PAPER Special Section on Signal Processing

An Efficient Reversible Image Authentication Method

Seungwu HAN[†a)], ***Student Member***, **Masaaki FUJIYOSHI**[††], ***and*** **Hitoshi KIYA**[††], ***Members***

SUMMARY This paper proposes an image authentication method that detects tamper and localizes tampered areas efficiently. The efficiency of the proposed method is summarized as the following three points. 1) This method offers coarse-to-fine tamper localization by hierarchical data hiding so that further tamper detection is suppressed for blocks labeled as genuine in the uppper layer. 2) Since the image feature description in the top layer is hidden over an image, the proposed method enciphers the data in the top layer rather than enciphers all data in all layers. 3) The proposed method is based on the reversible data hiding scheme that does not use highly-costed compression technique. These three points makes the proposed method superior to the conventional methods using compression techniques and methods using multi-tiered data hiding that requires integrity verification in many blocks even the image is genuine. Simulation results show the effectiveness of the proposed method.

key words: *integrity verification, one-way hash function, symmetric cipher algorithm, payload*

1. Introduction

Currently, powerful computers and smart software make modification of digital images very easy. Moreover, digital images are often widely distributed through the Internet. It is, therefore, very simple for malicious users to make any tampered image available to others. Insuring digital image integrity has therefore became a major issue. An appropriate mechanism is essential to protect the integrity of an image.

Source authentication and integrity verification of digital multimedia contents often have been performed by digital signatures. A digital signature is a data string which associates a piece of information with some original entity [1], [2]. Secure one-way hash function is generally applied to an image to produce a digital signature. It, however, requires the storage and transmission of a signature string for authentication besides the transmission of the image itself.

To improve such inconvenience, image authentication methods utilizing data hiding technique have been proposed [3]–[8]. In these methods, the signature or the feature of an image is embedded into and extracted from the image, where an image conveying data is referred to as a *stego* image. These methods, however, distort images and cannot recover the original images after authentication.

By using *reversible* data hiding schemes [9]–[12], image tamper detection methods that recover the original image after authentication have been proposed [13]–[17]. The former two methods [13], [14] employ highly-costed compression based data hiding, while the latter three methods [15]–[17] are free from compression technique. This paper focuses the latter non-compression-based methods.

Among non-compression-based conventional reversible authentication methods, one [15] does not serve the accurate tamper localization because of its data hiding capacity limitation, while the rest [16], [17] are able to serve accurate tamper localization by multi-tiered data hiding. Methods use multi-tiered data hiding, however, have to verify integrity in many blocks for complete tamper detection, though the target image is genuine.

This paper proposes an efficient reversible authentication method. The proposed method is cost effective in three points. 1) It serves coarse-to-fine tamper localization by hierarchical data hiding [14] so that further integrity verification is suppressed for blocks labeled genuine in upper layer. 2) It enciphers the signature for secure authentication, but only in the top layer in which signature is hidden over the image [17]. 3) It is based on the non-comprresion-based data hiding scheme [12].

This paper consists of six sections. In Sect. 2, a brief overview of the conventional methods [13]–[17] are given. The novel method is proposed in Sect. 3. Experimental results and further discussion for making the proposed method more practical are given in Sect. 4 and 5, respectively. Conclusions are drawn in Sect. 6.

2. Background

This section gives the framework of reversible image authentication and particular converntional methods.

2.1 Reversible Image Authentication

A typical reversible image authentication method is shown in Fig. 1. A reversible image authentication method has two steps in the process to generate stego images as shown in Fig. 1(a): an authentication data generation and reversible data hiding. That is, in part (a), the generated data are hidden to the image in a reversible manner.

The counterpart process is shown in Fig. 1(b): an extraction of hidden data, recovery of the original image, and integrity verification. In part (b), authentication data are generated from the recovered image, and are compared with

Manuscript received December 11, 2007.
Manuscript revised March 14, 2008.

[†]The author is with the Graduate School of System Design, Tokyo Metropolitan University, Hino-shi, 191-0065 Japan.
[††]The authors are with the Faculty of System Design, Tokyo Metropolitan University, Hino-shi, 191-0065 Japan.
a) E-mail: han-seungwu@sd.tmu.ac.jp

DOI: 10.1093/ietfec/e91–a.8.1907

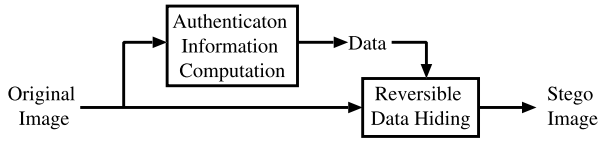
the extracted data. If two data are identical, it determines that the image has not been modified, and the recovered image is labeled as genuine.

