Bull. Soc. Photogr. Imag. Japan. (2014) Vol. 24 No. 1: 1–5

Original Paper

Hierarchical Image Authentication Based on Reversible Data Hiding

Shoko Imaizumi* and Kanichi Taniguchi*

Abstract: In this paper, we propose an image authentication based on hierarchical reversible data hiding. The proposed scheme decreases the costs necessary to detect and locate tampered areas by using efficiently multiplexed layers. This scheme reduces both the payload size and the amount of hash operations. We improved the structure of layers and the division of blocks in the conventional scheme. Performance analysis shows the validity of the proposed scheme.

Key words: Authentication, Tamper detection, Tamper localization, Reversible data hiding, Hash function

1. Introduction

With the growth in computational performance, it has become easy to modify digital images. Due to the increase in image tampering, image authentication has become important. Many tamper detection schemes have been studied to confirm image authenticity.

By using reversible data hiding [1–4], tamper detection schemes that recover the original image after authentication have been proposed [5–8]. The former schemes [5) 6)] use highly costed compression based data hiding, while the latter schemes [7) 8)] are free from compression techniques. This paper is focused on the latter non-compression-based schemes and is especially aimed at improving the conventional scheme [8)] in terms of the payload size and the amount of hash operations.

The conventional scheme [8)] detects tampered areas by comparing the hash values of recovered blocks with those extracted from stego blocks. This scheme can easily embed the target data into images and confirm image authenticity with accuracy. Moreover, it can detect not only tampering but also locate tampered areas in images. However, the conventional scheme has two problems. First, the embeddable pixels in each block are decreased because the size of blocks gets smaller on the bottom layers. Second, the amount of hash operations increases, making the blocks smaller, and the time for hash operations also increases. Therefore, we aim not to reduce the size of the unit for embedding and solve the above problems in the conventional scheme.

In this paper, we propose an efficient reversible image authentication that reduces both the payload size and the amount of hash operations. The proposed scheme improves the structure of layers and the division of blocks in the conventional scheme. It decreases costs necessary to detect and locate tampered areas by using hierarchically multiplexed layers. Our scheme is based on reversible data hiding. We give simulation results and show the validity of the proposed scheme.

2. Conventional Scheme

A conventional scheme [8)] can be a reversible image authentication that detects tampering and locates tampered areas efficiently. This scheme decreases costs through coarse-to-fine tamper localization by hierarchical data hiding, encipherment of only the top layer rather than all data among all layers, and the use of reversible data hiding without highly costed compression techniques.

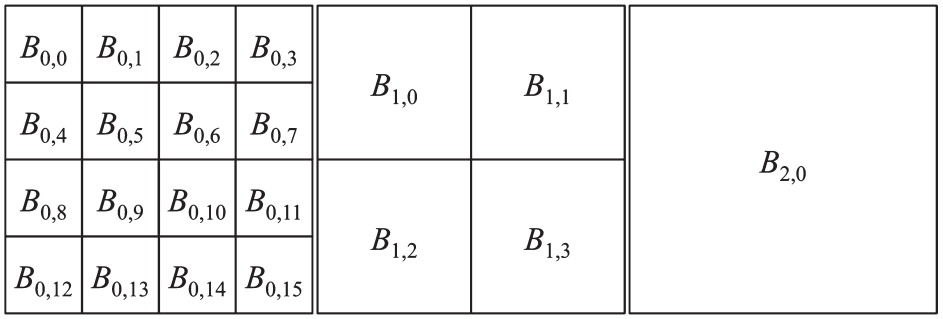
2.1 Data Hiding

We prepare image I with $X \times Y$ pixels and set I as I_l.

1) $l := 0$, $c := 0$.
2) Fig. 1 shows the order for dividing image I_l, hierarchically. We divide image I_l into C_l blocks in the l-th layer. The size of each block is $X_l \times Y_l$ pixels.
$$C_l = [X|X_l]\,[Y|Y_l], \quad l = 0, 1, ..., L-1, \tag{1}$$
where L is the number of layers.
3) N-bit hash value $h_{l,c}$ of block $B_{l,c}$, which is given as,
$$h_{l,c} = \{h_{l,c,n} \mid h_{l,c,n} \in \{0, 1\}\}, \quad c = 0, 1, ..., C_l - 1, \quad n = 0, 1, ..., N-1, \tag{2}$$
is embedded into $B_{l,c}$ itself by using reversible data hiding [4)]. Stego block $\hat{B}_{l,c}$ is obtained. Note that $h_{L-1,0}$ is encrypted by using an encryption key and is embedded into the image for higher security.
4) $c := c + 1$.
a) If $c = C_l$, combine all stego blocks $\hat{B}_{l,c}$. Stego image $\hat{I}_l$ is obtained.
b) Else, return to Step 3).
5) $l := l + 1$.

