of the host image to estimate the number k of LSBs for data hiding. Pixels in the noise non-sensitive regions are embedded by a k-bit LSB substitution with a lager value of k than that of the pixels in noise sensitive regions. Moreover, an optimal pixel adjustment process is used to enhance stego-image visual quality obtained by simple LSB substitution method. To ensure that the adaptive number k of LSBs remains unchanged after pixel modification, the LSBs number is computed by the high-order bits rather than all the bits of the image pixel value. The theoretical analyses and experiment results show that the proposed method achieves higher embedding capacity and better stego-image quality compared with some existing LSB methods.*

Keywords

Data Hiding, Adaptive Least Significant Bits Substitution, Human Visual System, High Embedding Capacity, Optimal Pixel Adjustment Process.

1. Introduction

With the development of the Internet and information processing technique, as an effective solution for copyright protection and information security, data hiding technique has been receiving much attention today.

Many data hiding methods have been proposed to hide secret data into an image [1-5]. Data payload (embedding capacity) and imperceptibility are the two most important properties of a data hiding system. Generally, data hiding schemes are categorized as LSB substitution, LSB matching and Pixel-Value Differencing (PVD). LSB substitution is the most commonly used method directly replacing the LSBs of pixels in the cover image with secret bits to get the stego-image [6, 7]. The LSB matching scheme was introduced by A. Ker et al., [8]. LSB matching also modifies the LSBs of the cover image for data hiding, but it does not simply replace the LSBs of the cover image as LSB replacement does. On the other hand, if one secret bit does not match the LSB of the cover image, then another one will be randomly added or subtracted from the cover pixel value [9-11]. PVD method provides good imperceptibility by calculating the difference of two consecutive pixels to determine the depth of the embedded bits [12]. This paper focuses on LSB replacement and PVD methods. The simple LSB scheme is limited mainly by artificial noises in the smooth regions of the image. Artificial noises seriously damage visual quality of the stego-image. To improve the perceptual quality of the stego-image, Wang et al. [13, 14] employed a genetic algorithm to generate a substitution table. According to this substitution table, the value of the secret data to be embedded into each host pixel is transformed to another value in advance which is closer to the original value of the host pixel; however, owing to the nature of a genetic algorithm, although the substitution table is good, it may not be the optimal solution. In order to obtain the optimal solution, Chang et al. [15, 16] proposed their dynamic programming strategy to efficiently pick out the best from all possible substitution tables. But the optimal substitution process may require huge computational cost because of using genetic algorithm and dynamic programming strategy. In Chan et al.'s methods [17, 18], the genetic algorithm is not required. An Optimal Pixel Adjustment Process (OPAP) is used to improve efficiency and enhance the visual quality of the stego-image generated by simple LSB substitution. The above-mentioned LSB techniques [13-18] replace the same length bits of each original pixel with the embedding data. However, not all pixels in the image can tolerate equal amounts of changes without noticeable distortion. Therefore, the stego-image has low quality when equally changing LSBs of all pixels. To solve this issue, some LSB based methods employed Human Visual System (HVS) masking characteristics to embed the secret data into the variable sizes of LSBs of each pixel

[19-22]. W. N. Lie et al. [19] created a piecewise mapping function according to the HVS contrast sensitivity to determine the adaptive numbers of LSBs for data hiding. Lee et al. [20] exploited the contrast and luminance property of HVS and achieved a variable-sized LSB insertion. In S. H. Liu et al.'s methods [21], each pixel of the original image is grouped according to its intensity, then the frequency of the original pixel in each group is counted, and a bitplane-wise data hiding method is used to embed the secret message into the original image by the principle of the pixel with high frequency priority. Similarly, Kekre et al. [22] determined the embedded capacity of each pixel by considering the luminance from the highest bits residual image. To further improve the quality of the stego-image, some PVD methods [23, 24] were proposed, and these schemes utilized the HVS sensitivity to intensity variations from smoothness to high contrast by the selection of the width of the range which the difference value of two neighbor pixels belongs to. Ref. [25, 26] checked more than two neighborhood pixels to determine the payload of each pixel; however, the embedding capacity of these methods is far less than that of PVD methods. Furthermore, Ref. [27, 28] used the Multi-Pixel Differencing (MPD) to estimate smoothness of each pixel. By combining the LSB insertion and PVD methods, Wu et al. [29] proposed a data hiding scheme with a better image quality by using PVD methods alone. In their approach, two consecutive pixels are embedded by the LSB replacement method if their difference value falls into a lower level; similarly, the PVD method is used if the difference value falls into a higher level. In other words, the secret data is hidden into the smooth areas by LSB substitution and PVD methods in the edge areas. Yang et al. [30] proposed an adaptive LSB steganographic method using PVD and LSB replacement. In their scheme, the difference value of two consecutive pixels is used to estimate the hiding capacity into the two pixels. Pixels located in the edge areas are embedded by a k-bit LSB substitution method with a greater value of k than that of the pixels located in smooth areas. The scheme embeds more secret data into edged areas than smooth areas in the host image.

From the above analysis, we can see that: (1) some simple LSB approaches equally change the LSBs of all pixels and have poor visual quality of the stego-image [13-18]; (2) Some improved LSB schemes [19-22] do not fully exploit the HVS masking characteristics, especially the edge masking effect, and they cannot obtain good imperceptibility; (3) Still other PVD related hiding methods follow the principle that the edge areas can tolerate more changes than smooth areas [23-30]. However, this principle obeyed by some existing data hiding schemes does not discriminate texture features from edge ones; the edge areas used by these schemes [23-30] contain both edges and textures. We know edges and sharp details are the most important structural information of an image, and human eyes are more sensitive to edges than textures [31, 32]. We should avoid abrupt changes in the image edge areas during the data embedding procedure [33]. In this paper, a novel adaptive image steganographic method is proposed. The proposed scheme obeys the principle that edge areas cannot endure abrupt changes, and can embed a large number of secret data while achieving high quality of the stego-image.

