A Sudoku Based Wet Paper Hiding Scheme

The Duc Kieu [1], Zhi-Hui Wang [3], Chin-Chen Chang [1, 2], and Ming-Chu Li [3]

[1] *Department of Information Engineering and Computer Science,*
Feng Chia University, Taichung 401724, Taiwan, R.O.C.
ktduc0323@yahoo.com.au

[2] *Department of Computer Science and Information Engineering,*
National Chung Cheng University, Chiayi 621, Taiwan, R.O.C.
ccc@cs.ccu.edu.tw

[3] *School of Software,*
Dalian University of Technology, Dalian, Liaoning, China
E-mail: wangzhihui1017@yahoo.cn
li_mingchu@yahoo.com

Abstract

Good image quality and high hiding capacity are two basic requirements of information hiding systems. Technically, it is very challenging to achieve these two factors simultaneously. The purpose of obtaining either high hiding capacity or good image quality are various from application to application. Inspired from the wet paper codes proposed by Fridrich et al., we propose an information hiding scheme for grayscale images. The proposed scheme first uses a secret key to randomly select a subset of pixels from a cover image as dry pixels. Next, the toral automorphism is applied to the cover image to maximize the number of dry pixel pairs. Then, each secret digit in the base-9 numeral system is embedded into one dry pixel pair. The experimental results show that the proposed scheme can achieve good image quality (i.e., PSNR > 46 dB) and flexible hiding capacity. In addition, unauthorized users without knowing the secret key and the secret parameters used for the toral automorphism can not extract the embedded message.

Keywords: *Sudoki, Wet Paper Hiding, Smart Home*

1. Introduction

The advances in network technologies and digital devices facilitate digital data distributions. However, distributing digital data over public networks such as the Internet is not really safe due to copy violation, counterfeiting, forgery, and fraud. Therefore, the protection of digital data, especially for confidential data, is in high demand. Traditionally, secret data can be protected by cryptographic methods such as DES [1] or RSA [2]. The drawback of cryptography is that cryptography can protect the secret data in transit, but once they have been decrypted, the content of the secret data has no further protection [3]. Alternatively, confidential data can be protected by using information hiding techniques. An information hiding system embeds secret data into a cover object (e.g., an image, audio, video, or written text) to obtain an embedded object (also called a watermarked object in watermarking applications or a stego object in steganographic applications). For more secure, a cryptographic technique can be applied to an information hiding scheme to encrypt the secret data prior to embedding.

In general, information hiding (also called data hiding or data embedding) includes digital watermarking and steganography [4]. Watermarking is used for copyright protection, broadcast monitoring, transaction tracking, etc. A watermarking scheme imperceptibly alters a cover object to embed a message about the cover object (e.g., owner's identifier) [3]. The robustness (i.e. the ability to resist certain malicious attacks such as common signal processing operations) of digital watermarking schemes is critical. In contrast, steganography is used for secret communications. A steganographic method undetectably alters a cover object to conceal a secret message [3]. Thus, steganographic methods can hide the very presence of covert communications.

The basic requirements of a data hiding scheme are visual quality of embedded images (also called visual quality for short), hiding capacity (also called payload), and robustness. A data hiding scheme with low image distortion is more secure than that with high distortion because it does not raise any suspicions of adversaries. A data hiding system with high payload (i.e., the number of bits which can be embedded into a cover pixel) is preferred because more secret data can be transmitted. The robustness is particularly important to robust watermarking applications but it is technically challenging to achieve the robustness requirement for high payload data hiding systems. Visual quality, hiding capacity, and robustness are the conflicting factors (i.e., inversely proportional). Thus, the tradeoff between the three factors above varies from application to application, depending on users' requirements and application domains. Consequently, different techniques are utilized for different applications. Therefore, a class of data hiding schemes is needed to span the range of possible applications.

In 2006, Mielikainen [5] proposed a new LSB-based scheme with the hiding capacity of 1 bit per pixel (bpp) and good visual quality measured by peak signal-to-noise ratio (PSNR) by using a binary function F. The embedding process of Mielikainen's scheme is described as follows. The secret data in binary form $S = b_0b_1...b_{L-1}$, where L is the length of S, is partitioned into secret bit pairs (b_i, b_{i+1})'s, where $i = 0, 2, \ldots, L - 2$. A grayscale cover image X sized $H \times W$ is partitioned into cover pixel pairs (p_i, p_{i+1})'s. During the embedding process, each secret bit pair (b_i, b_{i+1}) is embedded into one cover pixel pair (p_i, p_{i+1}) at a time by adding and subtracting p_i or p_{i+1} by one, or keeping p_i or p_{i+1} unchanged. These embedding rules are determined by the secret bit pair (b_i, b_{i+1}), least significant bit of p_i (i.e. LSB(p_i)), the returned value of the binary function F (i.e. $F(p_i, p_{i+1})$ or $F(p_{i-1}, p_{i+1})$), and whether the p_{i+1}'s grayscale value is even or odd. The aforementioned binary function F is defined as $F(p_i, p_{i+1}) = \text{LSB}(\lfloor p_i / 2 \rfloor + p_{i+1})$.