2.2 Conventional Methods and Those Problems

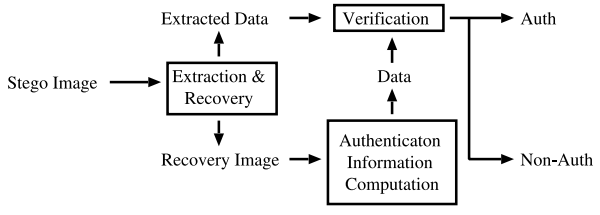
This section briefly mentions the typical conventional methods; they are compression-based methods [13], [14] and non-compression-based methods [15]–[17].

Among compression-based methods, one method [13] reversibly compresses the least significant bitplane among bitplanes meeting the criteria that the rooms generated by compression is larger than the length of the hash of the whole image. The other method [14] uses arithmetic encoder to reversibly compresses less significant bitplanes of the image by utilizing more significant bitplanes to create the rooms to hiding data block-by-block. This method repeats such embedding process multiple times. They use compression techniques that usually cost highly.

On the other hand, the non-compression-based methods [15]–[17] are based on the block-based reversible data hiding scheme [12] that uses statistics of pixels. They, however, have problems. Since one method [15] has limitation in the data hiding capacity for small blocks, it does not serve accurate tamper localization. The other methods [16], [17] using multi-tiered data hiding (Fig. 2) localizes suspected areas in each tier and logically multiplies areas to serve accurate tamper localization. They, however, have to verify integrity in many blocks, though the target image is genuine.



(a) Data generation and data hiding.



(b) Data extraction, image recovery, and verification.

Fig. 1 Block diagram of typical reversible image authentication.

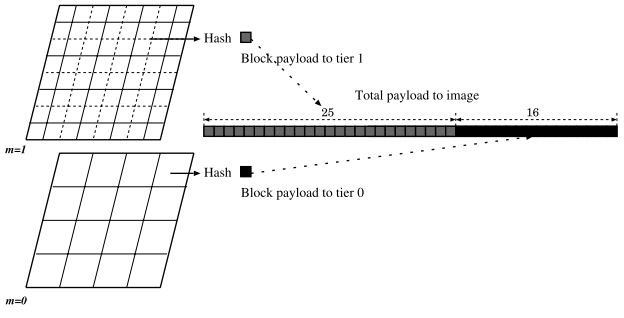


Fig. 2 An example of multi-tiered data hiding [16], [17].

In the next section, an efficient reversible authentication method is proposed.

3. Propose Method

This section proposes an image authentication method that improves the efficiency of tamper detection and localization through the following three features.

1) The proposed method is based on the reversible data hiding scheme [12] that does not use highly-costed compression techniques.
2) The proposed method localizes tampered areas with a coarse-to-fine manner so that no further integrity verification is required to blocks once labeled as genuine.
3) The proposed method enciphers only the image feature description that is hidden over the image as the top layer [17].

As in Fig. 3, the proposed method consists of two parts. They are part (a) and (b) which each part has $(M+1)$ stages, where a stage is for a *layer*. Each stage in part (a) has two steps: feature generation and data hiding. Meanwhile, each stage in part (b) has three steps: hidden data extraction, image recovery, and integrity verification.

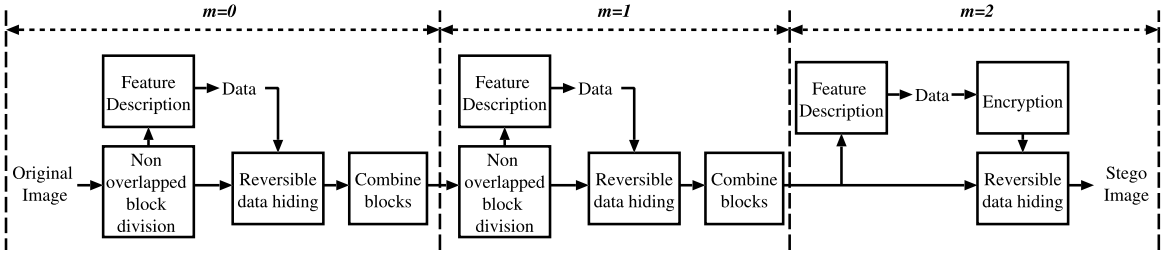
The proposed method hides the image feature description to the image hierarchically as shown in Fig. 4. For the m-th layer, an image with $X \times Y$ pixels is divided into H_m blocks which each block consists of $X_m \times Y_m$ pixels, where $H_m = XY/X_mY_m$ and $m = 0, 1, \ldots, M-1$. An image feature descriptor that generates an N-bits length data string is applied to each block, and the generated data string is hidden to the block from that data string is generated. That is, integrity is verified in terms of blocks.