The rest of this paper is organized as follows. The human visual masking model is described in Section 2. The proposed method is presented in Section 3. Experiments are shown in Section 4, and analyses and discussions are given in Section 5. Conclusions are drawn in Section 6.

2. Human Visual Masking Model in Spatial Domain for Data Hiding

Designing image adaptive steganographic schemes with human visual perception can obtain higher capacity and lower distortion. In this approach, we exploit the luminance masking, texture masking and edge masking features of the high order image generated by extracting high order bits of the original image and create a spatial HVS masking model in a better way, and then use the visual masking model to develop an adaptive data hiding scheme.

Human eyes usually have different sensitivity to different luminance. In fact, human eyes are more sensitive to changes in the areas with middle level luminance, while less sensitive to changes in those areas with high and low gray-scale values. So, the luminance masking of each pixel can be estimated as

$$\alpha(i,j) = \frac{\left|x(i,j) - 128\right|}{128} \tag{1}$$

where $x(i,j)$ is the pixel value at the spatial position (i, j) of the host image $\boldsymbol{I}$.

Moreover, distortions are much less visible in highly textured regions than in smooth areas. The smooth regions possess smaller entropy value, while the textured areas possess greater entropy value. Hence, we can depict the texture masking by using the entropy value of the sliding window (All the calculations are based on the image block of size $(2l + 1) \times (2l + 1)$, where $1 \le l \le 4$). Greater entropy value corresponds to the texture or edge regions, while smaller entropy value corresponds to the flat areas. Let $H(i,j)$ be the entropy value of sub-block centered by the pixel at the position (i, j), and the entropy $H(i, j)$ can be used to depict approximately the texture characteristics of the pixel at the position (i, j). This maximum entropy is achievable when all of the gray-levels have the same probability. In other words, an image block receives its maximum entropy when it contains the same number of all of the gray-scale values in that block. For a 256-level image block with size $(2l + 1) \times (2l + 1)$, the maximum entropy value $H_{\max}$ is computed by

$$H_{\max} = -\sum_{i=-l}^{l}\sum_{j=-l}^{l}\frac{1}{(2l+1)^2}\log_2\left(\frac{1}{(2l+1)^2}\right) = 2\log_2(2l+1). \tag{2}$$

Using $H_{\max}$ as the normalization factor, the normalized entropy $\beta(i, j)$ of each pixel can be obtained by the formula

$$\beta(i,j)=\frac{H(i,j)}{H_{\max}}. \tag{3}$$

Image areas with prominent edges have greater variance value, while smooth image areas have smaller variance value. Let $V(i, j)$ be the variance (mean square error) of the image block centered by the pixel $I(i, j)$. Therefore, we can use the variance $V(i, j)$ of the image blocks to indicate the edge feature. In addition, we know that the maximum variance is in the block where adjacent pixels have the maximum and minimum permissible gray-scale value. The maximum variance $V_{\max}$ is given by

$$V_{max}=\frac{\left(2l^2+2l\right)\left(2l^2+2l+1\right)}{\left(2l+1\right)^4}G^2 < \left(\frac{\left(2l^2+2l+\frac{1}{2}\right)}{\left(2l+1\right)^2}G\right)^2=\left(\frac{G}{2}\right)^2. \tag{4}$$

where G is the maximum permissible gray-scale value. Now, we can get the normalized variance $\gamma(i, j)$ as follows

$$\gamma(i,j)=\frac{V(i,j)}{V_{\max}}=\frac{V(i,j)}{(G/2)^2}. \tag{5}$$

It is well known that sharp edges play an important role in human spatial vision [34]. To achieve good imperceptibility, a good data hiding scheme should prevent abrupt changes in edge areas. Because of large entropy values corresponding to the texture or edge areas, the texture masking also includes the impact of the edge parts when it is calculated by the entropy. To avoid corrupting the edge easily and causing severe distortion to the original image during data hiding, we must ensure low hiding capacity in the edge areas. Based on all the above considerations, the effect of HVS masking characteristics is expressed by the formula

$$\phi(i,j)=\alpha(i,j)\times\{\beta(i,j)-\gamma(i,j)\}. \tag{6}$$

Now, we can compute the bit depth $k'(i, j)$ of each pixel that can be used for data hiding by the following formula

$$k'(i,j)=round\left\{(7-r-1)\times\frac{\phi(i,j)-min(\phi)}{max(\phi)-min(\phi)}+1\right\}. \tag{7}$$

where $1\le r\le 6$, $1\le k'(i,j)\le 7-r$, and r represents the highest bits number of each pixel used to calculate the hiding capacity in each pixel. Function *round*(), *max*() and *min*() return the nearest integer, the maximum and minimum value of an expression respectively.

Finally, in order to ensure that the bit depth $k'(i, j)$ of each pixel obeys uniform distribution as far as possible, histogram equalization is applied to the bit depth $k'(i, j)$ to obtain the final number $k(i, j)\,k(i, j)$ of LSBs in each pixel for data hiding. Fig. 1 illustrates the relation between the adaptive number $k(i, j)$ of LSBs and the number r of highest bits for the calculation of the hiding capacity in each pixel.

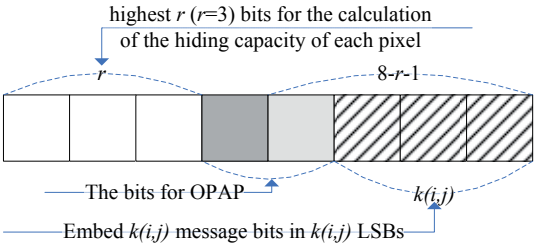


Fig. 1. Relation between the adaptive LSBs number $k(i, j)$ and the highest bits number r in each pixel.