To fully exploit the modification directions of Mielikainen's scheme, Zhang and Wang proposed a new exploiting modification direction (EMD) method [6]. The embedding process of the EMD scheme is summarized as follows. Firstly, the binary secret data S is first partitioned into the segments of α bits. Secondly, each α-bit segment is converted into β secret digits in the base-$(2n + 1)$ numeral system, where n is a positive integer. Next, each secret digit d is embedded into one segment of n pixels. The value of α is computed by $\alpha = \lfloor \beta \times \log_2(2n + 1) \rfloor$. For instance, if $n = 2$ and $\beta = 2$, then the number of bits of one segment is $\alpha = 4$. Thirdly, a given grayscale cover image X sized $H \times W$ is divided into groups of n pixels. One secret digit d in the base-$(2n + 1)$ numeral system (also called a secret digit for short) is embedded into one group of n cover pixels by increasing or decreasing only one cover pixel in the group by 1. Let us denote the grayscale values of pixels in an n-pixel group as an n-dimensional vector $(p_1, p_2, ..., p_n)$ and calculate the value y of the extraction function G as a weighted sum modulo $(2n + 1)$. That is, $y = G(p_1, p_2, ..., p_n) = \sum_{1 \leq i \leq n} (p_i \times i) \bmod (2n + 1)$. According to the secret digit d and the value y of the extraction function G, the embedding rules can be divided into three cases as follows. Case 1: if $d = y$, then d is embedded by no modification on the pixel group. Case 2: if $d \neq y$, calculate $s = (d - y) \bmod (2n + 1)$. Next, if $s \leq n$, then increase the value of p_s by 1. Case 3: if $d \neq y$, calculate $s = (d - y) \bmod (2n + 1)$. Then, if $s > n$, then decrease the value of p_{2n+1-s} by 1. To improve the hiding capacity of the EMD method, Chang et al. [7] proposed an information hiding scheme by using a Sudoku solution. The review of Chang et al.'s scheme is presented in Subsection 2.1.

The aforementioned schemes conceal secret data in raster scan manner (i.e., from left to right and from top to bottom). As a result, these schemes may be vulnerable to steganalytic attacks because the embedding positions are publicly known. To enhance the steganographic security of information hiding systems, Fridrich et al. proposed a novel steganographic scheme called writing on wet paper [8]. Fridrich et al.'s scheme is reviewed in Subsection 2.2.

Thus, from the aforementioned considerations, aimed at improving the steganographic security of Chang et al.'s scheme, we propose a steganographic scheme with good visual quality (i.e., PSNR > 46 dB) and high hiding capacity by using the idea from the wet paper codes. First, the proposed scheme utilizes a secret key to randomly select a subset of pixels from a cover image as dry pixels. Next, the toral automorphism is performed on the cover image so that the number of dry pixel pairs is maximized. Then, each secret digit in the base-9 numeral system (also called a secret digit for short) is hidden into one dry pixel pair at a time. The details of the proposed method are described in Section 3.

The rest of the paper is organized as follows. The reviews of Chang et al.'s scheme, wet paper codes, and the toral automorphism are presented in Subsections 2.1, 2.2, and 2.3, respectively. Section 3 details the proposed scheme. The experimental results and discussions are presented in Section 4. Finally, some conclusions are made in Section 5.

2. Related works

2.1. Chang et al.'s scheme

Inspired from Zhang and Wang's scheme, recently, Chang et al. [7] proposed an information hiding scheme by using a Sudoku solution to enhance the hiding capacity of the EMD method. Sudoku is a logic-based number placement puzzle [9]. Sudoku is a 9×9 matrix which contains nine 3×3 sub-blocks, each contains different digits from 1 to 9. In addition, each row and each column of a Sudoku grid also contain different digits from 1 to 9. An example of a Sudoku solution is shown in Figure 1.

