International Journal of Security and Its Applications
Vol.8, No.1 (2014), pp.389-400
http://dx.doi.org/10.14257/ijsia.2014.8.1.36

Lossless Data Hiding Technique using Reversible Function

Sang-Ho Shin[1], Ho Hwang[2] and Jun-Cheol Jeon[2]

[1]School of Computer Science and Engineering, Kyungpook National University
80 Daehakro, Bukgu, Daegu, 702-701, Korea
[2]Dept. of Computer Engineering, Kumoh National Institute of Technology
61 Daehakro, Gumi, Gyeongbuk, 730-701, Korea
shshin80@infosec.knu.ac.kr, kcats9731@gmail.com, jcjeon@kumoh.ac.kr

Abstract

The most of the previous lossless data hiding techniques are that secret data are embedded into cover image. So, the relationship between the embedding capacity and PSNR of these techniques is always an inverse proportion. In contrast, the embedded position information of secret data are embedded into a location map in the proposed technique in order to achieve thedirectly proportional relationship. The proposed technique is based on a property of self-inverse in reversible function, it is the composite operation between reversible functions. In the embedding procedure, a stego image without distortion is generated using this property.In order to evaluate the efficiency and security of the proposed technique, the embedding capacity and PSNR are used in the experiments. In the experimental results, the embedding capacity and PSNR of the proposed technique are greater than it of the previous techniques.

Keywords: *Lossless data hiding technique;reversible function;embedding capacity; PSNR*

1. Introduction

With the growth of the Internet and computing technologies, data hiding, is the technique that secret data is hided in the meaningful host data in order to distract the attention of the observers [1-3], is attracting a lot of public attention. Besides, variety data in digital media such as text, image, audio and video files are being transmitted over the Internet. Many data hiding techniques were proposed [4-12].

Lossless data hiding is the technique that invisible data (which is called a secret) are embedded into a digital image (which is called a cover image).In this technique, a distortion on the image (which is called a stego image) after data embedding should be low. An advantage characteristic of lossless data hiding is reversibility, that is, the embedded data can remove from stego image in order to restore the original image. It can provide an authentication and integrity of a cover image. Secret data are embedded into a cover image in such away that an authorized party could extract the secret data, and also recover the original cover image [13-15].

The previous lossless data hiding techniques can be classified into two major categories: difference expansion (DE) and histogram shifting. Tian proposed a DE-based lossless data hiding technique for the first time [14, 15]. A DE means that 1-bit secret data is embedded into an expanded difference within two consecutive pixel values in an image, and the difference is expanded by its binary representation and the addition of 1-bit secret data. An embedding capacity of his technique is close to 0.5 bit-per-pixel (bpp); but, there exists the significant distortion of stego image quality because bit-replacements of cover image pixels. Besides, this

ISSN: 1738-9976 IJSIA

technique does not suitable for multiple embedding, which accumulates dramatic image

Table 1. The Truth Table of $Toffoli$ Reversible Function

Input			Output		
A	B	C	A'	B'	C'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	**1**
1	1	1	1	1	**0**

distortion within consecutive pixel values [16-20].

In the meantime, Ni et al. proposed a data hiding technique based histogram shifting [21]. Typical histogram is a graphical representation of the distribution of data. In this technique, it is acts as a graphical representation of the tonal distribution in a cover image. The histogram shifting is that secret data are embedded into the original peak pixel areas after the original peak pixel values is shifted by the direction of zero point. Ni *et al.'s*, scheme offers invisible image distortions with little auxiliary information; but, the embedding capacity is limited by the number of frequency of the peak pixels [22-26].

In this paper, we propose a new lossless data hiding technique without distortion of stego image. The proposed technique is based on a property of self-inverse in reversible function, it is the composite operation between reversible functions. In order to embed and extract a secret data, we constructed a pattern table using the property of self-inverse, and this table generated a stego image. Although a location map in embedding procedure is generated, distortion of stego image does not exist because the embedded position of secret data is embedded into location map. In the experimental results, the embedding capacity and $PSNR$ of the proposed technique are greater than it of the previous techniques [15, 27].

This paper is organized as follows. Section 2 introduces reversible function concept. The proposed technique is discussed in Section 3. Section 4 analyzes the efficiency and security between the proposed and previous techniques. Finally, Section 5 gives the conclusions.