3. Proposed Steganographic Scheme with Adaptive LSB Substitution

To obtain high embedding capacity and good invisibility of the stego-image, firstly, we model the HVS masking effect in a better way (see the above section), and then a new image steganographic method is proposed by using the adaptive LSB method and the OPAP presented by Chan [17, 18]. The proposed method is based on the concept that edge areas can tolerate a smaller number of changes than highly textured areas, and not more changes than smooth areas. In fact, the method embeds more secret data into noise non-sensitive areas than noise sensitive areas. Here, the calculation of hiding capacity $k(i, j)$ of each pixel is based on the highest r bits of each pixel in the cover image so that the adaptive number $k(i, j)$ of LSBs of each pixel should remain unchanged before and after data hiding and the adaptation can be achieved with no overhead.

3.1 Data Hiding

Let $\boldsymbol{I}$ be the original 256-level grayscale image of size $m\times n$ represented as

$$I=\left\{x(i,j)\middle|\begin{matrix}0\le i<m,0\le j<n,\\ x(i,j)\in\{0,1,...,255\}\end{matrix}\right\}. \tag{8}$$

W be the t-bit secret data represented as

$$W=\{w(i)|0\le i<t,w(i)\in\{0,1\}\}. \tag{9}$$

The detailed data hiding algorithm is given as follows.

Step 1: Extract the highest r (say r= 3) bits of the original image $\boldsymbol{I}$ to get the residual image I_r.

Step 2: Calculate the adaptive number $k(i, j)$ of LSBs of each pixel in the original cover-image based on the residual image I_r using (7).

Step 3: Generate a pseudo random sequence P with number 0 and 1 by a secret key defined as

$$P = \left\{ p(i) \middle| 0 \le i < t, p(i) \in \{0,1\} \right\}. \tag{10}$$

The ultimate secret data $\tilde{W}$ for hiding is obtained by applying the element-wise XOR operation of the original secret messages $\boldsymbol{W}$ and the pseudo random sequence $\boldsymbol{P}$ represented as

$$\tilde{W} = \left\{ \tilde{w}(i) \middle| \tilde{w}(i) = w(i) \otimes p(i), 0 \le i < t \right\}. \tag{11}$$

where $\otimes$ denotes XOR operator (the same below).

Step 4: For the (i, j)th pixel of original image $\boldsymbol{I}$, $k(i, j)$ bits binary secret data are read from the ultimate secret data $\tilde{W}$ one by one denoted as $b(i, j)$, and then transform the binary number b into its decimal value $d(i, j)$. For example, assume $b(i, j) = 1001_{(2)}$, then $d(i, j) = 9$.

Step 5: Hide $k(i, j)$ bits binary secret data $b(i, j)$ into the cover-image $\boldsymbol{I}$ by replacing the $k(i, j)$ LSBs of the pixel value $x(i, j)$ with the integer $d(i, j)$, the resulting gray-scale value of the stego-pixel is expressed as

$$x'(i, j) = x(i, j) - x(i, j) \bmod 2^{k(i,j)} + d(i, j). \tag{12}$$

Step 6: To reduce the hiding error between $x(i, j)$ and $x'(i, j)$, the OPAP [17, 18] is used to enhance the quality of stego-image obtained by simple LSB methods. Which bits of each pixel value are used for OPAP is shown in Fig. 1. Let $\delta(i, j)$ be the hiding error between $x(i, j)$ and $x'(i, j)$ which is given by $\delta(i, j) = x'(i, j) - x(i, j)$, where $-2^{k(i,j)} < \delta(i, j) < 2^{k(i,j)}$. The new gray-scale value $x''(i, j)$ of the final stego-image S can be obtained by adjusting the gray-scale value $x'(i, j)$ with the following formula.

$$x''(i, j) = \begin{cases} x'(i, j) - 2^{k(i,j)}, & \text{if } 2^{k(i,j)-1} < \delta(i, j) < 2^{k(i,j)} \text{ and } x'(i, j) \bmod 2^{8-r} \ge 2^{k(i,j)}; \\ x'(i, j), & \text{if } 2^{k(i,j)-1} < \delta(i, j) < 2^{k(i,j)} \text{ and } x'(i, j) \bmod 2^{8-r} < 2^{k(i,j)}; \\ x'(i, j), & \text{if } -2^{k(i,j)-1} \le \delta(i, j) \le 2^{k(i,j)-1}; \\ x'(i, j), & \text{if } -2^{k(i,j)} < \delta(i, j) < -2^{k(i,j)-1} \text{ and } x'(i, j) \bmod 2^{8-r} \ge 2^{8-r} - 2^{k(i,j)}; \\ x'(i, j) + 2^{k(i,j)}, & \text{if } -2^{k(i,j)} < \delta(i, j) < -2^{k(i,j)-1} \text{ and } x'(i, j) \bmod 2^{8-r} < 2^{8-r} - 2^{k(i,j)}. \end{cases} \tag{13}$$

3.2 Data Extraction

In the data extraction process, given the stego-image S, the hidden messages can be readily extracted without referring to the original cover-image. The extraction process consists of the following steps.

Step 1: Extract the highest r (say r= 3) bits of the final stego-image $\boldsymbol{S}$ to get the residual image S_r, note that S_r is the same as I_r since data hiding is not applied to the highest r bits of each pixel.

Step 2: Calculate the adaptive number $k(i, j)$ of LSBs of each pixel in the stego-image based on the residual image S_r using (7).

Step 3: Extract $k(i, j)$ LSBs of the (i, j)th pixel value $x''(i, j)$ of stego-image $\boldsymbol{S}$ directly. Let $d'(i, j)$ denote the extracted secret data, and it can be defined as

$$d'(i, j) = x''(i, j) \bmod 2^{k'(i,j)}. \tag{14}$$

Then the secret message $b'(i, j)$ is obtained by transforming the decimal value $d'(i, j)$ to a binary string with $k(i, j)$ bits.