According to Sudoku properties, Chang et al.'s scheme converts a binary secret message into secret digits in the base-9 numeral system and then modifies the values of cover pixel pairs for concealing the secret digits. Thus, every digit in the Sudoku grid is decreased by 1 so that the Sudoku grid contains digits from 0 to 8.

Next, the modified Sudoku solution is used to generate the reference matrix R, as shown in Figure 2, which is used for the embedding and extracting processes.

5	3	4	6	7	8	9	1	2
6	7	2	1	9	5	3	4	8
1	9	8	3	4	2	5	6	7
8	5	9	7	6	1	4	2	3
4	2	6	8	5	3	7	9	1
7	1	3	9	2	4	8	5	6
9	6	1	5	3	7	2	8	4
2	8	7	4	1	9	6	3	5
3	4	5	2	8	6	1	7	9

Figure 1. An example of a Sudoku solution

p_{i+1}

p_i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	...	252	253	254	255
0	4	2	3	5	6	7	8	0	1	4	2	3	5	6	7	8	0	1	...	4	2	3	5
1	5	6	1	0	8	4	2	3	7	5	6	1	0	8	4	2	3	7	...	5	6	1	0
2	0	8	7	2	3	1	4	5	6	0	8	7	2	3	1	4	5	6	...	0	8	7	2
3	7	4	8	6	5	0	3	1	2	7	4	8	6	5	0	3	1	2	...	7	4	8	6
4	3	1	5	7	4	2	6	8	0	3	1	5	7	4	2	6	8	0	...	3	1	5	7
5	6	0	2	8	1	3	7	4	5	6	0	2	8	1	3	7	4	5	...	6	0	2	8
6	8	5	0	4	2	6	1	7	3	8	5	0	4	2	6	1	7	3	...	8	5	0	4
7	1	7	6	3	0	8	5	2	4	1	7	6	3	0	8	5	2	4	...	1	7	6	3
8	2	3	4	1	7	5	0	6	8	2	3	4	1	7	5	0	6	8	...	2	3	4	1
9	4	2	3	5	6	7	8	0	1	4	2	3	5	6	7	8	0	1	...	4	2	3	5
10	5	6	1	0	8	4	2	3	7	5	6	1	0	8	4	2	3	7	...	5	6	1	0
11	0	8	7	2	3	1	4	5	6	0	8	7	2	3	1	4	5	6	...	0	8	7	2
12	7	4	8	6	5	0	3	1	2	7	4	8	6	5	0	3	1	2	...	7	4	8	6
13	3	1	5	7	4	2	6	8	0	3	1	5	7	4	2	6	8	0	...	3	1	5	7
14	6	0	2	8	1	3	7	4	5	6	0	2	8	1	3	7	4	5	...	6	0	2	8
15	8	5	0	4	2	6	1	7	3	8	5	0	4	2	6	1	7	3	...	8	5	0	4
16	1	7	6	3	0	8	5	2	4	1	7	6	3	0	8	5	2	4	...	1	7	6	3
17	2	3	4	1	7	5	0	6	8	2	3	4	1	7	5	0	6	8	...	2	3	4	1
:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:
252	4	2	3	5	6	7	8	0	1	4	2	3	5	6	7	8	0	1	...	4	2	3	5
253	5	6	1	0	8	4	2	3	7	5	6	1	0	8	4	2	3	7	...	5	6	1	0
254	0	8	7	2	3	1	4	5	6	0	8	7	2	3	1	4	5	6	...	0	8	7	2
255	7	4	8	6	5	0	3	1	2	7	4	8	6	5	0	3	1	2	...	7	4	8	6

Figure 2. An example of the reference matrix *R*

Each secret digit d is embedded into a cover pixel pair (p_i, p_{i+1}) as follows. Firstly, the cover pixel pair (p_i, p_{i+1}) is located onto the reference matrix R at the row p_i and the column p_{i+1}. Secondly, three sets of candidate elements are identified by $C_1 = \{R(p_i, p_{i+1} - 4), R(p_i, p_{i+1} - 3), R(p_i, p_{i+1} - 2), R(p_i, p_{i+1} - 1), R(p_i, p_{i+1}), R(p_i, p_{i+1} + 1), R(p_i, p_{i+1} + 2), R(p_i, p_{i+1} + 3), R(p_i,$