3.1 Image Feature Description

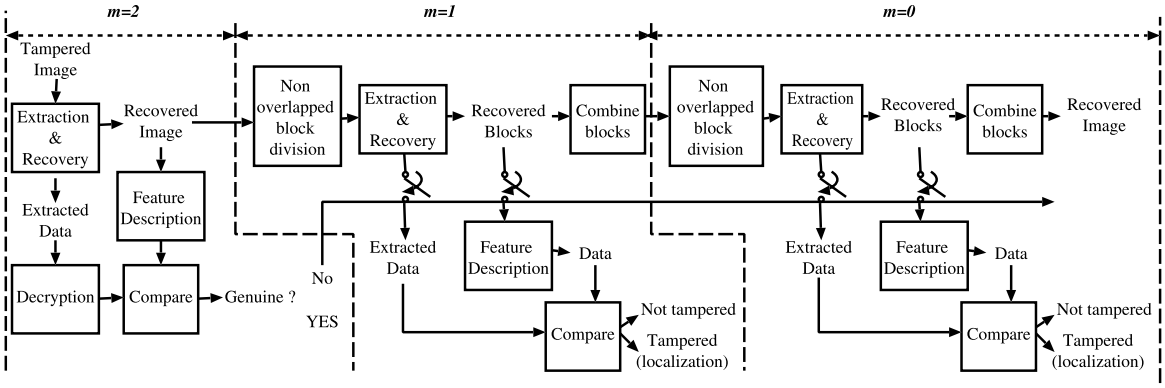
An image feature descriptor generates a data string that is to be reversibly hidden to the input image. Though any arbitrary descriptor is able to be used, an one way hash function is employed in this paper to improve the reliability of tamper detection and to guarantee the *payload* (length) of the description. An one-way hash function that generates N-bits length hash is applied to each block in each layer. The hash for the h-th block in the m-th layer is represented by $\mathbf{w}_{m,h} = \left\{ w_{m,h,n} \middle| w_{m,h,n} \in \{0,1\}, n = 0, 1, \ldots, N-1 \right\}$, where $h = 0, 1, \ldots, H_m - 1$.

3.2 Encipherment of Feature Description

The proposed method employs a cipher algorithm for secure authentication, it, however, enciphers only the description of the M-th layer, $\mathbf{w}_{M,H_M}$, where $H_M = 1$. Though any arbitrary cipher algorithm is able to be used, a symmetric cipher algorithm is employed in this paper to guarantee the payload of the description. The cipher description is represented by



(a) Data generation and data hiding.



(b) Data extraction, image recovery, and verification.

Fig. 3 The proposed method (the number of layers $M = 2$).

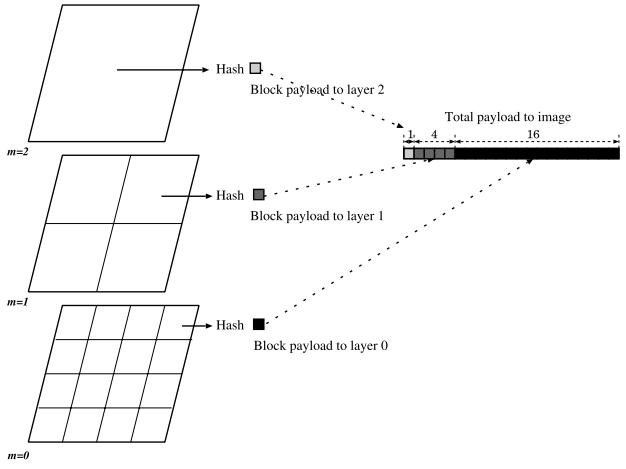
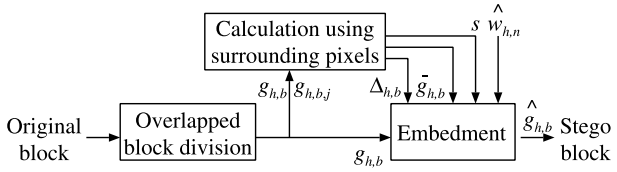
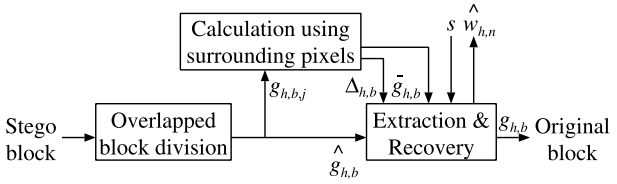


Fig. 4 An example of layer structure for an image in the proposed method (the number of layers $M = 2$).



(a) Data hiding algorithm.



(b) Hidden data extraction and image recovery algorithm.

Fig. 5 Reversible data hiding in the proposed method.

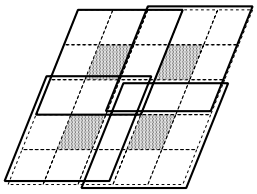
$\hat{\mathbf{w}}_{M,H_M} = \left\{\hat{w}_{M,H_M,n} \middle| \hat{w}_{M,H_M,n} \in \{0,1\}, n = 0,1,\ldots,N-1\right\}$, if it is specified. Hereafter, $\mathbf{w}_{m,h}$ and $\hat{\mathbf{w}}_{m,h}$ are simply represented by $\mathbf{w}_{m,h}$ unless an explicit distinction between them is required.