Step 4: Repeat Step 1-3 until all secret data W' is obtained. Finally, the final secret messages W'' can be obtained by the element-wise XOR operation of the secret data W' and the pseudo random sequence $\boldsymbol{P}$ generated by the same method in data hiding, and it can be expressed as

$$W'' = \left\{ w''(i) \middle| w''(i) = w'(i) \otimes p(i), 0 \le i < t \right\}. \tag{15}$$

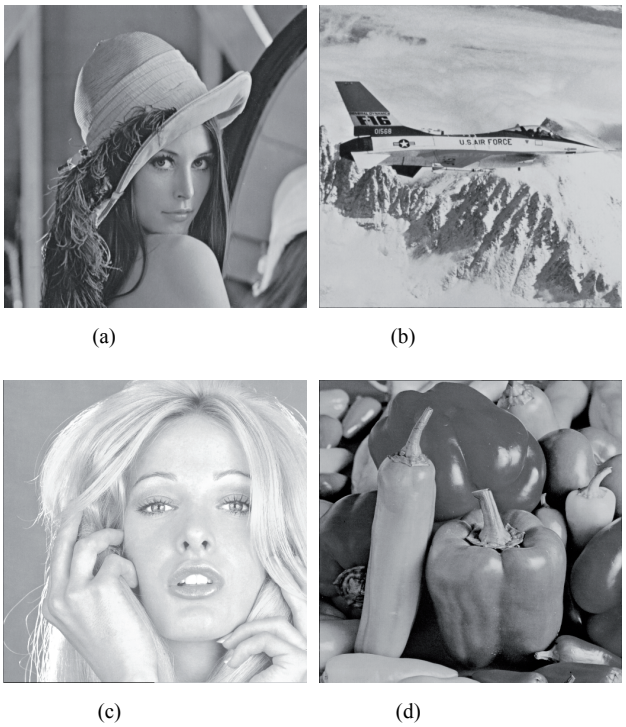
4. Experimental Results

In the experiments, some different types of grayscale images with size of 512×512 are used as the cover-images, and four of them are shown in Fig. 2. We set the slide window size in (2) l = 1. This paper adopts the Peak Signal-to-Noise Ratio (PSNR) to evaluate the qualities of the stego-images. To illustrate the imperceptibility of the proposed steganographic method, Fig. 3 shows the corresponding stego-images of four cover images in Fig. 2 obtained by the proposed scheme, where the number of highest bits r=4 is used. Fig. 4 shows the difference between the cover-image and the stego-image by the proposed method, and the gray-scale values in the difference images are scaled by 20 times.

From Fig. 3, we can notice that there are no perceptible distortions occurring on edge areas by observing the stego-images generated by the presented method. In the experiments, the PSNR values for all the test images processed by the proposed method turned out to be higher than 39 dB with r = 4, which means the distortion caused by the proposed method is imperceptible to the human eyes. The proposed scheme can achieve good imperceptibility. It is partially because the proposed scheme obeys the concept that the edge areas cannot tolerate great change, and then embeds more secret data into noise non-sensitive areas than noise sensitive areas. In addition, as shown in Fig. 4, the embedding watermark is adaptive to the original image features by observing the difference images. There is low watermark strength in image edge areas. In reality, data hiding has higher capacity in noise non-sensitive regions than noise sensitive ones. Even any visual difference is hardly noticeable on the watermarked image because of the full utilization of HVS masking characteristics.

Furthermore, we have also compared the proposed scheme with Wu et al.'s method [29]. The detailed comparison results are listed in Tab. 1. On average, one can see

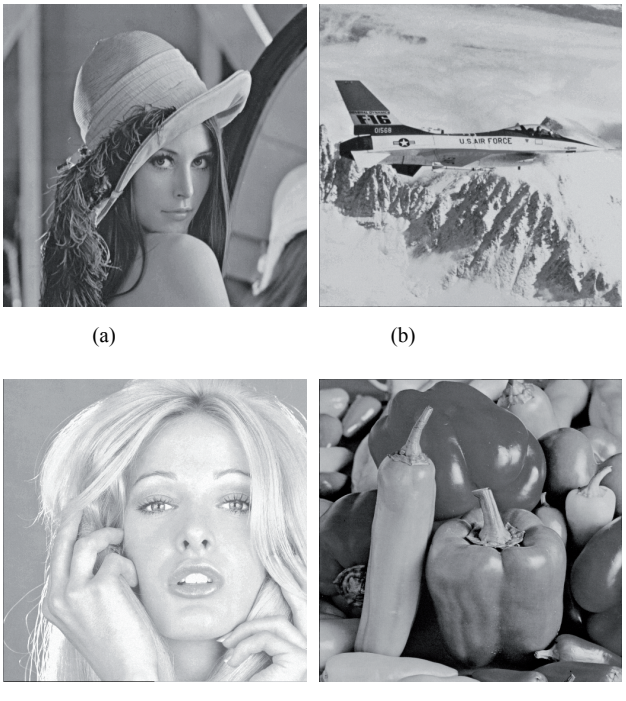
that the proposed scheme with r = 4 obtains 13049 more bits than Wu et al.'s while the PSNR value increases by 2.14 dB



(a) (b)

(c) (d)

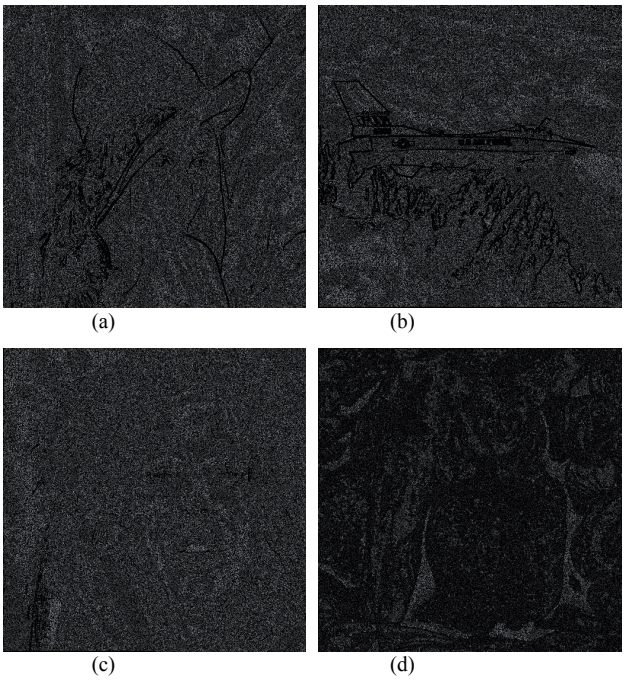
Fig. 2. Four cover images. (a) Lena. (b) F16. (c) Tiffany. (d) Peppers.