$p_{i+1} + 4)\}$, $C_2 = \{R(p_i - 4, p_{i+1}), R(p_i - 3, p_{i+1}), R(p_i - 2, p_{i+1}), R(p_i - 1, p_{i+1}), R(p_i, p_{i+1}), R(p_i + 1, p_{i+1}), R(p_i + 2, p_{i+1}), R(p_i + 3, p_{i+1}), R(p_i + 4, p_{i+1})\}$, and $C_3 = \{R(x_b, y_b), R(x_b, y_b + 1), R(x_b, y_b + 2), R(x_b + 1, y_b), R(x_b + 1, y_b + 1), R(x_b + 1, y_b + 2), R(x_b + 2, y_b), R(x_b + 2, y_b + 1), R(x_b + 2, y_b + 2)\}$, where $x_b = \lfloor p_i / 3 \rfloor \times 3$ and $y_b = \lfloor p_{i+1} / 3 \rfloor \times 3$. Next, search from C_1, C_2, and C_3 to find out three candidate elements $R(x_h, y_h)$, $R(x_v, y_v)$, and $R(x_w, v_w)$, respectively, such that $R(x_h, y_h) = R(x_v, y_v) = R(x_w, v_w) = d$. Then, among the found candidate elements $R(x_h, y_h)$, $R(x_v, y_v)$, and $R(x_w, v_w)$, select the candidate element $R(x_f, y_f)$ with a minimum distortion. That is, $R(x_f, y_f) = \min_{j\in\{h,\, v,\, w\}}\{|p_i - x_j| + |p_{i+1} - y_j|\}$. Finally, the stego pixel pair is obtained by $(p_i', p_{i+1}') = (x_f, y_f)$.

At the receiving end, the embedded secret digits can be exactly extracted from the received stego image V sized $H\times W$ by $d = R(p_i, p_{i+1})$. The other details of Chang et al.'s method can be found in the original article [7].

2.2. Wet paper codes

The schemes of Mielikainen, Zhang and Wang, and Chang et al. embed secret data in raster scan order (i.e., from left to right and from top to bottom). Consequently, these schemes may be vulnerable to steganalytic attacks because the embedding positions are publicly known. To improve the steganographic security of information hiding systems, Fridrich et al. proposed a novel steganographic scheme called writing on wet paper [8]. In the wet paper codes (WPC), an arbitrary subset C of the cover image X sized $H\times W$ is chosen by the sender using a pseudo-random number generator (PRNG). Then, a secret message is embedded into the subset C to obtain the stego image V. At the receiving side, expected recipients still can extract the embedded secret message without knowing the subset C. The pixels in the subset C are called dry pixels and the other pixels are called wet pixels. The dry pixels may be modified to embed the secret data and the wet pixels are kept unchanged during the embedding phase. The other details of the WPC scheme can be found in the original article [8].

2.3. Toral automorphism

The 2-dimensional toral automorphism [10] can be seen as a tool to relocate the locations of pixels of an image. The toral automorphism was used by some researchers for information hiding systems [11, 12]. Given a square image X sized N, the toral automorphism changing the pixel located at the position (i, j) to the new position (i', j') can be represented by

$$\begin{bmatrix} i' \\ j' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ k & k+1 \end{bmatrix} \times \begin{bmatrix} i \\ j \end{bmatrix} \bmod N,$$

where $0 \le i, j, i', j' \le N - 1$.

It is clear that the new position (i', j') is specified if the parameter k is known. Thus, the parameter k can be considered as a secret key. After some iterations of the transformation, the image X becomes a random-like image X'. However, after further iterations of the transformation, the image X' returns to the original image X. If the original image X is reconstructed after t iterations, then t is called the recurrence time [10]. In this paper, we use the toral automorphism to maximize the number of dry pixel pairs.

3. The proposed method

Inspired from the idea of the WPC scheme, we propose a steganographic scheme with good image quality (i.e., PSNR > 46 dB), flexible hiding capacity, and improved steganographic security. The details of the proposed scheme are described below.

3.1. The embedding phase

Let us assume that we have an original cover image X sized $H \times W$, a secret message in the base-9 notational system is S. The diagram of the proposed embedding process is shown in Figure 3.