2. Reversible Function

An arbitrary function f with domain X and codomain Y is commonly denoted by $f: X \rightarrow Y$. It is represented by $f: \mathbb{B}^n \rightarrow \mathbb{B}$ on Boolean algebra, where $\mathbb{B}$ is a set which consists of 1-bit as 0 or 1 ($\mathbb{B} = \{0, 1\}$), and a set $\mathbb{B}^n$ consists of a n-bit ($\mathbb{B}^n = \{00 \dots 0, 00 \dots 1, \dots, 11 \dots 1\}$). On the other hand, a reversible function f^r on Boolean algebra is denoted by $f^r: \mathbb{B}^n \rightarrow \mathbb{B}^n$. It is defined by Eq. (1).

$$f^r(b_1, b_2, \ldots, b_n) = c_1, c_2, \ldots, c_n, \quad (1)$$

where $b_1, b_2, \ldots, b_n$ and $c_1, c_2, \ldots, c_n$ are binary values and c_i is represented by Eq. (2).

$$c_i = f_i(b_1, \ldots, b_{i-1}, b_{i+1}, \ldots, b_n) \odot b_i, \quad (2)$$

where $f_i: \mathbb{B}^n \rightarrow \mathbb{B}$ is an arbitrary Boolean function and '$\odot$' indicates Boolean algebra operator such as AND, OR, XOR or NOT. For example, $Toffoli$ reversible function $f^r_{(Toffoli)}: \mathbb{B}^3 \rightarrow \mathbb{B}^3$ can be represented by Eq. (3).

$$f^r_{(Toffoli)}(b_1, b_2, b_3) = c_1, c_2, c_3, \quad (3)$$

where c_1, c_2 and c_3 are b_1, b_2 and $f_{(AND)}(b_1, b_2) \oplus b_3$ (where $f_{(AND)}(b_1, b_2) = b_1 \wedge b_2$, '$\wedge$' and '$\oplus$' indicate an AND and XOR), respectively. The truth table of this function is shown in Table 1. Typical function f takes n inputs and generates a single output; the reversible function f^r takes n inputs and produces n outputs.

It has some properties as follows. For any general function $f: X \rightarrow Y$, an inverse function f^{-1} should be required in order to perform an arithmetic operation $Y \rightarrow X$. Also, f should be an one-to-one mapping between domain and codomain elements so that there exists an inverse function f^{-1}. But, a reversible function f^r can operate $f^r: X \rightarrow Y$ and $f^r: Y \rightarrow X$. This is because it perform a self-inverse and this fact can be represented by Eq. (4).

$$f \circ f^{-1} = f^r \circ (f^r)^{-1} = f^r \circ (f^r \circ \cdots \circ f^r) = I, \quad (4)$$

where '$\circ$' and I indicate a composite arithmetic operation between reversible functions and an identity function, respectively. That is, $f^r \circ \cdots \circ f^r$ can act as an inverse function f^{-1}. All reversible functions can be represented as a matrix form because the number of inputs and outputs is the same. For example, $Toffoli$ reversible function [28] is represented as a matrix form by Eq. (5). And it can perform a self-inverse as shown in Eq. (6). In this paper, we propose a lossless data hiding technique based on properties of reversible function.

$$f^r_{(Toffoli)} = \begin{bmatrix} 1&0&0&0&0&0&0&0 \\ 0&1&0&0&0&0&0&0 \\ 0&0&1&0&0&0&0&0 \\ 0&0&0&1&0&0&0&0 \\ 0&0&0&0&1&0&0&0 \\ 0&0&0&0&0&1&0&0 \\ 0&0&0&0&0&0&0&1 \\ 0&0&0&0&0&0&1&0 \end{bmatrix} \quad (5)$$

$$f^r_{(Toffoli)} \circ f^r_{(Toffoli)} = \begin{bmatrix} 1&0&0&0&0&0&0&0 \\ 0&1&0&0&0&0&0&0 \\ 0&0&1&0&0&0&0&0 \\ 0&0&0&1&0&0&0&0 \\ 0&0&0&0&1&0&0&0 \\ 0&0&0&0&0&1&0&0 \\ 0&0&0&0&0&0&0&1 \\ 0&0&0&0&0&0&1&0 \end{bmatrix} \begin{bmatrix} 1&0&0&0&0&0&0&0 \\ 0&1&0&0&0&0&0&0 \\ 0&0&1&0&0&0&0&0 \\ 0&0&0&1&0&0&0&0 \\ 0&0&0&0&1&0&0&0 \\ 0&0&0&0&0&1&0&0 \\ 0&0&0&0&0&0&0&1 \\ 0&0&0&0&0&0&1&0 \end{bmatrix} = I \quad (6)$$

3. The Proposed Technique

In this section, we discuss the main concept, the embedding and extraction algorithms of the proposed technique.