(a) (b)

(c) (d)

Fig. 3. Four stego-images generated by the proposed scheme. (a) Lena (embedded data are 757332 bits, PSNR is 39.3134 dB). (b) F16 (embedded data are 735236 bits, PSNR is 39.5478 dB). (c) Tiffany (embedded data are 777888 bits, PSNR is 39.1234 dB). (d) Peppers (embedded data are 786014 bits, PSNR is 39.0636 dB).



(a) (b)

(c) (d)

Fig. 4. The difference images between the cover-image and the stego-image by the proposed scheme. (a) Lena. (b) F16. (c) Tiffany. (d) Peppers.

Cover images	Wu et al.'s method [29]		The proposed method	
	Capacity (bits)	PSNR (dB)	Capacity (bits)	PSNR (dB)
Elaine	755027	37.25	761204	39.32
Lena	757000	38.22	757332	39.31
Baboon	720288	34.26	785572	39.16
Peppers	776160	37.46	786014	39.06
Toys	769529	36.91	785376	38.89
Girl	776308	37.14	785482	38.71
Goldhill	764345	37.41	742300	39.48
Barbara	744389	36.33	785134	39.06
Zelda	781306	37.61	785896	39.11
Tiffany	777356	37.27	777888	39.12
average	762171	36.99	775220	39.12

Tab. 1. Comparison of results of Wu et al.'s and the proposed methods with r=4.

5. Analyses and Discussions

In order to further evaluate the performance of the proposed method, we test some different images by using various number of highest bits r where r=1-6. The detailed results of four test images “Lena”, “F16”, “Tiffany” and “Peppers” are listed in Tab. 2. The overall performance of the scheme with various r on different type of images is given in Tab. 3. From Tab. 2, it can be seen that the hiding capacity of each image is different according to the noise sensitivity of the cover image. The higher the noise sensitivity of the cover image, the lower the hiding capacity, which in part indicates the effectiveness of the proposed HVS masking model in Sec. 2. In addition, this approach has relatively steady performance for much different types of images, and the hiding capacity monotonously increases and PSNR value decreases with the highest bits numbers r for HVS computation, respectively (See Tab. 3).

r	Lena			F16			Tiffany			Peppers		
	bit rate (bpp)	Capacity (bits)	PSNR (dB)	bit rate (bpp)	Capacity (bits)	PSNR (dB)	bit rate (bpp)	Capacity (bits)	PSNR (dB)	bit rate (bpp)	Capacity (bits)	PSNR (dB)
1	5.3566	1404200	22.22	5.4515	1429077	23.12	5.9001	1546664	21.37	5.4813	1436888	22.54
2	4.3120	1130377	28.44	4.7288	1239624	27.53	4.9900	1308092	27.36	4.9684	1302440	27.26
3	3.5255	924198	34.54	3.8218	1001866	33.59	3.7186	974815	33.89	3.9915	1046341	33.02
4	2.8890	757332	39.31	2.8047	735236	39.55	2.9674	777888	39.12	2.9984	786014	39.06
5	1.9921	522218	45.14	1.9749	517702	45.25	1.9982	523815	45.13	1.7976	471221	45.77
6	1.0000	262144	51.14	1.0000	262144	51.15	1.0000	262144	51.14	1.0000	262144	51.15

Tab. 2. The embedding capacity and PSNR values of four test images for r=1-6.

r	bit rate (bpp)	Capacity (bits)	PSNR (dB)
1	5.2634	1379767	22.69
2	4.4940	1178068	28.45
3	3.7809	991137	33.65
4	2.9425	771354	39.23
5	1.9561	512787	45.27
6	1.0000	262144	51.14

Tab. 3. The average hiding capacity and PSNR values of the proposed method with r=1-6.

In fact, we can derive the expectation of the PSNR values of the stego-images produced by the resented scheme for various number of highest bits r. The following section will discusses the expectation of the PSNR values of the stego-images produced by this scheme.

For a single pixel $x(i,j)$, the hiding error between $x'(i,j)$ and $x(i,j)$ meets $-2^{k(i,j)} < \delta(i,j) < 2^{k(i,j)}$. Let $\delta'(i,j) = x''(i,j) - x(i,j)$ be the hiding error between $x''(i,j)$ and $x(i,j)$. $\delta'(i,j)$ can be computed as follows by the similar analysis in [18]:

$$
\begin{aligned}
&Case\ 1: 2^{k(i,j)-1} < \delta(i,j) < 2^{k(i,j)} \\
&\quad and\ x'(i,j) \bmod 2^{8-r} \ge 2^{k(i,j)} \\
&\delta'(i,j) = x''(i,j) - x(i,j) = x'(i,j) - 2^{k(i,j)} - x(i,j) \\
&\quad = \delta(i,j) - 2^{k(i,j)} \\
&\quad \Rightarrow 2^{k(i,j)-1} - 2^{k(i,j)} < \delta'(i,j) < 2^{k(i,j)} - 2^{k(i,j)} \\
&\quad \Rightarrow -2^{k(i,j)-1} < \delta'(i,j) < 0 \\
&Case\ 2: 2^{k(i,j)-1} < \delta(i,j) < 2^{k(i,j)} \\
&\quad and\ x'(i,j) \bmod 2^{8-r} < 2^{k(i,j)} \\
&\delta'(i,j) = x''(i,j) - x(i,j) = x'(i,j) - x(i,j) = \delta(i,j) \\
&\quad \Rightarrow 2^{k(i,j)-1} < \delta'(i,j) < 2^{k(i,j)} \\
&Case\ 3: -2^{k(i,j)-1} \le \delta(i,j) \le 2^{k(i,j)-1} \\
&\delta'(i,j) = x''(i,j) - x(i,j) = x'(i,j) - x(i,j) = \delta(i,j) \\
&\quad \Rightarrow -2^{k(i,j)-1} \le \delta'(i,j) \le 2^{k(i,j)-1} \\
&Case\ 4: -2^{k(i,j)} < \delta(i,j) < -2^{k(i,j)-1} \\
&\quad and\ x'(i,j) \bmod 2^{8-r} \ge 2^{8-r} - 2^{k(i,j)} \\
&\delta'(i,j) == x''(i,j) - x(i,j) = x'(i,j) - x(i,j) = \delta(i,j) \\
&\quad \Rightarrow -2^{k(i,j)} < \delta'(i,j) < -2^{k(i,j)-1} \\
&Case\ 5: -2^{k(i,j)} < \delta(i,j) < -2^{k(i,j)-1} \\
&\quad and\ x'(i,j) \bmod 2^{8-r} < 2^{8-r} - 2^{k(i,j)} \\
&\delta'(i,j) = x''(i,j) - x(i,j) = x'(i,j) + 2^{k(i,j)} - x(i,j) \\
&\quad = \delta(i,j) + 2^{k(i,j)} \\
&\quad \Rightarrow -2^{k(i,j)} + 2^{k(i,j)} < \delta'(i,j) < -2^{k(i,j)-1} + 2^{k(i,j)} \\
&\quad \Rightarrow 0 < \delta'(i,j) < 2^{k(i,j)-1}
\end{aligned}
$$

Based on the above analysis, it can be seen that the absolute $\delta'(i,j)$ may fall into the range $2^{k(i,j)-1} \le |\delta'(i,j)| < 2^{k(i,j)}$ only when $x'(i,j) \bmod 2^{8-r} < 2^{k(i,j)}$ (Case 2) and $x'(i,j) \bmod 2^{8-r} \ge 2^{8-r} - 2^{k(i,j)}$ (Case 4); while for other possible values of $x'(i,j)$, $\delta'(i,j)$ falls into the range $0 \le |\delta'(i,j)| \le 2^{k(i,j)-1}$. Case 2 and Case 4 mean that the $8-r-k(i,j)$ bits of pixel $x(i,j)$ for OPAP (See Fig. 1) have the same value 0 and 1 respectively. If the probability of a pixel with value 0 or 1 is 0.5 in the cover-images, then the probability p of the $8-r-k(i,j)$ bits having same value 0 or 1 is $0.5^{8-r-k(i,j)}$. For instance, assume r=2, $k(i,j)$=2, then the probability $p=0.5^{8-r-k(i,j)}=0.0625$. So, the probability of $\delta'(i,j)$ falls into the range $2^{k(i,j)-1} \le |\delta'(i,j)| < 2^{k(i,j)}$ is $2p = 2*0.5^{8-r-k(i,j)} = 0.5^{7-r-k(i,j)}$, while the probability of $\delta'(i,j)$ falls into the range $0 \le |\delta'(i,j)| \le 2^{k(i,j)-1}$ is $1-2p = 1-0.5^{7-r-k(i,j)}$.

Therefore, if the secret data W obeys uniform distribution, $\delta'(i,j)$ is also uniformly distributed. Given the number of highest bits r and the embedded bit-rate $\bar{k}$, the expected mean square error (MSE) caused by the proposed method can be computed as follows

$$
\begin{aligned}
&E(MSE) = E\left(\delta'(i,j)^2\right) \\
&= 0.5^{8-r-\bar{k}} \times E\left(\delta'(i,j)^2\right)\Big|_{2^{\bar{k}-1} < \delta'(i,j) < 2^{\bar{k}}} \\
&\quad + 0.5^{8-r-\bar{k}} \times E\left(\delta'(i,j)^2\right)\Big|_{-2^{\bar{k}} < \delta'(i,j) < -2^{\bar{k}-1}} \\
&\quad + \left(1 - 2 \times 0.5^{8-r-\bar{k}}\right) \times E\left(\delta'(i,j)^2\right)\Big|_{0 \le |\delta'(i,j)| \le 2^{\bar{k}-1}} \\
&= 0.5^{8-r-\bar{k}} \times \frac{\left(2^{\bar{k}-1}-1\right)^2 - 1}{12} + 0.5^{8-r-\bar{k}} \times \frac{\left(2^{\bar{k}-1}-1\right)^2 - 1}{12} \\
&\quad + \left(1 - 0.5^{7-r-\bar{k}}\right) \times \frac{\left(2 \times 2^{\bar{k}-1}+1\right)^2 - 1}{12} \\
&= 0.5^{7-r-\bar{k}} \times \frac{\left(2^{\bar{k}-1}-1\right)^2 - 1}{12} + \left(1 - 0.5^{7-r-\bar{k}}\right) \times \frac{\left(2^{\bar{k}}+1\right)^2 - 1}{12}
\end{aligned}
\tag{16}
$$

According to (16), the expectation of PSNR obtained by the proposed scheme can be defined as:

$$PSNR_E = 10 \cdot \log_{10}\left(\frac{255^2}{MSE}\right). \tag{17}$$

Tab. 4 lists the expectation of PSNR value for r=1-6, where the embedded bit-rate $\bar{k}$ comes from the column labeled bit rate in Tab. 3. Note that the embedded bit-rate $\bar{k}$ = 1 when r=6, and that the proposed scheme is degraded into simple LSB replacement method, so the expectation of PSNR value is low for r=6. Moreover, Tab. 5 shows the comparison between the average PSNR value of the proposed approach and that of C. H. Yang's [30], in which C. H. Yang's scheme uses a 2-5 division with D_{12} =15. From Tab. 5, we can see that the proposed method achieves 4.19 dB higher PSNR values of stego-images than C. H. Yang's when secret data of the same size are embedded, on average. To a certain degree, this is because our approach can discriminate fully textured areas from edge ones, and avoid serious changes in image edge areas.

r	Embedded bit-rate $\bar{k}$ □bpp□	Expected MSE	Expected PSNR (dB)
1	5.2634	68.24300	29.79
2	4.4940	19.75500	35.17
3	3.7809	4.93890	41.20
4	2.9425	0.81001	49.05
5	1.9561	0.04756	61.36
6	1.0000	0.66667	49.89

Tab. 4. The expectation of MSE and PSNR value for r=1-6 by the proposed scheme.