3.3 Reversible Data Hiding

This section describes the non-compression-based data hiding algorithm (Fig. 5(a)) and the corresponding hidden data extraction and image recovery algorithm (Fig. 5(b)) are described. It also describes a parameter that is used in both algorithms.

The proposed method reversibly hides N-bits hash $\mathbf{w}_h$ to the corresponding h-th block in the m-th layer based on the reversible data hiding scheme [12]. In a data hiding step, a bit of a hash is hidden in terms of overlapped subblocks as shown in Fig. 6(a). Pixel $g_{m,h,b}$ is the center pixel of the b-th overlapped subblock in the h-th block in the m-th layer, where $b = 0, 1, \ldots, B_{m,h} - 1$.

This data hiding uses a parameter that is used for all H_m blocks and commonly used in embedding and extraction processes. Therefore, derivation of the parameter is firstly described in the next section. Then, embedding and extraction algorithms that both of them use the derived parameter



(a) Placement of subblocks.

$g_{h,b,0}$	$g_{h,b,1}$	$g_{h,b,2}$
$g_{h,b,3}$	$g_{h,b}$	$g_{h,b,4}$
$g_{h,b,5}$	$g_{h,b,6}$	$g_{h,b,7}$

(b) A subblock.

Fig. 6 Subblock for data hiding.

are described.

It is noted that the parameter can be unified for all blocks in all layers as described in Sect. 5. That is, only one parameter is used for all blocks among all layers in an image.

3.3.1 Parameter Derivation

The algorithm to derive parameter s_m for the m-th layer from an original image is following.

1. $h := 0$.
2. $b := 0, \beta_{m,h} := 0$.
3. In the b-th subblock of the h-th block (Fig. 6(b)), the average value is obtained from the surrounding pixels, $g_{m,h,b,j}$ ($j = 0, 1, \ldots, 7$), by Eq. (1). Difference between center pixel $g_{m,h,b}$ and average $\bar{g}_{m,h,b}$ is also derived by Eq. (2).

$$\bar{g}_{m,h,b} = \left\lfloor \frac{1}{8} \sum_{j=0}^{7} g_{m,h,b,j} \right\rfloor, \tag{1}$$

$$d_{m,h,b} = g_{m,h,b} - \bar{g}_{m,h,b}. \tag{2}$$

4. $\Delta_{h,b}$ is obtained by Eq. (3).

$$\Delta_{m,h,b} = \begin{cases} g_{\max,m,h,b} - \bar{g}_{m,h,b}, & d_{h,b} \geq 0 \\ g_{\min,m,h,b} - \bar{g}_{m,h,b}, & d_{h,b} < 0 \end{cases}, \tag{3}$$

$$g_{\max,m,h,b} = \max_j g_{m,h,b,j}, \tag{4}$$

$$g_{\min,m,h,b} = \min_j g_{m,h,b,j}. \tag{5}$$

5. Parameter $s_{m,h,b}$ that is a candidate of s_m is derived by Eq. (6).

$$s_{m,h,b} = \begin{cases} \left|\Delta_{m,h,b}\right|, & \bar{g}_{m,h,b} + 2d_{m,h,b} < 0 \\ & \text{or} \quad 2^K - 2 < \bar{g}_{m,h,b} + 2d_{m,h,b} \\ \infty, & \text{others} \end{cases}, \tag{6}$$

where K represents the quantization bits for pixel values, i.e., $K = 8$ for eight-bits quantized grayscale images.

6. If $s_{m,h,b} = \left|\Delta_{m,h,b}\right|, \beta_{m,h} := \beta_{m,h} + 1$.
7. $b := b + 1$. Continue to Step 2 unless $b = B$.
8. The minimum of $s_{m,h,b}$'s becomes $s_{m,h}$. That is,

$$s_{m,h} = \min_b s_{m,h,b}. \tag{7}$$

9. $h := h + 1$. Continue to Step 2 unless $h = H$.
10. The minimum of $s_{m,h}$'s becomes s_m. That is,

$$s_m = \min_h s_{m,h}. \tag{8}$$

3.3.2 Hiding Algorithm

As in Fig. 5(a), this algorithm decides whether $g_{m,h,b}$ is embeddable or not based on parameter s_m. One bit data $w_{m,h,n}$ is hidden into an embeddable pixel, $g_{m,h,b}$, by the following steps.