Received 19th, September 2013; Accepted 5th, March 2014

*Graduate School of Advanced Integration Science, Chiba University, 1-33 Yayoicho, Inage-ku, Chiba-shi, Chiba 263-8522, Japan



(a) L_0 ($l = 0$) (b) L_1 ($l = 1$) (c) L_2 ($l = 2$)

Fig. 1. Hierarchical division in the conventional scheme [8] ($L = 3$).

a) If $l := L$, stego image $\hat{I}$ is obtained.
b) Else, $c := 0$, $I_l := \hat{I}_{l-1}$, and return to Step 2).

2.2 Tamper detection and localization

We investigate stego image $\hat{I}$ with $X \times Y$ pixels and set $\hat{I}$ as $\hat{I}_l$.

1) $l := L - 1$, $c := 0$.
2) We divide stego image $\hat{I}_l$ into C_l blocks in the l-th layer, as shown in Fig. 1.
3) a) If the target block is determined as a genuine block in l + 1-th layer except in $l = L - 1$, go to 6).
   b) Else, embedded hash value $h_{l,c}$, which is given as Eq. (2), is extracted from stego block $\hat{B}_{l,c}$ by using reversible data hiding [4]. Block $B_{l,c}$ is restored. Note that in case of $l = L - 1$, $h_{L-1,0}$ is obtained by decryption using the key used in encryption.
4) N-bit hash value $\eta_{l,c}$ is calculated from restored block $B_{l,c}$.
   $\eta_{l,c} = \{\eta_{l,c,n} \mid \eta_{l,c,n} \in \{0, 1\}\}$. (3)
5) Extracted hash value $h_{l,c}$ is compared with $\eta_{l,c}$.
   a) If $h_{L-1,0} = \eta_{L-1,0}$, $B_{L-1,0}$ is determined to be a genuine block, that is, restored image I is an original image without tampering. Exit this procedure.
   b) If $h_{l,c} = \eta_{l,c}$ ($l \neq L - 1$), $B_{l,c}$ is determined to be a genuine block.
   c) Else, $B_{l,c}$ is determined to be a tampered block.
   Note that this step means tamper detection in $l = L - 1$ and tamper localization in $l \neq L - 1$.
6) $c := c + 1$.
   a) If $c = C_l$, combine all blocks $B_{l,c}$. Image I_l is obtained.
   b) Else, return to step 3).
7) $l := l - 1$,
   a) If $l = -1$, all tampered blocks are obtained.
   b) Else, $c := 0$, $\hat{I}_l := I_{l+1}$, and return to step 2).

2.3 Problems of the conventional scheme

The conventional scheme [8] using hash operations can detect tampering without multiple encryption procedures. It can also localize the positions of tampering by using the hierarchical structure. This scheme, however, increases both the payload size and the amount of hash operations when given a large number for hierarchy L.

In the next section, we propose an efficient scheme for composing a hierarchical structure. Our scheme reduces the above problems in the conventional scheme.

3. Proposed Scheme

In this section, we describe a novel authentication scheme based on reversible data hiding. The proposed scheme efficiently introduces a multiplex hierarchy to reduce both the payload size and the amount of hash operations. In this paper, we suppose that we divide an original image into 16 blocks. In case of 16 blocks, the number of layers L is four. Note that even if an image is tampered in multiple blocks, our scheme can correctly detect and locate the tampered blocks by the combination of these multiplexed layers.

3.1 Data Hiding

We prepare image I with $X \times Y$ pixels and set I as I_l.