Capacity (bits)	Average PSNR (dB)	
	C.H. Yang's method [30]	The proposed method
551282	36.45	40.62
500000	36.86	41.04
450000	37.22	41.50
400000	37.75	42.01
350000	38.39	42.58
300000	39.21	43.24

Tab. 5. Comparison between the average PSNR value of the proposed approach and that of C.H. Yang's [30] , where C.H. Yang's scheme uses a 2-5 division with D_{12}=15.

6. Conclusion

In this paper, we have proposed a novel steganographic method by using human visual system (HVS) and LSB substitution, which obeys the concept that the edges cannot tolerate great change. The number k of LSBs for data embedding is adaptive to image pixels by considering the HVS sensitivity to luminance, texture and edge of the host image. The value of k is calculated by the high-order bits rather than all the bits of the image pixel value, and secret data is embedded into the LSBs not the high-order bits of image pixels, which ensures that the adaptive LSBs number k remain unchanged after embedding. Extensive experimental results and the theoretical analyses demonstrate the proposed scheme can differentiate textures from edges effectively and avoid abrupt changes in image edge areas. When compared to some existing LSB methods, the proposed method achieves higher embedding capacity and imperceptibility.

In the future, we will exploit the HVS model and difference expansion to develop a lossless watermark scheme with high quality of the stego-image.

Acknowledgements

This work was supported by National Natural Science Foundation of China (60736016, 60873198), Scientific Research Fund of Hunan Provincial Education Department of China (08C018) and National Basic Research Program of China (2006CB303000, 2009CB326202).

References

[1] BENDER, W., GRUHL, D., MORIMOTO, N., AIGUO LU Techniques for data hiding. *IBM Systems Journal*, 1996, vol. 35, no. 3-4, p. 313-336.

[2] SHU-KEI YIP, OSCAR C. AU, HOI-MING WONG, CHI-WANG HO Block-based lossless data hiding in delta domain. In *Proc. ICME 2006*, Toronto, Ontario (Canada), 2006, p. 857-860.

[3] CHING-YU YANG Based upon RBTC and LSB substitution to hide data. In *Proc. First International Conference on Innovative Computing, Information and Control (ICICIC'06)*, Beijing (China), Aug. 30 - Sept. 1, 2006, vol. 1, p. 476-479.

[4] CHIN-CHEN CHANG, CHIA-CHEN LIN, CHUN-SEN TSENG, WEI-LIANG TAI Reversible hiding in DCT-based compressed images. *Information Sciences*, 2007, vol. 177, no. 13, p. 2768-2786.

[5] YANG YOU, YU PING, XU JIANGFENG An improved LSB algorithm based on multi-transformation. In *Proc. 2008 International Symposium on Information Science and Engineering (ISISE'08)*. Shanghai (China), Dec. 20-22, 2008, vol. 1, p. 487-491.

[6] THIEN, C. C., LIN, J. C. A simple and high-hiding capacity method for hiding digit-by-digit data in images based on modulus function. *Pattern Recognition*, 2003, vol. 36, p. 2875-2881.

[7] CHIN-CHEN CHANG, MIN-HUI LIN, YU-CHEN HU A fast and secure image hiding scheme based on LSB substitution. *International Journal of Pattern Recognition and Artificial Intelligence*, 2002, vol. 16, no. 4, p. 399-416.

[8] KER, A. Improved detection of LSB steganography in grayscale images. In *Proc. 6th International Workshop*. Toronto (Canada), May 23-25, 2004, Springer LNCS, vol. 3200, p. 97–115.

[9] SHARP, T. An implementation of key-based digital signal steganography. In *Proc. 4th International Information Hiding Workshop*. Pittsburgh (USA), April 25-27, 2001, Springer LNCS, vol. 2137, p. 13–26.

[10] JARNO MIELIKAINEN LSB matching revisited. *IEEE Signal Processing Letters*, 2006, vol. 13, no. 5, p. 285-287.

[11] XIAOLONG LI, BIN YANG, DAOFANG CHENG, TIEYONG ZENG A generalization of LSB matching. *IEEE Signal Processing Letters*, 2009, vol. 16, no. 2, p. 69-72.

[12] JEN-CHANG LIU, MING-HONG SHIH Generalizations of pixel-value differencing steganography for data hiding in images. *Fundamenta Informaticae*, 2008, vol. 83, no. 3, p. 319-335.

[13] RAN-ZAN WANG, CHI-FANG LIN, JA-CHEN LIN Hiding data in images by optimal moderately significant bit replacement. *IET Electronics Letters*, 2000, vol. 36, no. 25, p. 2069-2070.

[14] RAN-ZAN WANG, CHI-FANG LIN, JA-CHEN LIN Image hiding by optimal LSB substitution and genetic algorithm. *Pattern Recognition*, 2001, vol. 34, p. 671-683.

[15] CHIN-CHEN CHANG, JU-YUAN HSIAO, CHI-SHIANG CHAN Finding optimal least-significant-bit substitution in image hiding by dynamic programming strategy. *Pattern Recognition*, 2003, vol. 36, p.1538-1595.

[16] CHIN-CHEN CHANG, CHI-SHIANG CHAN, YI-HSUAN FAN Image hiding scheme with modulus function and dynamic programming strategy on partitioned pixels. *Pattern Recognition*, 2006, vol. 39, no. 6, p. 1155-1167.