Table 2. The Example of a Pattern Table for $f^r_{(NOT)} \circ f^r_{(NOT)}$

Case (mod 4)	A pixel in cover image	A pixel in stego image
	LSB_2	LSB_2
$1(=01_{(2)})$	00	00
$2(=10_{(2)})$	01	01
$0(=00_{(2)})$	10	10
$3(=11_{(2)})$	11	11

3.1. The Main Concept

Unlike previous lossless data hiding techniques is that secret data are directly embedded into cover image, the embedded positions of secret data are embedded into a location map in the proposed technique. A location map means a set of information for position of embedded secret data, and it is the same size of cover image. Also, a pattern table is constructed using a property of self-inverse in reversible function and, an advantage of this table is that distorionless stgeo image is generated. This is because a pattern table is based on an identity function which consists composite operation between reversible functions as shown in Eq. (4).

Given that reversible function $f^r: \mathbb{B}^2 \rightarrow \mathbb{B}^2$, for example, a $f^r_{(NOT)}$is represented by Eq. (7).

$$f^r_{(NOT)}(b_1, b_2) = c_1, c_2, \tag{7}$$

wherec_1 and c_2 are b_2 and b_1, respectively. And it can be expressed as a matrix form by Eq. (8).

$$f^r_{(NOT)} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \tag{8}$$

$f^r_{(NOT)}$is satisfied by Eq. (9).

$$f^r_{(NOT)} \circ f^r_{(NOT)} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = I \tag{9}$$

So, we can construct a pattern table as shown in Table 2. In Table 2,LSB_2 indicates least significant bit(LSB) two bits of a pixel value in an image. And the meaning of "case (mod 4)" is that an i-th pixel value (S_i) in a secret image (SI) is applied by modulo arithmetic operation.For $f^r_{(NOT)} \circ f^r_{(NOT)}$, the number of cases of secret is four such as $0(=00_{(2)})$, $1(=01_{(2)})$, $2(=10_{(2)})$ and $3(=11_{(2)})$, and the order of these is "$\cdots \longrightarrow 1 \longrightarrow 2 \longrightarrow 0 \longrightarrow 3 \longrightarrow 1 \longrightarrow \cdots$".The number of orders is $4!\,(=24)$.

The example of the embedding procedure is as follows. Given that an i-th pixel value $C_i$of cover image (CI), a location map which is the same size of CI, a j-th secret s_j and a pattern table for $f^r_{(NOT)} \circ f^r_{(NOT)}$ as shown in Table 2, if LSB_2 of $C_i(=124)$ is $00$and $s_j = 1$, it corresponds first case. So, i-th pixel value ST_i of stego image (STI) which is the same value as a C_i is generated. And then, i-thindex in a location map is written by 1. The meaning of '1' in location map is that secret s_j is embedded into CI. On the other hand, if a pair of LSB_2 of $C_i$and s_j do not correspond in the pattern table, this case does not perform the embedding. Also, corresponding index in a location map is written by 0. Other pixels in cover image are repeated at the same method. Lastly, a pattern table and location map through secure channel are transmitted.

3.2. The Embedding Algorithm

Input: a CI with size of $M \times M$ and a SI with size of $N \times N$

Output: STI with size of $M \times M$, a pattern table and a location map

Step 1: Choose a positive integer n in order to determine the number of inputs and outputs of reversible function $f^r: \mathbb{B}^n \rightarrow \mathbb{B}^n$ and calculate$m = 2^n$, where m indicates the number of cases of secret image, and the other meaning is the number of reversible functions as$m = |f^r|$.