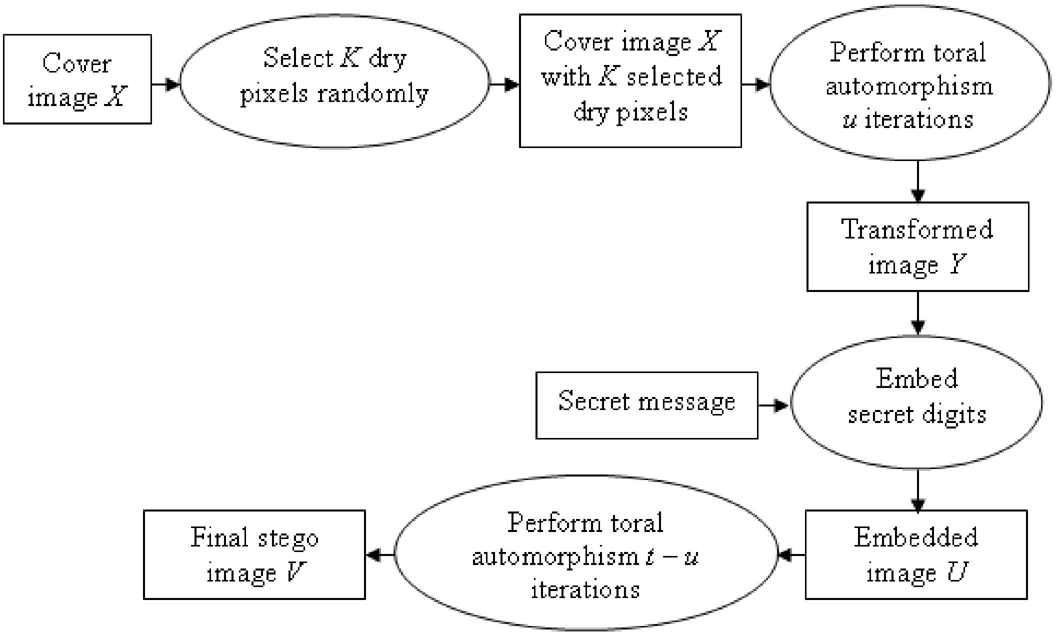

Cover image X
Select K dry pixels randomly
Cover image X with K selected dry pixels
Perform toral automorphism u iterations
Transformed image Y
Secret message
Embed secret digits
Embedded image U
Perform toral automorphism $t - u$ iterations
Final stego image V

Figure 3. The diagram of the proposed embedding process

The proposed method works as follows. Based on the concept of the wet paper codes (WPC) proposed by Fridrich et al. [8], firstly, we randomly select K dry pixels (i.e., changeable pixels) of the cover image X using a pseudo-random number generator (PRNG) with a secret seed s, where $0 \leq K \leq H \times W$. The $H \times W - K$ remaining pixels are regarded as wet pixels (i.e., unchangeable pixels). The secret seed s and K are considered as secret keys and pre-shared with expected receivers. A temporary matrix T sized $H \times W$ is used to record the dry pixels in the cover image X. Actually, T is a bit map in which $T[i][j] = 1$ if $X[i][j]$ is a dry pixel; otherwise, $T[i][j] = 0$, where $0 \leq i \leq H - 1$ and $0 \leq j \leq W - 1$. Secondly, pixels in the cover image X are paired using some paring rule (e.g., in raster scan order). A pixel pair (p_i, p_{i+1}) is defined as a restricted pair if p_i and p_{i+1} are wet pixels. Otherwise, the pixel pair (p_i, p_{i+1}) is defined as a non-restricted pair. The proposed method embeds secret digits into non-restricted pairs only. That is, the restricted pairs are left unchanged during the embedding process. Thirdly, the toral automorphism [10] is used to relocate pixels in the cover image X such that the number of non-restricted pixel pairs in the cover image X is maximized. That is, the number of restricted pixel pairs in X is minimized. Let the number of iterations that the number of non-restricted pixel pairs in the cover image X is maximized and the recurrence time be *u* and *t*, respectively. The resulting image is denoted as *Y*. It is noted that when we apply the toral automorphism *u* iterations to the cover image *X*, we also apply the toral automorphism *u* iterations to the temporary matrix *T* to maintain the information of the restricted and non-restricted pixel pairs. Fourthly, analogous to Chang et al.'s scheme, the binary secret message *S* is converted into secret digits in the base-9 numeral system (also called secret digits for short). These secret digits are then embedded into the image *Y* by adopting Chang et al.'s method [7] to obtain the embedded image *U*. That is, Chang et al.'s method is adopted to embed the secret digits into the non-restricted pixel pairs only. Finally, the toral automorphism is applied $t - u$ times to the embedded image *U* to get the final stego image *V*. When the embedding process has been done, the sender sends the stego image *V* and secret parameters *K*, *s*, and *k* to expected recipients, where *k* is the parameter of the toral automorphism.

3.2. The extracting phase

At the receiving side, an authorized recipient can extract the embedded secret digits from the received stego image *V* using the pre-shared secret parameters *K*, *s*, and *k*. The diagram of the proposed extracting process is displayed in Figure 4.

