Advanced Science and Technology Letters
Vol.29 (SIP 2013), pp.96-99
http://dx.doi.org/10.14257/astl.2013.29.20

Reversible Data Hiding Scheme Using Toffoli Gate

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

[1] Department of Computer Engineering,
Kumoh National Institute of Technology, Gumi, South Korea
[2] School of Computer Science and Engineering,
Kyungpook National University, Daegu, South Korea
kcats9731@gmail.com, shshin80@infosec.knu.ac.kr, jcjeon@kumoh.ac.kr

Abstract. In this paper, we propose a new reversible data hiding scheme without distortion of stego image. In the proposed scheme, Toffoli gate is used in embedding and extraction procedures. This gate provides a distortionless of stego image because it has a characteristic of self-inverse. In the experimental results, the embedding capacity and PSNR of the proposed technique are greater than the previous techniques have.

Keywords: Reversible data hiding; Toffoli gate; embedding capacity; PSNR

1 Introduction

Unlike typical data hiding, reversible data hiding is the technique that not only secret data is extracted and but also a cover image can be recovered at the same time. Although the embedding capacity is lower than it of typical data hiding, an image quality of stego image is high. Also, this technique can provide an authentication and integrity of a cover image because of reversibility. So, reversible data hiding techniques are applied in a sensitive field to change in pixel such as military and medical images [1].

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 [2]. 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. Moreover, this technique does not suitable for multiple embedding, which accumulates dramatic image distortion within consecutive pixel values.

In the meantime, Ni et al. proposed a data hiding technique based histogram shifting [3]. 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

[*] Corresponding author (Tel.:+82-54-478-7534)

ISSN: 2287-1233 ASTL

peak pixel areas after the original peak pixel values are shifted by the direction of zero point.

Table 1. An example of pattern table for $() \circ ()$

Case (mod 8)	A pixel in cover image	A pixel in stego image
	${}_{3}$	${}_{3}$
$1(=001_{(2)})$	000	000
$3(=011_{(2)})$	001	001
$2(=010_{(2)})$	010	010
$4(=100_{(2)})$	011	011
$5(=101_{(2)})$	100	100
$7(=111_{(2)})$	101	101
$0(=000_{(2)})$	110	110
$6(=110_{(2)})$	111	111

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.

In this paper, a new reversible data hiding scheme is proposed. In the proposed scheme, we use a Toffoli gate in embedding and extraction procedures. In the experimental results, the embedding capacity and PSNR of the proposed scheme are greater than it of the previous techniques.

2 Toffoli gate

Toffoli gate (also called a "*controlled-controlled-not*" (CCNOT) gate) is one of the reversible logics, and it is an universal logic gate, which means that any reversible circuit can be constructed. It has three-bit inputs and outputs [4].

This gate can be represented as a form of reversible Boolean function by Eq. (1).

$$() = ({}_{1}, {}_{2}, {}_{3}) = {}_{1}, {}_{2}, {}_{3}, \qquad (1)$$

where ${}_{1}$, ${}_{2}$ and ${}_{3}$ are ${}_{1}$, ${}_{2}$ and $({}_{1} \wedge {}_{2}) \oplus {}_{3}$ (where '$\wedge$' and '$\oplus$' indicate an and), respectively. It can be satisfied by Eq. (2).

$$() \circ () = , \qquad (2)$$

where '$\circ$' and indicate a composite arithmetic operation between reversible functions and an identity function, respectively. In this paper, a characteristic of Eq. (2) is used in embedding and extracting procedures.

3 Proposed Scheme

In the proposed scheme, the embedded positions of secret data are embedded into a location map. 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 reversible characteristic of Toffoli gate. The proposed scheme consists of two procedures: the embedding and extraction.

3.1 The embedding procedure

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: Construct a pattern table for $f_{(Toffoti)} \circ f_{(Toffoti)}$ as shown in Table 1. In Table 1, the order of converted secret of eight-ary's expression is as Eq. (3) And the number of orders is 8!. LSB_3 indicates least significant bit (LSB) three bits of a pixel value in an image. And the meaning of "case $(\bmod\ 8)$" is that an i-th pixel value (S_i) in a secret image (SI) is applied by modulo arithmetic operation.

$$\cdots \rightarrow 1 \rightarrow 3 \rightarrow 2 \rightarrow 4 \rightarrow 5 \rightarrow 7 \rightarrow 0 \rightarrow 6 \rightarrow 1 \rightarrow \cdots \qquad (3)$$

Step 2: Convert an i-th pixel value (S_i) in SI into eight-ary's expression as Eq. (4).

$$S_i \quad \{3 \times s_i, \ldots, 3 \times s_{(i+1)} - 1\}, \qquad (4)$$

where $1 \quad i \; N^2 - 1$. Let a set S consists of $3 \times N^2$ elements that compose of m-ary's values, and it is expressed by Eq. (5).

$$S = \{s_0, \ldots, s_{(3 \times N2 - 1)}\} \qquad (5)$$

Step 3: Embed a secret into a location map. 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 $f_{(Toffoti)} \circ A_{Toffoti)}$ as shown in Table 1, for example, if LSB_3 of $C_i (= 120)$ is 000 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-th index 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_3 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 extraction procedure

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

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

Step 1: Extract a j-th $(0 \; j \; 3 \times N^2 - 1)$ secret from i-th $(0 \; i \; M^2 - 1)$ 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.

S**tep 2**: Convert the calculated s_0**, ...,** $S(3\times N2\_1)$ into pixel values by 8. And then, they are reconstructed by a form of *RSI* and *RdI*.

Table 2. Result of the embedding capacity and PSNR between the proposed and previous techniques for three test images

		DE	HS	Proposed
Lena	Embedding capacity	39,566	47,201	131,672
	PSNR	44.20	48.54	oo
Baboon	Embedding capacity	34,256	18,533	130,064
	PSNR	42.82	48.29	oo
Airplane	Embedding capacity	40,657	30,631	131,212
	PSNR	43.54	48.39	oo

4 Analysis and Conclusion

Result of the embedding capacity and PSNR of the proposed scheme is greater than the previous techniques as shown in Table 2. Moreover, PSNR of the proposed scheme is infinity because of using the reversible characteristic of Toffoli gate. In this paper, we proposed a new reversible data hiding scheme using Toffoli gate. We have been performed the embedding and extraction procedures by a pattern table and a location map. We obtained that the embedding capacity and PSNR of the proposed scheme are greater than it of the previous techniques.

Acknowledgements. 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 (2013-028190).

References

1. Katzenbeisser, Stfan and Fabien A.P. Petitcolas: Information hiding techniques for steganography and digital watermarking. Norwood: Artech house (2000)
2. Jun Tian: Reversible Data Embedding Using a Difference Expansion. Circuits and Systems for Video Technology, IEEE Transactions on. Vol. 13(8), 890-896 (2003)
3. Yu-Chiang Li, Chia-Ming Yeh and Chin-Chen Chang: Data hiding based on the similarity between neighboring pixels with reversibility. Digital Signal Processing. Vol. 20(4), 1116-1128 (2010)
4. David McMahon: Quantum computing explained. Wiley (2007)