Step2: Choose a reversible function $f^r: \mathbb{B}^n \rightarrow \mathbb{B}^n$ of m cases. And then, construct apattern table of $f^r_{(chosen)}: \mathbb{B}^n \rightarrow \mathbb{B}^n$ as follows.

> **Step 2.1**: Choose the number of LSBs ($|LSB|$) for each pixel within divisors of n. According to the number of LSBs, the number of required pixels in CI is determined as $m/|LSB|$ (where $|LSB|$ is always even).
>
> **Step 2.2**: Choose the number of cases of secret within divisors of m (where the number of cases is more than 1).

Step 3: Convert an$i$-th pixel value (S_i) in SI into m-ary's expression as Eq. (10).

$$S_i \Longrightarrow \left\{s_i\lceil\log_m 255\rceil, \ldots, s_{(i+1)}\lceil\log_m 255\rceil - 1\right\}, \tag{10}$$

where$1 \leq i \leq N^2 - 1$. Let a set $\mathbb{S}$ consists of $(N^2)\lceil\log_m 255\rceil$ elements that compose of m-ary's values, and it is expressed by Eq. (11).

$$\mathbb{S} = \left\{s_0, \ldots, s_{(N^2)\lceil\log_m 255\rceil - 1}\right\} \tag{11}$$

Step 4: Embed a j-th $(0 \leq j \leq (N^2)\lceil\log_m 255\rceil - 1)$ secret into a i-th pixel value in a cover image with the pattern table, if j-th secret and LSB_2 of i-th pixel value are corresponded. Otherwise, the embedding does not perform. If a secret bit is embedded into cover image, 1 is represented at corresponding pixel index in location map. Otherwise, 0 is represented. If the embedding procedure is completed, a stego image is generated, and then apattern table of reversible function and location map through secure channel are transmitted.

3.3. The Extraction Algorithm

Input: STI with size of $M \times M$, a pattern table and a location map

Output: a recoveredCI (RCI) with size of $M \times M$ and a recovered SI (RSI)with size of $N \times N$

Step 1: Extract a j-th $(0 \leq j \leq (N^2)\lceil\log_m 255\rceil - 1)$ secret from i-th $(0 \leq i \leq M^2 - 1)$ pixel value in a stego image.Given that a location map and the pattern table, if i-th value of a location map is 1, corresponding secret $s_j$and cover image pixel value $C_i$are extracted from ST_i by the pattern table. Otherwise, a cover image pixel value $C_i$are extracted from ST_i by the pattern table.

Step 2: Convert the calculated $\mathrm{s}_0, \ldots, \mathrm{s}_{(\mathrm{N}^2)\lceil\log_\mathrm{m} 255\rceil - 1}$into pixel values by m. And then, they are reconstructed by a form of $RSI$and RCI.

Table 3. The Example of a Pattern Table for $f^r: \mathbb{B}^1 \rightarrow \mathbb{B}^1$

Case 1 (mod 2)	A pixel in cover image	A pixel in stego image
	LSB_1	LSB_1
$1(=1_{(2)})$	0	0
$0(=0_{(2)})$	1	1

4. The Experimental Results

In this section, the embedding capacity and PSNR of the proposed scheme are analyzed.

4.1. The Measurement Tools

In order to evaluate the efficiency and security of data hiding technique, there exist two typical measurement tools: the embedding capacity and PSNR. The embedding capacity meansthe amount of embedded secret data in a cover image, and it can evaluate the efficiency of data hiding technique. That is, if the embedding capacity of an arbitrary technique is more increased, we can say that this technique has a good efficiency. It is generally measured in *bit-per-pixel* (*bpp*) or bit.

$PSNR$is the abbreviation for "peak signal-to-noise ratio" and it is the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. Nowadays, $PSNR$ is the most popular distortion measurement tool in the field of image and video coding and compression. It is usually measured in *decibels* (dB), and well known that these difference distortion metrics are not very well correlated with the human visible system (HVS). This might be a problem for their application in secret image since sophisticated data hiding techniques exploit in one way or the other effects of these schemes [1][2]. The detailed $PSNR$ is represented by Eq.(12).

$$PSNR = 10\log(MAX^2/MSE), \tag{12}$$

whereMAX is the maximum value that a pixel can be represented. It is 255 because grey-scale test images were used in this paper. $MSE$is the abbreviation for "mean squared error" and it is represented by Eq.(13).