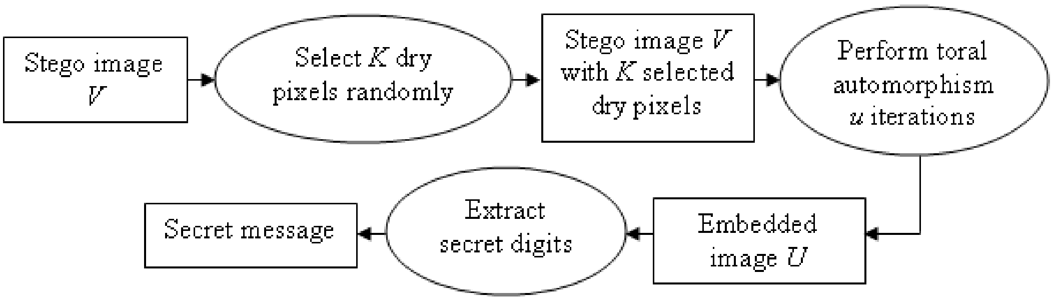
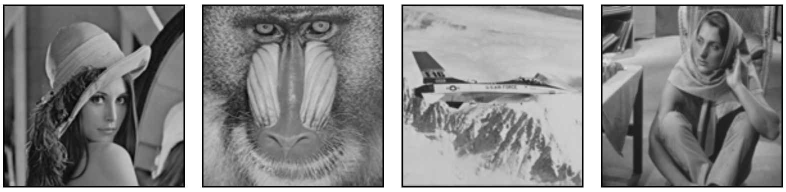

Stego image V
Select K dry pixels randomly
Stego image V with K selected dry pixels
Perform toral automorphism u iterations
Embedded image U
Extract secret digits
Secret message

Figure 4. The diagram of the proposed extracting process

The proposed extracting process works as follows. First, the recipient uses the same PRNG with seed *s* to randomly choose *K* dry pixels in the received stego image *V*. Second, the toral automorphism is executed *u* iterations to the stego image *V* and the temporary matrix *T* to get the embedded image *U*. Then, based on the temporary matrix *T*, the extracting process of Chang et al.'s scheme is adopted to extract the embedded secret digits from the non-restricted pixel pairs of the embedded image *U*. Finally, the extracted secret digits are concatenated and converted back to the binary form to obtain the original secret message.

4. Experimental results and discussions

To evaluate the performance of the proposed method, we implemented Zhang and Wang's scheme, Chang et al.'s scheme, and the proposed scheme by using Borland C++ Builder 6.0 software running on the Pentium IV, 3.6GHz CPU, and 1.49GB RAM hardware platform. The secret message *S* was randomly generated by using the library function `random()`. Four commonly used grayscale images sized 512×512, as shown in Figure 5, were used as the cover images in our simulations to test the performance of the proposed method in terms of hiding capacity and visual quality of stego images. In our experiments, the secret parameter of the used toral automorphism and the secret seed of the used PRNG were set to be $k = 2$ and $s = 15$, respectively.



(a) Lena (b) Baboon (c) F16 (d) Barbara

Figure 5. Four test images sized 512×512

The visual quality of stego images (called visual quality for short) was evaluated by using peak signal-to-noise ratio (PSNR) which is defined as PSNR = $10\times\log_{10}(255^2 / MSE)$ (dB), where MSE is the mean square error representing the distortion between the original cover image X sized $H\times W$ and the stego image V sized $H\times W$. Hiding capacity C (also called capacity for short) was measured by bits per pixel (bpp). That is, it was computed by the ratio of the total number of embedded secret bits and the total number of pixels in the cover image X. The hiding capacities and the PSNR values of the proposed method with various values of K for test images are shown in Table 1. K = 10% means that the number of selected dry pixels is 10 percent of the total number of pixels in the cover image X.

Table 1. Hiding capacities and PSNR values of the proposed method for test images with various values of K

Images	Lena		Baboon		F16		Barbara	
K	PSNR	C	PSNR	C	PSNR	C	PSNR	C
10%	53.83	0.29	53.84	0.29	53.89	0.29	53.89	0.29
20%	51.05	0.54	51.10	0.54	51.06	0.54	51.08	0.54
30%	49.57	0.77	49.56	0.77	49.55	0.77	49.58	0.77
40%	48.57	0.96	48.58	0.96	48.61	0.96	48.58	0.96
50%	47.89	1.13	47.91	1.13	47.91	1.13	47.90	1.13
60%	47.45	1.26	47.42	1.26	47.42	1.26	47.41	1.26
70%	47.09	1.37	47.08	1.37	47.08	1.37	47.05	1.37
80%	46.82	1.44	46.83	1.44	46.84	1.44	46.83	1.44
90%	46.70	1.49	46.68	1.49	46.71	1.49	46.70	1.49
100%	46.65	1.50	46.67	1.50	46.61	1.50	46.65	1.50

To compare the performance of two related works and the proposed method, the performance results of Zhang and Wang's and Chang et al.'s methods in terms of visual quality and hiding capacity are shown in Table 2.