1. $h := 0$.
2. $b := 0, n := 0$.
3. By Eq. (9), $\hat{g}_{m,h,b}$, the pixel with hidden data, is derived from embeddable $g_{h,b}$.

$$\hat{g}_{m,h,b} = \begin{cases} \bar{g}_{m,h,b} + 2d_{m,h,b} + w_{m,h,n}, & \left|\Delta_{m,h,b}\right| < s_m \\ g_{m,h,b}, & \text{others} \end{cases}. \tag{9}$$

4. If $\left|\Delta_{m,h,b}\right| < s_m, n := n + 1$.
5. $b := b + 1$. Continue Step 3 until $b = B$.
6. $h := h + 1$. Continue Step 2 until $h = H$.
7. H_m of Stego blocks are combined to form stego image.

3.3.3 Hidden Data Extraction and Image Recovery Algorithm

As in Fig. 5(b), the following algorithm is applied to stego image blocks to extract hidden data $\mathbf{w}_{m,h}$ and restore the original image block.

1. $h := 0$.
2. $b := 0, n := 0$.
3. $\Delta_{m,h,b}$ is obtained by Eq. (10).

$$\Delta_{m,h,b} = \begin{cases} g_{\max,m,h,b} - \bar{g}_{m,h,b}, & \hat{g}_{m,h,b} - \bar{g}_{m,h,b} \geq 0 \\ g_{\min,m,h,b} - \bar{g}_{m,h,b}, & \hat{g}_{m,h,b} - \bar{g}_{m,h,b} < 0 \end{cases}. \tag{10}$$

4. Data bit $w_{m,h,n}$ is extracted by the following equation, if $\left|\Delta_{m,h,b}\right| < s_m$.

$$w_{m,h,n} = (\hat{g}_{m,h,b} - \bar{g}_{m,h,b}) \bmod 2. \tag{11}$$

5. Pixel $g_{m,h,b}$ of the image is restored by Eq. (12).

$$g_{m,h,b} = \begin{cases} \frac{\hat{g}_{m,h,b} + \bar{g}_{m,h,b} - w_{m,h,n}}{2}, & \left|\Delta_{m,h,b}\right| < s_m \\ \hat{g}_{m,h,b}, & \text{others} \end{cases}. \tag{12}$$

6. If $\left|\Delta_{m,h,b}\right| < s_m, n := n + 1$.
7. $b := b + 1$. Continue to Step 3 unless $b = B$.
8. N-bits data sequence $\mathbf{w}_{m,h}$ and h-th recovered image block are obtained.
9. $h := h + 1$. Continue to Step 2 unless $h = H$.
10. H_m of $\mathbf{w}_{m,h}$'s and the recovered image in the m-layer are obtained.

This algorithm requires image-and layer-dependent parameter s_m to extract data and recover image in the m-th layer in an image. That is, s_m's have to be transmitted from the data hiding step. It is, however, noted that the parameter can be unified for all blocks in all layers as described in Sect. 5. Furthermore, it is noted that no parameter transmission is required at the data extraction and image recovery side by introducing the default parameter that does not depend to any image, as described in Sect. 5.

3.4 Integrity Verification

Integrity verification process in this proposed method is comparing two image features as shown in Fig. 3(b). One is the extracted (and decrypted for the M-th layer) feature description, and the other is the feature description generated from the recovered image. If both descriptions are the same among all H_m blocks, the image is not modified. On the other hand, one is different from the other in the h-th block in the m-th layer, the h-th block of the image is altered. That is, the proposed method detects tampering and also localizes the altered region by the unit of block.

Since the proposed method has the layer structure as shown in Fig. 4, if the image is labeled as genuine in the M-th layer, integrity verification among the rest M layers are completely unnecessary. The proposed method, then, skips regeneration of the feature description from the recovered image and comparing two features as shown in Fig. 3(b). If the h-th block is labeled as tampered in the m-th layer, this method verifies integrity in the $(m-1)$-th layer. It, however, integrity verification is applied to only the blocks subordinate to the tampered block, and the blocks subordinate to the genuine blocks are free from integrity verification.

3.5 Features

This section describes the three features of the proposed method that contributes efficient image authentication.

3.5.1 Hierarchical Data Hiding

As shown in Fig. 4, the proposed method hides image feature descriptions to the image hierarchically [14] rather than hides data in a multi-tiered structure [16], [17]. Hierarchical data hiding introduces coarse-to-fine tamper localization to the proposed method. That is, successive integrity verification is only applied to blocks that are subordinate to the block labeled as tampered in the upper layer. The rest blocks that are subordinate to the genuine blocks are free from integrity verification process; regenerate of the feature description from recovered image block and comparing the regenerated and extracted features. In particular, if the integrity of the image is verified in the top layer, the M-th layer, no further verification is required in the proposed method. That is, integrity verification process runs only once. While the multi-tier based method [16] has to verify integrity in many blocks, though the image is genuine.