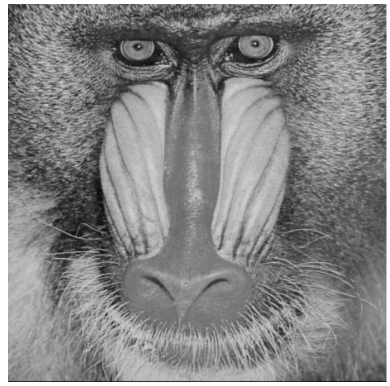
$$MSE = \frac{1}{M^2}\sum_{i=0}^{M^2-1}(C_i - ST_i)^2, \tag{13}$$

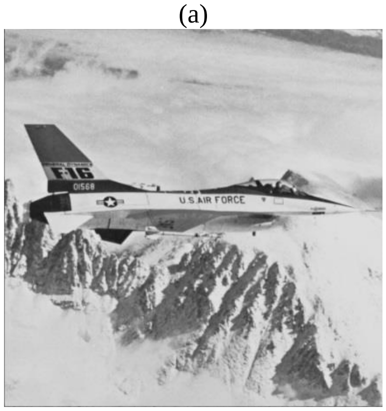
where$M$ indicates the size of CI and STI. C_i andST_i are i-th pixel values in CI and STI, respectively. Given that two grey-scale images, if $PSNR$ value is close to infinity ($=\infty$), the distortion between two images is zero, that is, two images are the same.On the other hand, if $PSNR$ value is close to zero, the distortion is higher, that is, two images are different. Generally, $PSNR$ value is more that 35 dB, the difference between two images cannot distinguish in HVS.If the distortion for an arbitrary technique is close to zero, we can say that the security of this technique is a good [1].

4.2. Analysis of Efficiency and Security

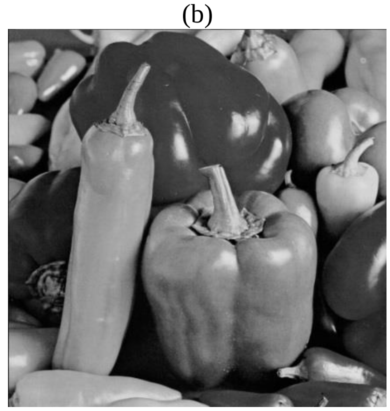
In the experiments, we used eight grey-scale test images as shown in Figure 2. The sizes of CI and $STI$are 512×512. The secret data was generated by Rand function in C++ Library. And then, generated secret bitstream was composed by each eight-bit. In order to implement the proposed scheme, the OpenCV Library and C++ programming language were used. Also, we

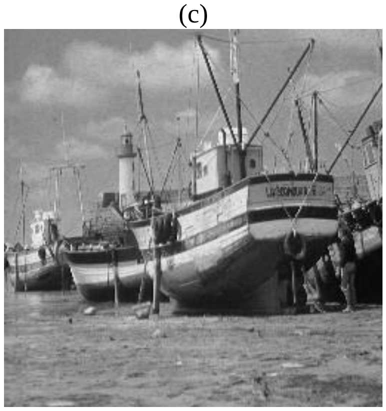

(a)

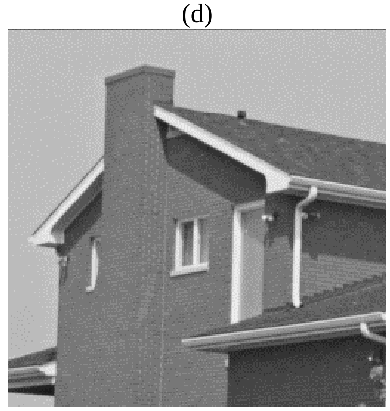

(b)

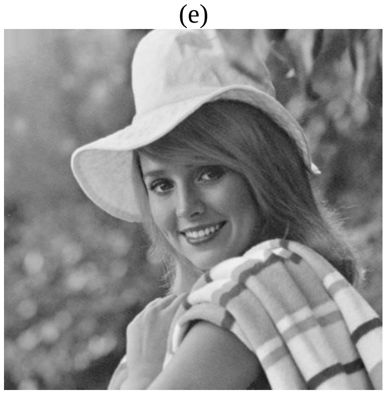


(c)