1) $l := 0$, $m := 0$.
2) We divide image I_l into 16 blocks and assign numbers to them, as shown in Figs. 2 and 3. The size of each block is $[X/4 \times Y/4]$ pixels.
   a) If $l = 0$, assign each block $B_{0,c}$ to groups $G_{0,m}$, as shown in Fig. 4(a).
   $G_{0,0} = \{B_{0,0}, B_{0,5}, B_{0,10}, B_{0,15}\}$, (4)
   $G_{0,1} = \{B_{0,1}, B_{0,6}, B_{0,11}, B_{0,12}\}$, (5)
   $G_{0,2} = \{B_{0,2}, B_{0,7}, B_{0,8}, B_{0,13}\}$, (6)
   $G_{0,3} = \{B_{0,3}, B_{0,4}, B_{0,9}, B_{0,14}\}$. (7)
   b) If $l = 1$, assign each block $B_{1,c}$ to groups $G_{1,m}$, as shown in Fig. 4(b).
   $G_{1,0} = \{B_{1,0}, B_{1,4}, B_{1,8}, B_{1,12}\}$, (8)
   $G_{1,1} = \{B_{1,1}, B_{1,5}, B_{1,9}, B_{1,13}\}$, (9)
   $G_{1,2} = \{B_{1,2}, B_{1,6}, B_{1,10}, B_{1,14}\}$, (10)
   $G_{1,3} = \{B_{1,3}, B_{1,7}, B_{1,11}, B_{1,15}\}$. (11)
   c) If $l = 2$, assign each block $B_{2,c}$ to groups $G_{2,m}$, as shown in Fig. 4(c).
   $G_{2,0} = \{B_{2,0}, B_{2,1}, B_{2,2}, B_{2,3}\}$, (12)
   $G_{2,1} = \{B_{2,4}, B_{2,5}, B_{2,6}, B_{2,7}\}$, (13)
   $G_{2,2} = \{B_{2,8}, B_{2,9}, B_{2,10}, B_{2,11}\}$, (14)
   $G_{2,3} = \{B_{2,12}, B_{2,13}, B_{2,14}, B_{2,15}\}$. (15)
   d) If $l = 3$, assign all blocks $B_{3,c}$ to group $G_{3,0}$, as shown in Fig. 4(d).
   $G_{3,0} = \{B_{3,0}, B_{3,1}, B_{3,2}, B_{3,3}, B_{3,4}, B_{3,5}, B_{3,6}, B_{3,7}, B_{3,8}, B_{3,9}, B_{3,10}, B_{3,11}, B_{3,12}, B_{3,13}, B_{3,14}, B_{3,15}\}$. (16)
   Note that the number of groups M_l is one in $l = 3$, while that is four in $l = 0$, 1, and 2.

Fig. 2. Division of image.

$B_{l,0}$	$B_{l,1}$	$B_{l,2}$	$B_{l,3}$
$B_{l,4}$	$B_{l,5}$	$B_{l,6}$	$B_{l,7}$
$B_{l,8}$	$B_{l,9}$	$B_{l,10}$	$B_{l,11}$
$B_{l,12}$	$B_{l,13}$	$B_{l,14}$	$B_{l,15}$

Fig. 3. Block numbers.

3) N-bit hash value $h_{l,m}$ of group $G_{l,m}$, which is given as,
$h_{l,m} = \{h_{l,m,n} \mid h_{l,m,n} \in \{0, 1\}\}$,
$n = 0, 1, ..., N-1$. (17)
is embedded into $G_{l,m}$ itself by using reversible data hiding [4]. Stego group $\hat{G}_{l,m}$ is obtained. Note that $h_{3,0}$ is encrypted by using an encryption key and is embedded into the image for higher security.
4) $m := m + 1$.
a) If $m = M_l$, we combine all stego groups $\hat{G}_{l,m}$. Stego image $\hat{I}_l$ is obtained.
b) Else, return to step 3).
5) $l := l + 1$.
a) If $l = 4$, stego image $\hat{I}$ is obtained.
b) Else, $m := 0$, $I_l := \hat{I}_{l-1}$, and return to step 2).

3.2 Tamper detection and localization

We investigate stego image $\hat{I}$ with $X \times Y$ pixels and set $\hat{I}$ as $\hat{I}_l$.

1) $l := 3$, $m := 0$.
2) We divide stego image $\hat{I}_l$ into 16 blocks and assign numbers to them, as shown in Figs. 2 and 3, and assign each block $B_{l,c}$ to groups $G_{l,m}$, as shown in Fig. 4.
3) Embedded hash value $h_{l,m}$ of original group $G_{l,m}$, which is given as Eq. (17), is extracted from stego group $\hat{G}_{l,m}$ by using reversible data hiding [4]. Group $G_{l,m}$ is restored. If $l = 3$, $h_{3,0}$ is obtained by decryption using the key used in encryption.
4) N-bit hash value $\eta_{l,m}$ is calculated from restored group $G_{l,m}$.
$\eta_{l,m} = \{\eta_{l,m,n} \mid \eta_{l,m,n} \in \{0, 1\}\}$. (18)
5) Extracted hash value $h_{l,m}$ is compared with $\eta_{l,m}$.
a) If $h_{3,0} = \eta_{3,0}$, $G_{3,0}$ is determined to be a genuine group, that is, restored image I is an original image without tampering. Exit this procedure.