[17] CHI-KWONG CHAN, L. M. CHENG. Improved hiding data in images by optimal moderately-significant-bit replacement. *IEE electronics letters*, 2001, vol. 37, no. 16, p. 1017-1018.

[18] CHI-KWONG CHAN, L. M. CHENG Hiding data in images by simple LSB substitution. *Pattern Recognition*, 2004, vol. 37, p. 469-474.

[19] WEN-NUNG LIE, LI-CHUN CHANG. Data hiding in images with adaptive numbers of least significant bits based on the human visual system. In *Proc. IEEE Int. Conf. Image Processing*. Kobe (Japan), October 24-28, 1999, p. 286-290.

[20] LEE, Y. K., CHEN, L. H. High capacity image steganographic model. *IEE Proc., Vis. Image Signal Process*, 2000, vol. 147, no. 3, p. 288-294.

[21] SHAO-HUI LIU, TIAN-HANG CHEN, HONG-XUN YAO, WEN GAO A variable depth LSB data hiding technique in images. In *Proc. 2004 International Conference on Machine Learning and Cybernetics*. Shanghai (China), Aug. 26-29, 2004, vol. 7, p. 3990-3994.

[22] KEKRE, H. B., ARCHANA ATHAWALE, PALLAVI N. HALARNKAR Increased capacity of information hiding in LSB's method for text and image. *International Journal of Electrical, Computer, and Systems Engineering*, 2008, vol. 2, no. 4, p. 246-249.

[23] WU, D.C., TSAI, W. H. A steganographic method for images by pixel-value differencing. *Pattern Recognit. Lett.*, 2003, vol. 24, no. 9-10, p. 1613–1626.

[24] CHUNG-MING WANG, NAN-I WU, CHWEI-SHYONG TSAI, MIN-SHIANG HWANG A high quality steganographic method with pixel-value differencing and modulus function. *Journal of Systems and Software*, 2008, vol. 81, no. 1, p. 150-158.

[25] CHIN-CHEN CHANG, TSENG, H.W. A steganographic method for digital images using side match. *Pattern Recognition Letters*, 2004, vol. 25, p.1431-1437.

[26] PARK, Y. R., KANG, H. H., SHIN, S. U., KWON, K. R. A steganographic scheme in digital images using information of neighboring pixels. In *Proc. International Conference on Natural Computation*. Berlin (Germany), 2005, Springer-Verlag LNCS, vol. 3612, p. 962–968.

[27] YANG, C. H., WENG, C. Y. A steganographic method for digital images by multi-pixel differencing. In *Proc. International Computer Symposium*. Taipei (Taiwan), December, 2006, p. 831 to 836.

[28] KI-HYUN JUNG, KYEOUNG-JU HA, KEE-YOUNG YOO Image data hiding method based on multi-pixel differencing and LSB substitution methods. In *Proc. 2008 International Conference on Convergence and Hybrid Information Technology (ICHIT '08)*. Daejeon (Korea), Aug. 28-30, 2008, p. 355-358.

[29] WU, H.-C., WU, N.-I., TSAI, C.-S., HWANG, M.-S. Image steganographic scheme based on pixel-value differencing and LSB replacement methods. *IEE Proceedings-Vision, Image and Signal Processing*, 2005, vol. 152, no. 5, p. 611-615.

[30] CHENG-HSING YANG, CHI-YAO WENG, SHIUH-JENG WANG, HUNG-MIN SUN Adaptive data hiding in edge areas of images with spatial LSB domain systems. *IEEE Transactions on Information Forensics and Security*, 2008, vol. 3, no. 3, p. 488-497.

[31] SHAH TRIIEHI, CHANDRAMOULI, R. Active steganalysis of sequential steganography. In *Proc. SPIE-IS&T Electronic Imaging: Security and Watermarking of Multimedia Contents V*, Santa Clara (CA), Jan. 2003, SPIE vo1.5020, p. 123-130.

[32] LAHOUARI GHOUTI, AHMED BOURIDANE, MOHAMMAD K. IBRAHIM Edge-preserving wavelet-based multisensor image fusion approach. In *Proc. EUSIPCO 2004, 12th European Signal Processing Conference*. Vienna (Austria), September 6-10, 2004, p. 61-64.

[33] SHENG-NAN YE, KAINA SU, CHUANG-BAI XIAO Video quality assessment based on edge structural similarity. In *Proc. 2008 Congress on Image and Signal Processing*. Sanya, Hainan (China), May 27-30, 2008, vol. 3, p. 445-448.

[34] LEVI, D. M., HARWERTH, R. S., PASS, A. F., et al. Edge sensitive mechanisms in humans with abnormal visual experience. *Exp. Brain Res.*, 1981, vol. 43, p. 270-280.

About Authors ...

Hengfu YANG was born in Hunan, China, 1974. He received the M.S. degree in Computer Application from Guizhou University, China, in 2003. He is currently pursuing a Ph.D. degree in Computer Application at School of Computer and Communication from Hunan University, China. His research interests include Information Hiding, Digital Watermarking, Multimedia and Image Processing.

Xingming SUN was born in Hunan, China, 1963. He received the B.S. degree in Mathematics from Hunan Normal University, China, in 1984, the M.S. degree in Computing Science from Dalian University of Science and Technology, China, in 1988, and the Ph. D. degree in Computing Science from Fudan University, China, in 2001. He is currently a Professor in School of Computer and Communication, Hunan University, China. His research interests include Network & Information Security, Digital Watermarking, Wireless Sensor Network Security, and Natural Language Processing.

Guang SUN was born in Shandong, China, 1973. He received the M.S. degree in Software Engineering from Hunan University, China, in 2005. He is currently a Ph.D. candidate in the School of Computer and Communication at Hunan University, China. His research interests include Network & Information Security, Software Watermarking, Software Birthmarking.