(d)


(e)


(f)


(g)

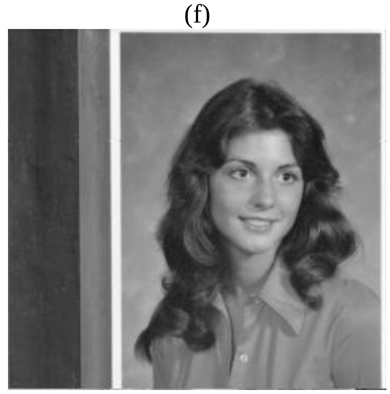

(h)

Figure 1. Eight Grey-scale Test Images

Table 4. The Example of a Pattern Table for $f^r: \mathbb{B}^2 \rightarrow \mathbb{B}^2$

Case 2 (mod 2)	Case 3 (mod 4)	A pixel in cover image	A pixel in stego image
		LSB_2	LSB_2
$1(=1_{(2)})$	$3(=11_{(2)})$	00	00
$0(=0_{(2)})$	$1(=01_{(2)})$	01	01
$0(=0_{(2)})$	$0(=00_{(2)})$	10	10
$1(=1_{(2)})$	$2(=10_{(2)})$	11	11

Table 5. Result of the Embedding Capacity of the Proposed and Previous Techniques

Test images	Difference expansion (bits)	Histogram Shifting (bits)	Proposed technique		
			Case 1 (bits)	Case 2 (bits)	Case 3 (bits)
Lena	39,566	47,201	65,524	131,680	130,906
Baboon	34,256	18,533	65,576	130,068	130,301
Airplane	40,657	30,631	65,456	131,014	131,230
Pepper	39,824	35,155	65,112	132,524	133,766
Boat	39,257	29,210	65,425	130,778	130,715
Man	39,447	40,748	67,276	130,578	128,837
House	40,002	35,868	66,782	130,852	123,277
Woman	39,872	37,602	68,258	130,430	131,238

have performed the experiments with examples of $f^r: \mathbb{B}^1 \rightarrow \mathbb{B}^1$ and $f^r: \mathbb{B}^2 \rightarrow \mathbb{B}^2$ as shown in Table 3 and 4, respectively.

In the proposed technique, if the embedding algorithm with $f^r: \mathbb{B}^1 \rightarrow \mathbb{B}^1$ and a cover image (size is $M \times M$) performs one round, the embedding capacity is roughly $M^2/4$bitsdue to the pattern table. If a secret and LSB pair of cover and stego pixels are 1 and 00 in Table 3, for example, the embedding can be performed. But, the embedding dose not perform the other LSBpairs such as 01, 10 and 11. That is, only one case of four LSBpairs is embedded. So, the probability of embedding is $1/4$. Hence, the embedding capacity is roughly $M^2/4$bits in one round.If the embedding algorithm with $f^r: \mathbb{B}^2 \rightarrow \mathbb{B}^2$ and a cover image (size is $M \times M$) performs one round, the embedding capacity is roughly $M^2/2$bits by the same probability logic.The result of the embedding capacity between the proposed and previous techniques [15, 27] is shown in Table 5. In Table 5, the embedding capacity of the proposed technique is greater than DE and histogram shifting techniques by 1.6 and 1.8 times, respectively. The size of $CI$is $512 \times 512 (= 262{,}144)$, and the embedding capacity of 'case 1' is roughly 65,536 bits in stochastic approach. The results of 'case 1' are close to 65,536 bits. Also, the results of 'case 1' and 'case 2' are close to 131,072 bits.

Table 6. Result of $PSNR$ of the Proposed and Previous Techniques

Test images	Difference expansion	Histogram Shifting	Proposed technique		
			Case 1	Case 2	Case 3
Lena	44.20	48.54	∞	∞	∞
Baboon	42.82	48.29	∞	∞	∞
Airplane	43.54	48.39	∞	∞	∞
Pepper	43.25	48.44	∞	∞	∞
Boat	43.84	48.38	∞	∞	∞
Man	44.56	48.56	∞	∞	∞
House	43.47	48.44	∞	∞	∞
Woman	43.88	48.57	∞	∞	∞

Table 7. Result of Multi Rounds Embedding of the Proposed and Previous Techniques for Lena Grey-Scale Image