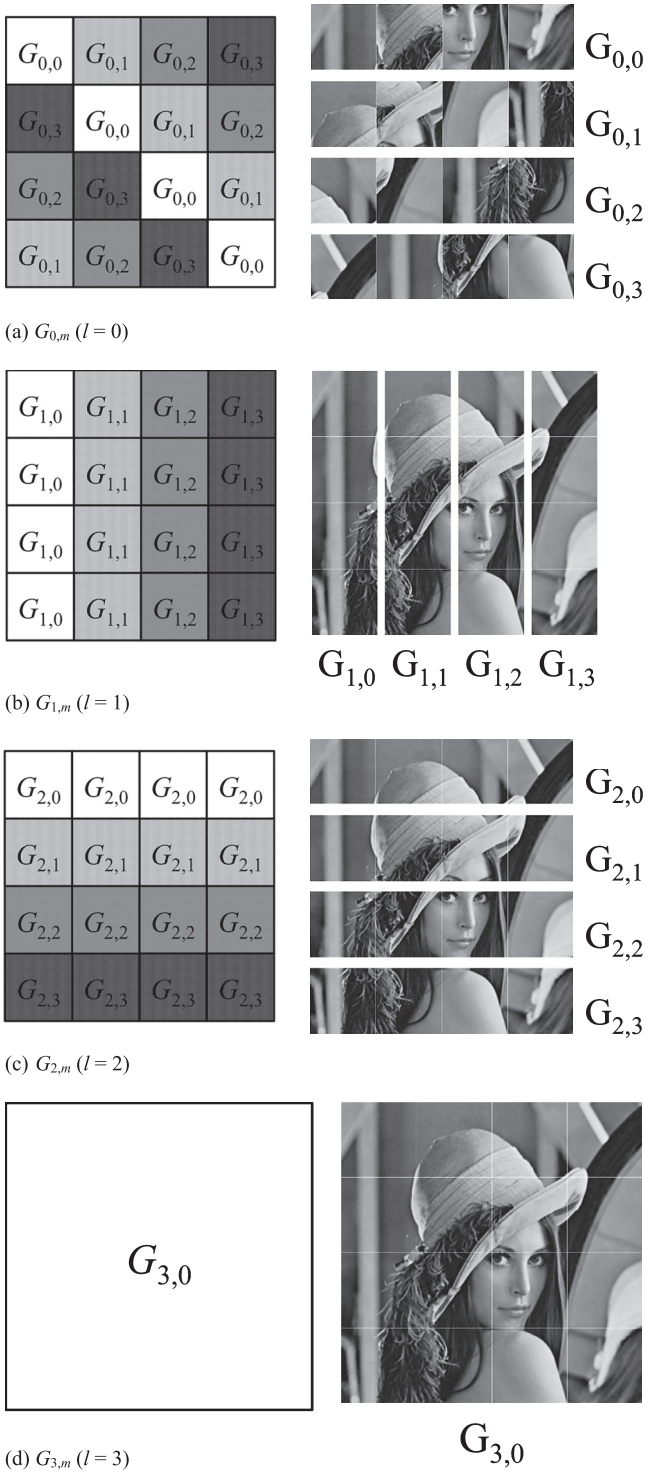


Fig. 4. Hierarchical division and grouping in the proposed scheme.

b) If $h_{l,m} = \eta_{l,m}$ ($l \neq 3$), $G_{l,m}$ is determined to be a genuine group.
c) Else, $G_{l,m}$ is determined to be a tampered group.
Note that this step means tamper detection in $l = 3$ and tamper localization in $l \neq 3$.
6) $m := m + 1$.
a) If $m = M_l$, combine all groups $G_{l,m}$. Image I_l is obtained.
b) Else, return to step 3).
7) $l := l - 1$.
a) If $l = -1$, all tampered groups are obtained.
b) Else, m := 0, $\hat{I}_l := I_{l+1}$, and return to step 2).

(a) Lenna (b) Airplane (c) Text

Fig. 5. 256 × 256-sized grayscale images from SIDBA [9].

Table 1. Payload size [bits].

Layer	Proposed	Conventional [8]
L_0	256	256
L_1	1024	1024
L_2	1024	4096
L_3	1024	—
Total	3328	5376

Table 2. Amount of hash operations [times].

Layer	Proposed	Conventional [8]
L_0	1	1
L_1	4	4
L_2	4	16
L_3	4	—
Total	13	21

8) Determine the blocks, all of whose groups $G_{l,m}$ have been tampered, as the tampered blocks.

3.3 Feature

Tables 1 and 2 show comparisons of the payload size and the amount of hash operations, respectively. Our scheme has reduced both payload and hash operations by 38%, respectively, compared with the conventional scheme [8]. A single hash operation is needed for tamper detection in both the proposed and the conventional schemes. In this example, the amount of hash operations for tamper localization is 12 times in the proposed scheme, while that is 20 times in the conventional scheme.