3.5.2 Encipherment of Only the Top Layer

As described in Sect. 3.2, the proposed method employs a cipher algorithm for secure authentication, but it enciphers the description in the top layer [17], the M-th layer, rather than the descriptions in all blocks in all layers. Since the top layer covers whole the image as shown in Fig. 4, it is able to detect tamper with only the top layer though tampered areas are not able to be localized. That is, it can decide whether tamper exists by the top layer. It is, therefore, determined that secure authentication is served even the proposed method enciphers only the top layer. Since it is general that a cipher algorithm costs highly, the proposed method is superior in the cost for cipher than encipherment of all features in all layers and encipherment of the image itself.

3.5.3 Non-compression-Based Reversible Data Hiding

The proposed method is based on the reversible data hiding scheme [12] that does not use any highly-costed compression technique as described in Sect. 3.3. While the conventional methods [13], [14] employ compression techniques, in particular, one conventional method [14] uses arithmetic codec. Since it is general that a compression technique costs highly, the proposed method that does not use any compression technique is superior in costs than the conventional methods [13], [14].

4. Experimental Results

4.1 Tamper Detection and Localization Ability

The proposed scheme was evaluated with 512×512-sized, i.e., $X = Y = 512$, grayscale images from CIPR-RPI [18] that are shown in Fig. 7. In this evaluation, SHA-256 [19] was used as the one-way hash function for describing image feature and SHA-256 gives 256-bits hash, i.e., $N = 256$. To encipher the hash in the M-th layer, data is encrypted by Rijndael symmetric encipherment algorithm of AES [20]. The number of layers is two, i.e., $M = 2$. Conditions are summarized in Table 1.

Figure 8(b) shows a tampered image in which the luminance of some portion are different from the original that is shown in Fig. 8(a). The proposed method firstly examines the image in the second layer ($m = M$) in which only one block covers the whole image, $H_m = 1$. This method detects the tamper as shown in Fig. 8(c). Since tamper is perceived in the second layer, the proposed method further examines lower layers. In the first layer, it detects and localizes tamper as shown in Fig. 8(d). The proposed method, therefore, further examines lower layers but only four blocks that are subordinate to the block labeled as tampered in the first layer. The tampered areas are localized in the 0th layer as shown in Fig. 8(e). The proposed method detects and localizes the tampered areas through coarse-to-fine localization by hierarchical data hiding.

(a) Airplane.

(b) Lena.

(c) Peppers.

(d) Sailboat.

(e) Tiffany.

Fig. 7 512×512-sized grayscale images for evaluation from CIPR-RPI [18].

Table 1 Conditions.

(a) Fundamental conditions.

Image size $X \times Y$	512×512 [pixels]
Image feature descriptor	SHA-256 [19]
Description length N	256 [bits]
Cipher algorithm	AES [20]
Number of layers M	2

(b) Layer condition.

Layer m	Block size $X_m \times Y_m$ [pixels]	# of blocks H_m	Payload NH_m [bits]
2	512×512	1	256
1	256×256	4	1024
0	128×128	16	4096

(a) Original image.

(b) Tampered image.

(c) Tamper is detected in the second layer.

(d) Localized tampered area in the first layer.

(e) Localized tampered area in the 0th layer.

Fig. 8 Results of tamper detection in each layer to hierarchical condition.

4.2 Efficiency of Tamper Localization

This section compares the costs for integrity verification between the proposed method and the multi-tier data hiding based conventional method [16] which both methods are based on the same reversible data hiding scheme [12].

Table 2 Conditions for the tamper localization in terms of 64×64-sized block.

(a) Proposed method (the number of layers $M = 3$).

Layer m	Block size $X_m \times Y_m$ [pixels]	# of blocks H_m
3	512×512	1
2	256×256	4
1	128×128	16
0	64×64	64

(b) Conventional method [16] (the number of tiers is 2).

Tier θ	Block size $X_\theta \times Y_\theta$	# of blocks H_θ
1	—	25†
0	128×128	16

† Consisting of nine of 128×128-size blocks, six of 128×64-sized blocks, six of 64×128-sized blocks, and four of 64×64-sized blocks.

Under the condition that a tampered area is localized as a block with 64×64 pixels, the proposed method makes four layers for an image with 512×512 pixels as shown in Table 2(a). While the conventional method makes two tiers for the image as shown in Table 2(b).

The conventional method firstly examines all 25 blocks in the top tier, while the proposed method firstly examines whether the image is tampered by verification of only one block in the top layer. If the image to be examined is genuine, both methods require no more integrity verification. Here, the cost for integrity verification for a block is represented by C, then the total verification cost for a genuine image of the conventional method, $C_{\text{conv,genuine}}$, is up to

$$C_{\text{conv,genuine}} = 25C. \tag{13}$$

Whereas, the total verification cost for a genuine image of the proposed method, $C_{\text{prop,genuine}}$, is small as

$$C_{\text{prop,genuine}} = C. \tag{14}$$

From these two equations, it is clear that the proposed method is superior in the verification cost than the conventional method [16].