Techniques		Tools	Round				
			1	2	3	4	5
Difference expansion		EC	39,566	63,676	84,066	101,089	120,619
		$PSNR$	44.20	42.86	41.55	40.06	37.66
Histogram shifting		EC	47,201	60,293	94,372	110,100	123,208
		$PSNR$	48.54	43.74	40.82	37.56	36.25
Proposed	Case 2	EC	131,680	263,421	526,952	1,053,893	2,107,807
		$PSNR$	∞	∞	∞	∞	∞

The distortion of stego image was naturally occurred because secret data were directly embedded into cover image in the previous techniques [15][27]. But, the distortion does not exist stego image in the proposed technique because the embedded position in CI of secret data was embedded into a location map. Also, cover and stego images are the same due to using the inverse property of reversible function. So, $PSNR$ result of our technique is infinity as shown in Table 6.

One of advantages for typical lossless data hiding techniques is that the even if an embedding procedure performs several times, the result of $PSNR$is good as shown in Table 7. In Table 7, if an embedding procedure performs five times, the embedding capacity of the proposed technique are greater than DE and histogram shifting technique by 17.4 and 17.1 times. Moreover, $PSNR$ of the previous techniques is progressively decreased, it is always infinity in our technique.

5. Conclusions

In this paper, we proposed a new lossless data hiding technique without distorition. The proposed technique is based on a reversible function, and it has a property of self-inverse which is composite operation between reversible functions. In order to embed and extract a secret data, we constructed a pattern table using the property of self-inverse, and this table generated a stego image. Although a location map was generated, distortion of stego image does not exist because the embedded position of secret data was embedded into location map. That is, secret data does not embed into cover image, directly. In the experimental results, the embedding capacity and $PSNR$ of the proposed technique were greater than it of the previous techniques.

Acknowledgement

This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Science, ICT & Future Planning (2011-0014977).

References

[1] S. Katzenbeisser and F. A. P. Petitcolas, "Information hiding techniques for steganography and digital watermarking", Norwood: Artech house, **(2000)**.
[2] I. J. Cox, M. L. Miller, J. A. Bloom, J. Fridrich and T. Kalker, "Digital watermarking and steganography", Morgan Kaufmann, **(2007)**.
[3] A. J. Menezes, P. C. Van Oorschot and A. Scott, "Handbook of Applied Cryptography", CRC press, BocaRaton, FL, **(1997)**.
[4] J.-C. Jeon, "Analysis of Hash Functions and Cellular Automata Based Schemes", International Journal of Security and Its Applications, vol. 7, no. 3, **(2013)**.
[5] V. Saxena, A. Harsulkar, P. Khemka and J. P. Gupta, "Performance Analysis of Color Channel for DCT Based Image Watermarking Scheme", International Journal of Security and its Applications, vol. 1, no. 2, **(2007)**.
[6] B. Vijaya Kumar, M. Radhika Mani and G. RoselineNesaKumari, "A New Marginal Color Image Water Marking Method based on Logical Operators", International Journal of Security and its Applications, vol. 3, no. 4, **(2009)**.
[7] N. Tiwari and M. Shandilya, "Secure RGB Image Steganography from Pixel Indicator to Triple Algorithm-An Incremental Growth", International Journal of Security and its Applications, vol. 4, no. 4, **(2010)**.
[8] A. Cheddad, J. Condell, K. Curran and P. McKevitt, "Digital image steganography: Survey and analysis of current methods", Signal Processing, vol. 90, no. 3, **(2010)**.
[9] S. H. Low, N. F. Maxemchuk, J. T. Brassil and L. O. Gorman, "Document marking and identification using both line and word shifting", Proceedings of the FourteenthAnnual Joint Conference of the IEEE Computer and Communications Societies, **(1995)** April 2-6.
[10] K. Fopalan, "Audio steganography using bitmodification", Proceedings of the IEEE international Conference on Acoustics, Speech, and Signal processing, **(2003)** April6-10.
[11] M. Iwata, K. Miyake and A. Shiozaki, "Digital Steganography Utilizing Features of JPEGImages", IEICE trans, Fundamentals. E87-A, **(2004)**.
[12] H. C. Wu, N. I. Wu, C. S. Tsai and M. S. Hwang, "Image Steganographic Scheme Based on Pixel-value Differencing and LSB Replacement Methods", IEE Proceedings Vision, Image & Signal Processing, vol. 152, no. 5, **(2005)**.
[13] J. Fridrich, M. Goljan and R. Du, "Lossless data embedding-new paradigm in digital watermarking", Special Issue on Emerging Applications of Multimedia Data Hiding, vol. 2, **(2002)**.
[14] T. Jun, "Reversible watermarking by difference expansion", Proceedings of workshop on multimedia and security, **(2002)**.
[15] J. Tian, "Reversible Data Embedding Using a Difference Expansion, Circuits and Systems for Video Technology", IEEE Transactions on, vol. 13, no. 8, **(2003)**.
[16] A. M. Alattar, "Reversible watermark using the difference expansion of ageneralized integer transform", IEEE Transactions on Image Processing, vol. 13, no. 8, **(2004)**.