Tables 1 and 2 show that the proposed method becomes Chang et al.'s method when K = 100%. In other words, Chang et al.'s scheme is a special case of the proposed scheme.

In addition, the hiding capacity of the proposed method is less than that of Zhang and Wang's method when $K \leq 40\%$. However, the hiding capacity of the proposed method is greater than that of Zhang and Wang's method when $50\% \leq K \leq 100\%$. It is very natural that the PSNR value of the EMD method is higher than that of the proposed method. This is because Zhang and Wang's method embeds one secret digit in the base-5 numeral system into one cover pixel pair whereas the proposed method conceals one secret digit in the base-9 numeral system into one cover pixel pair.

Table 2. The performance results of Zhang and Wang's and Chang et al.'s methods

Methods / Images	Zhang and Wang		Chang et al.	
	PSNR	*C*	PSNR	*C*
Lena	52.09	1	46.65	1.5
Baboon	52.10	1	46.67	1.5
F16	52.12	1	46.61	1.5
Barbara	52.12	1	46.65	1.5

The purpose of using the toral automorphism in our proposed scheme is to maximize the number of non-restricted pixel pairs in the cover image *X*. The gains in terms of dry pixel pairs thanks to the use of the toral automorphism for test images with various values of *K* are shown in Table 3. It is clear that the gain in secret bits, which can be embedded more in the cover image *X*, via the use of the toral automorphism is treble the number of gained dry pixel pairs.

Table 3. The gained dry pixel pairs using toral automorphism for test images with various values of *K*

Factors / *K*	Initial dry pixel pairs	Maximized dry pixels pairs	Gained dry pixel pairs	Gained secret bits
10%	24907	24996	89	267
20%	47203	47432	229	687
30%	66847	67038	191	573
40%	83934	84117	183	549
50%	98304	98559	255	765
60%	110068	110379	311	933
70%	119207	119475	268	804
80%	125751	125978	227	681
90%	129729	129880	151	453

With the uses of the random selection of dry pixels from the cover image *X* and the toral automorphism, the proposed method can improve the steganographic security of Zhang and Wang's and Chang et al.'s methods. That is, the unintended recipients can not extract the embedded secret message unless they know the secret keys *K*, *s*, and *k* which are used for selecting dry pixel pairs, PRNG, and the toral automorphism.

5. Conclusions

In this paper, we propose a steganographic scheme for grayscale images in spatial domain. The proposed scheme uses the idea from the wet paper codes to randomly select a subset of pixels from a cover image as dry pixels for the embedding process. In addition, the toral automorphism is applied to the cover image to maximize the number of dry pixel pairs. The proposed scheme can achieve good image quality and high hiding capacity. That is, the PSNR value is greater than 46 dB for all test images and the hiding capacity can be achieved up to 1.5 bpp. Furthermore, the embedded message can not be extracted if the secret parameters *K*, *s*, and *k* are unknown.

References

[1] R. M. Davis, “The Data Encryption Standard in Perspective,” IEEE Communications Magazine, Vol. 16, No. 6, 1978, pp. 5-9.

[2] R. Rivest, A. Shamir, and L. Adleman, “A Method for Obtaining Digital Signatures and Public-key Cryptosystems,” Communications of the ACM, Vol. 21, No. 2, 1978, pp. 120-126.

[3] I. J. Cox, M. L. Miller, J. A. Bloom, J. Fridrich, and T. Kalker, “Digital Watermarking and Steganography,” Morgan Kauffman, 2007, ISBN: 978-0-12-372585-1.

[4] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, “Information Hiding-A Survey,” Proceedings of the IEEE, Vol. 87, No. 7, 1999, pp. 1062-1078.

[5] J. Mielikainen, “LSB Matching Revisited,” IEEE Signal Processing Letters, Vol. 13, No. 5, May 2006, pp. 285-287.

[6] X. Zhang and S. Wang, “Efficient Steganographic Embedding by Exploiting Modification Direction,” IEEE Communications Letters, Vo. 10, No. 11, Nov. 2006, pp. 1-3.