If one 64×64-sized block contains tampered area, the proposed method firstly detects tamper in the top layer. Then, it localizes tampered are progressively by coarse-to-fine localization. That is, integrity verification are applied to four blocks in the second, third, and fourth layers. Therefore, the total verification cost for an one block tampered image of the proposed method, $C_{\text{prop,tampered}}$, is given as

$$C_{\text{prop,tampered}} = 13C. \tag{15}$$

While the conventional method firstly localizes a tampered area in the top tier by examining 25 blocks, and four blocks that are overlapped with the block labeled as tampered in the top layer are examined in the second layer. Thus, the total verification cost for an one block tampered image of the conventional method, $C_{\text{prop,tampered}}$, is up to

$$C_{\text{prop,tampered}} = 29C. \tag{16}$$

From these two equations, it is clear that the proposed method reduces the verification cost as compared to the conventional method [16].

5. Further Discussion

The hidden data extraction and image recovery algorithm in the proposed method requires parameter s_m for the m-th layer in each image. That is, s_m is image- and layer-dependent parameter. This section discusses the improvement of this inconvenience to make the proposed method more practical. That is, the parameter unification and the introduction of the default parameter.

Table 3 shows that parameters s_m's for five images shown in Fig. 7 under the condition listed in Table 1. That is, hierarchical data hiding with three layers in which one 512×512-sized block in the top layer, four 256×256-sized blocks in the second layer, and 16 128×128-sized blocks in the third layer.

The first and easy approach of improvement is unifying different s_m's to the single parameter for the image. For "Airplane," 10 can be chosen as the single parameter according to Table 3. This unification, however, still requires to memorize the unified parameter as an image-dependent parameter.

Thus, the second approach introduces the concept of the default parameter to the proposed method. By this concept, it no longer requires to memorize either layer- and image-dependent parameters for images that the default parameter is suited. For example, 6 can be a candidate of the default parameter for several images, including images shown in Fig. 7, based on an investigation shown in Table 3. Other images may require layer- and image-dependent parameter rather than the default parameter for guaranteeing the capacity.

For such images, two ways to overcome this inconvenience exist, except for employing a reversible data hiding scheme having large capacity [21]. One is hiding the value used as the parameter to the upper layer by an arbitrary reversible data hiding scheme. It is an easy way, but the hidden value could be changed by an image tampering, and it could lead a misjudgment in tamper detection. The other way is transmitting a stego image and its corredponding parameter simultaneously, but through different channels and/or media. This way requires extra communication costs, the value is never damaged by an image tampering, and tamper detection works properly.

Table 3 Parameters s_m's for layers in images.

Image	s_0	s_1	s_2
Airplane	23	32	10
Lena	31	15	56
Peppers	24	10	7
Sailboat	67	14	6
Tiffany	18	18	49

6. Conclusions

This paper has proposed a reversible image authentication that detects tamper and localizes tampered area efficiently. The proposed method 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 employment of the reversible data hiding scheme that does not use highly-costed compression technique.

Acknowledgment

This work has been partly supported by the Grant-in-Aid for Young Scientists (B), No.17700119, from the Ministry of Education, Culture, Sports, Science and Technology of Japan.

References

[1] B. Schneier, Applied Cryptography — Protocols, Algorithms, and Source Code in C, 2nd ed., John Wiley & Sons, New York, NY, 1996.
[2] R. Gennaro and P. Rohatgi, "How to sign digital streams," Proc. IACR Annual Int. Cryptology Conf., pp.180–197, Santa Barbara, CA, the U.S., Aug. 1997.
[3] M. Schneider and S.F. Chang, "A robust content based digital signature for image authentication," Proc. IEEE Int. Conf. Image Process., vol.3, pp.227–230, Switzerland, Sept. 1996.
[4] P.W. Wong, "A public key watermark for image verification and authentication," Proc. IEEE Int. Conf. Image Process., vol.1, pp.425–429, Chicago, IL, the U.S., Oct. 1998.
[5] C.Y. Lin and S.F. Chang, "Semi-fragile watermarking for authenticating JPEG visual content," Proc. SPIE, vol.3971, pp.140–151, San Jose, CA, the U.S., Jan. 2000.
[6] Q. Sun and S.F. Chang, "Semi-fragile image authentication using generic wavelet domain features and ECC," Proc. IEEE Inf. Conf. Image Process., vol.2, pp.901–904, New York, NY, the U.S., Sept. 2002.
[7] J. Fridrich, "Security of fragile authentication watermarks with localization," Proc. SPIE, vol.4675, pp.691–700, San Jose, CA, the U.S., Jan. 2002.
[8] J. Wu, B.B. Zhu, S. Li, and F. Lin, "A secure image authentication algorithm with pixel-level tamper localization," Proc. IEEE Int. Conf. on Image Process., vol.3, pp.1573–1576, Singapore, Oct. 2004.
[9] J. Fridrich, M. Goljan, and R. Du, "Lossless data embedding — New paradigm in digital watermarking," EURASIP J. Applied Signal Process., vol.2002, no.2, pp.185–196, Feb. 2002.
[10] J. Tian, "Reversible data embedding using a difference expansion," IEEE Trans. Circuits Syst. Video Technol., vol.13, no.8, pp.890–896, Aug. 2003.
[11] M.U. Celik, G. Sharma, A.M. Tekalp, and E. Saber, "Lossless generalized-LSB data embedding," IEEE Trans. Image Process., vol.14, no.2, pp.253–266, Feb. 2005.
[12] H.L. Jin, M. Fujiyoshi, and H. Kiya, "Lossless data hiding in the spatial domain for high quality images," IEICE Trans. Fundamentals, vol.E90-A, no.4, pp.771–777, April 2007.
[13] J. Fridrich, M. Goljan, and R. Du, "Invertible authentication," Proc. SPIE, vol.3971, pp.197–208, San Jose, CA, the U.S., Jan. 2001.
[14] M.U. Celik, G. Sharma, E. Saber, and A.M. Tekalp, "Lossless watermarking for image authentication: A new framework and an implementation," IEEE Trans. Image Process., vol.15, no.4, pp.1042–1049, April 2006.