[17] M. Carli, P. Campisi, and A. Neri, "Perceptual aspects in data hiding", Telecommunication Systems, vol. 33, **(2006)**.
[18] M. U. Celik, G. Sharma, A. M. Tekalp and E. Saber, "Lossless generalized-LSB data Embedding", IEEE Transactions on Image Processing, vol. 14, no. 2, **(2005)**.
[19] C. C. Chang, Lu and T. C., "A difference expansion oriented data hiding scheme for restoring the original host images", Journal of Systems and Software, vol. 79, no. 12, **(2006)**.
[20] C. C. Lee, H. C. Wu, C. S. Tsai, and Y. P. Chu, "Adaptive lossless steganographic scheme with centralized difference expansion", Pattern Recognition, vol. 41, no. 6, **(2008)**.
[21] Z. Ni, Y.-Q. Shi, N. Ansari and W. Su, "Reversible data hiding, Circuits and Systems for Video Technology", IEEE Transactions, vol. 16, no. 3, **(2006)**.
[22] C.-F. Lee and H.-L. Chen, "A novel data hiding scheme based on modulus function", Journal of Systems and Software, vol. 83, no. 5, **(2010)**.
[23] J.-D. Lee, Y.-H. Chiou and J.-M. Guo, "Reversible data hiding based on histogram modification of SMVQ indices", Information Forensics and Security, IEEE Transactions on, vol. 5, no. 4, **(2010)**.
[24] I.-C. Lin, Y.-B. Lin and C.-M. Wang, "Hiding data in spatial domain images with distortion tolerance", Computer Standards & Interfaces, vol. 31, no. 2, **(2009)**.
[25] H. Luo, F.-X. Yu, H. Chen, Z.-L. Huang, H. Li and P.-H. Wang, "Reversible data hiding based on block median preservation", Information Sciences, vol. 181, no. 2, **(2011)**.
[26] W.-L. Tai, C.-M. Yeh and C.-C. Chang, "Reversible data hiding based on histogram modification of pixel differences", Circuits and Systems for Video Technology, IEEE Transactions on, vol. 19, no. 6, **(2009)**.
[27] Y.-C. Li, C.-M. Yeh and C.-C. Chang, "Data hiding based on the similarity between neighboring pixels with reversibility", Digital Signal Processing, vol. 20, no. 4, **(2010)**.
[28] D. McMahon, "Quantum computing explained", Wiley, **(2007)**.

Authors

Sang-Ho Shin is currently a Ph.D. candidate in School of Computer Science and Engineering at Kyungpook National University. He received B.S. degree from Kumoh National Institute of Technology in 2006, the M.S. degree from Kyungpook National University in 2008. His current research interests are cryptography, cellular automata, quantum-dot cellular automata, quantum secret sharing and cloud computing security.

Ho Hwang is currently an undergraduate in Department of Computer Engineering at Kumoh National Institute of Technology. His current research interests are reverse engineering, computer forensics and quantum-dot cellular automata.

Jun-CheolJeon is currently a professor in Department of Computer Engineering at Kumoh National Institute of Technology. He received B.S. degree from Kumoh National Institute of Technology in 2000, the M.S. and Ph.D. degrees from Kyungpook National University in 2003 and 2007 respectively. His current research interests are cryptography, cellular automata, quantum-dot cellular automata and quantum computation.