[7] C. C. Chang, Y. C. Chou, and T. D. Kieu, “An Information Hiding Scheme Using Sudoku,” Proceedings of The Third International Conference on Innovative Computing, Information and Control (ICICIC2008), Dalian, China, Jun. 2008. pp. 17-21.

[8] J. Fridrich, M. Goljan, P. Lisonek, and D. Soukal, “Writing on Wet Paper,” IEEE Transactions on Signal Processing, Vol. 53, No. 10, Oct. 2005, pp. 3923-3935.

[9] E. Russell and F. Jarvis, “Mathematics of Sudoku ii,” Mathematical Spectrum, Vol. 39, No. 2, Jan. 2007, pp. 54-58.

[10] G. Voyatzis and I. Pitas, “Applications of Toral Automorphisms in Image Watermarking,” Proceedings of the IEEE International Conference on Image Processing, Lausanne, Switzerland, Vol. 2, Sep. 1996, pp. 237-240.

[11] X. Wu and Z. H. Guan, “A Novel Digital Watermark Algorithm Based on Chaotic Maps,” Physics Letters A, Vol. 365, No. 5-6, Jun. 2007, pp. 403-406.

[12] Y. T. Wu, Y. S. Frank, “Digital Watermarking Based on Chaotic Map and Reference Register,” Pattern Recognition, Vol. 40, No. 12, Dec. 2007, pp. 3753-3763.

Authors

The Duc Kieu received the B.S. degree in mathematics from the University of Pedagogy, Vietnam, in 1995, the B.S. degree in information technology from the University of Natural Sciences, Vietnam, in 1999, and the M.S. degree in computer science from Latrobe University, Australia, in 2005. Currently, he is a Ph.D. candidate under Professor Chen-Chen Chang’s supervision at Feng Chia University, Taiwan. His current research interests include information hiding, image processing, and data compression.

Zhi-Hui Wang received the B.S. degree in software engineering in 2004 from the North Eastern University, Shenyang, China, and the M.S. degree in software engineering in 2007 from Dalian University of Technology, Dalian, China. She is currently pursuing her Ph.D. degree in computer software and theory from Dalian University of Technology, Dalian, China. Her research interests include data hiding and image processing.

Chin-Chen Chang (F'99) received the B.S. degree in applied mathematics and the M.S. degree in computer and decision sciences from the National Tsing Hua University, Hsinchu, Taiwan, R.O.C., in 1977 and in 1979, respectively, and the Ph.D. degree in computer engineering from the National Chiao Tung University, Hsinchu, in 1982.

During the academic years of 1980–1983, he was on the faculty of the Department of Computer Engineering at the National Chiao Tung University. From 1983 to 1989, he was on the faculty of the Institute of Applied Mathematics, National Chung Hsing University, Taichung. From 1989 to 1992, he was the Head and Professor at the Institute of Computer Science and Information Engineering, National Chung Cheng University, Chiayi, where he was he Dean of the College of Engineering from 1992 to 1995. From 1995 to 1997, he was the Provost at National Chung Cheng University, where he was the Acting President from 1996 to 1997. From 1998 to 2000, he was the Director of Advisory Office of the Ministry of Education of the R.O.C. From 2002 to 2005, he was a Chair Professor of National Chung Cheng University. Since 2005, he has been a Chair Professor of Feng Chia University, Taichung. In addition, he has been a Consultant to several research institutes and government departments. His research interests include database design, computer cryptography, image compression, and data structures.

Ming-Chu Li received a Ph.D. degree from the University of Toronto, Toronto, Canada, in 1998. During 1997-2002, he worked as a system software Engineer in North America, where he helped in the design and implementation of algorithms and the structures of projects. In 2002, he was a Full Professor of Computer Science at Tianjin University, Tianjin, China. In 1993, he was an Associate Professor at Beijing University of Science and Technology, Beijing, China. Prof. Li is currently a Full Professor of Computer Science at DaLian University of Technology (DLUT), Dalian, China, where he has been since September 2004. He is also the Vice Dean of School of Software of DLUT. His research interests include Hamiltonian Graph Theory, NP-Theory and Algorithms, Network and Information Security, Reputation Systems, and Grid computing and its applications. Prof. Li received several projects by National Nature Science Foundation of China, High-technology 863 plan of China and 973 plan of China since 2002, and has published more than 80 papers in journals and international academic conferences. He is the chair of 2007 International workshop on Graph Theory, Algorithm and its Applications, and 2008 workshop among Asia Information security labs.