[15] S. Han, H.L. Jin, M. Fujiyoshi, and H. Kiya, "Lossless data hiding in the spatial domain for image tamper detection," Proc. IEEE Int. Sympo. Intelligent Signal Process. and Comm. Sys., pp.760–763, Yonago, Japan, Dec. 2006.
[16] S. Han, H.L. Jin, M. Fujiyoshi, and H. Kiya, "Image tamper detection based on multi-tier marks using invertible data hiding," IEICE Technical Report, SIP2007-10, April 2007.
[17] S. Han, H.L. Jin, M. Fujiyoshi, and H. Kiya, "Applying cipher to the reversible image authentication," Proc. Fundamentals Conf. IEICE 2007, no.A-4-2, Sept. 2007.
[18] "Still images and sequences," Center for Image Processing, Renesselaer Polytechnic Institute. [Online]. Available: http://www.cipr.rpi.edu
[19] "Secure hash standard," NIST FIPS 180-2, Aug. 2002. [Online]. Available: http://csrc.nist.gov/publications/fips/fips180-2/fips180-2withchangenotice.pdf
[20] "Advanced encryption standard," NIST FIPS 197, Nov. 2001. [Online]. Available: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
[21] H.L. Jin, M. Fujiyoshi, and H. Kiya, "Improvement in the image quality and the capacity of the reversible data hiding," Proc. Int. Tech. Conf. Circuits/Sys., Comp. and Comm., vol.1, pp.135–136, Busan, Korea, July 2007.

Seungwu Han received his B.Eng. degree from Tongmyong University of Information Technology, Korea in 2003, and his M.Sci. degree from Pukyong National University, Korea in 2005. Since 2006, he has been a Ph.D. candidate at Tokyo Metropolitan University, Japan. His research interests include image processing and security for multimedia.

Masaaki Fujiyoshi received his B.Arts, M.Eng., and Ph.D. degrees from Saitama University, Japan in 1995, 1997, and 2001, respectively. In 2001, he joined Tokyo Metropolitan University, Japan, where he is currently an Assistant Professor of Information and Communication Systems Engineering, Faculty of System Design. His research interests include image processing, secure communications, and spread spectrum communications. Dr. Fujiyoshi served as an Associate Editor for the J. IEICE from 2005 to 2007. He has been an Assistant Secretary of the Smart Infomedia Systems Committee of the IEICE from 2007. He is a Member of the ITE (Institute of Image Information and Television Engineers, Japan) and the IEEE. He received the Young Engineer Award from the IEICE in 2001.

Hitoshi Kiya received his B.Eng. and M.Eng. degrees from Nagaoka University of Technology, Japan in 1980 and 1982, respectively, and his D.Eng. degree from Tokyo Metropolitan University, Japan in 1987. In 1982, he joined Tokyo metropolitan University, where he is currently a Professor of Information and Communication Systems Engineering, Faculty of System Design. He was a Visiting Fellow at the University of Sydney, Australia from Oct. 1995 to March 1996. His research interests include digital signal processing, multirate systems, adaptive filtering, image processing and security for multimedia. Prof. Kiya served as an associate editor for the IEICE Trans. Fundamentals (Japanese Edition) and the IEEE Trans. Signal Processing from 1998 to 2002 and from 1998 to 2000, respectively. He has been the chair of the Signal Processing Committee of the IEICE from 2007 and was the chair of the Media Engineering Committee of the ITE (Institute of Image Information and Television Engineers, Japan) from 2005 to 2007. He is a Member of the ITE and the IIEEJ (Institute of Image Electronics Engineers of Japan), and a Senior Member of the IEEE.