4. Experimental Results

The proposed scheme was evaluated with 256 × 256-sized, i.e., $X = Y = 256$, 8-bit grayscale bitmap images from SIDBA [9], as shown in Fig. 5. We summarize the conditions of the experiments in Table 3.

Figs. 6(a) and 6(b) show a couple of examples of stego images for the proposed scheme and the conventional scheme [8], respectively. We summarize the evaluation for the stego images by PSNR in Fig. 7. The PSNR for the stego image "Lenna" using the proposed scheme was 42.11 dB, while that using the conventional scheme was 35.43 dB. In the cases for "Airplane" and "Text," the proposed scheme similarly improved the PSNR over the conventional scheme. Thus, the proposed scheme is efficient for embed-

Table 3. Experimental Conditions.

Image size [pixels]	256 × 256	
Hash function	SHA-256	
Hash length N [bits]	256	
Number of layers L	Proposed	Conventional [8]
	4	3

(a) Proposed (b) Conventional [8]

Fig. 6. Stego images by using the proposed scheme and the conventional scheme [8].

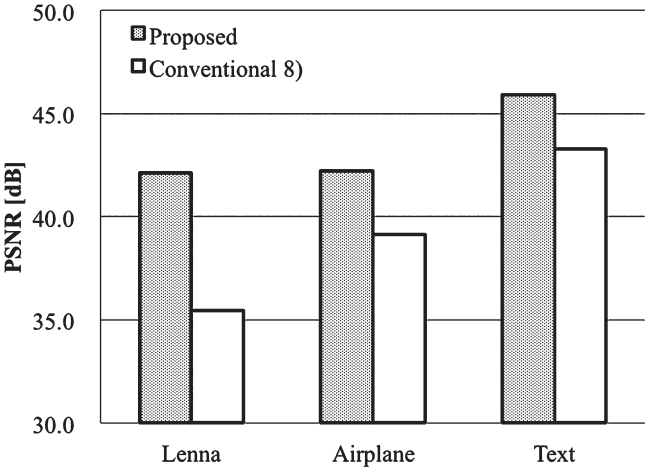


Fig. 7. PSNRs of the stego images.

(a) Tampered image (b) Detected image

Fig. 8. Result of tamper localization.

ding data.

For example, a tampered area is shown in Fig. 8(a). In this case, the tampered blocks are detected as shaded ones in the proposed scheme, as shown in Fig. 8(b).

5. Summary

We proposed an efficient image authentication based on reversible data hiding. The proposed scheme introduces hierarchically multiplexed layers to detect and locate tampered areas. This scheme decreases both the payload size and the amount of hash operations. We improved the structure of layers and the division of blocks in the conventional scheme. Through comparison with the conventional scheme, we showed the validity of the proposed scheme.

Acknowledgement

This work was supported by the Photographic Research Fund of Konica Minolta Science and Technology Foundation.

References

1) J. Tian, “Reversible data embedding using a difference expansion”, IEEE Trans. Circuits Syst. Video Technol., **13**(8), 890–896 (2003).
2) A. M. Alattar, “Reversible watermark using the difference expansion of a generalized integer transform”, IEEE Trans. Image Process., **13**(8), 1147–1156 (2004).
3) D. M. Thodi and J. J. Rodriguez, “Expansion embedding techniques for reversible watermarking”, IEEE Trans. Image Process., **16**(3), 721–730 (2007).
4) H. L. Jin, M. Fujiyoshi, and H. Kiya, “Lossless data hiding in the spatial domain for high quality images”, IEICE Trans. Fundamentals., **E90-A**(4), 771–777 (2007).
5) J. Fridrich, M. Goljan, and R. Du, “Invertible authentication”, Proc. SPIE, **4314**, 197–208 (2001).
6) M. U. Celik, G. Sharma, and A. M. Tekalp, “Lossless watermarking for image authentication: a new framework and an implementation”, IEEE Trans. Image Process., **15**(4), 1042–1049 (2006).
7) K. Watanabe, M. Fujiyoshi, and H. Kiya, “Image Authentication with Access Control Based on Reversible Data Hiding”, Technical report of IEICE, **110**(115), 81–86 (2010), (in Japanese, ICSS2010-25).
8) S. Han, M. Fujiyoshi, and H. Kiya, “A reversible image authentication method without memorization of hiding parameters”, IEICE Trans. Fundamentals., **E92-A**(10), 2572–2579 (2009).
9) M. Onoe, M. Sasaki, and Y. Inamoto, “SIDBA Standard Image Data Base”, MIPC Report, **79**(1) (1979).