2009 Fifth International Conference on Information Assurance and Security

Reversible Information Hiding Considering Hierarchical Access Control

Masaaki FUJIYOSHI, Seungwu HAN*, and Hitoshi KIYA
Dept. of Information and Communication Systems Engineering, Tokyo Metropolitan University
Hino-shi, Tokyo 191–0065, Japan
Email: mfujiyoshi@ieee.org, kiya@eei.metro-u.ac.jp

Abstract

This paper proposes a reversible information hiding for supporting hierarchical control of access to embedded data. The proposed method firstly hides the most important information to an image by the reversible manner in which information is enciphered. To a stego image to which once information is hidden, this method embeds different information that is enciphered with a different key. In the proposed method, only one key corresponding to the most important data is managed, and other keys are generated from the managed key through a one-way hash function. The privileged user receives the managed key and he/she extracts and deciphers all hidden data, whereas the unprivileged user receives a key that for the least important data. The proposed method also has tamper detection ability. Simulation results show the effectiveness of the proposed method.

1. Introduction

Information hiding technology has been diligently studied, for not only security-relate problems [1], [2], in particular, intellectual property rights protection of digital contents [3], but also non security-oriented [4]. A information hiding technique embeds data into a target signal referred to as the *original* signal. It, then, generates a slightly distorted signal that is referred to as a *stego* signal. Many of information hiding techniques extract hidden data but leave a stego signal as it is [5].

In military and medical applications, restoration of the original signal as well as extraction hidden data are desired [6], [7]. *Reversible* information hiding techniques that restore the original image have been proposed [6]–[15]. Several methods hide different information to an image multiple times for improving capacity [13] and efficient tamper detection [14], [15]. This paper also proposes a reversible information hiding method that hides different information to an image multiple times, but for hierarchical access control to information.

Hierarchical access control techniques have been studied to protect hierarchically scalable content such as JPEG 2000 coded image [16], [17], MPEG-4 fine granularity scalability coded video [16], and multimedia composite content [18]. In these methods, the privileged user is allowed to access full component of the content, whereas the unprivileged user can access the absolute minimal component of the content.

This paper proposes a reversible information hiding method that serves hierarchical access control to hidden information. A stego image generated by the proposed method conveys multiple information in itself, and accessing hidden information is controlled according to its importance and the right of users given by position or payment. Only one key is managed in the proposed method for access control, and keys to be delivered to users are generated from the managed key.

2. Reversible Information Hiding

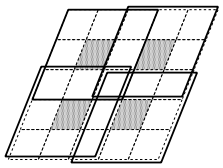
This section briefly mentions the reversible information hiding algorithm that is used in this paper.

Several information hiding methods have been proposed [6]–[12]. Though bijective transformation-based [6], compression-based [7], [8], difference expansion-based [9], [10], and histogram shifting-based [11] exist, this paper focuses the method that memorizes neither location map nor parameter for fixed length data [12]. To save the space, the algorithm based on the focused method is briefly mentioned.

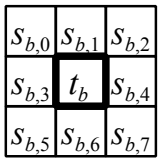
The algorithm used in this paper divides an original image to 3×3-sized overlapping blocks as shown in Fig. 1 (a). In b-th block where $b = 0, 1, \ldots, B$, a data bit is hidden to center pixel t_b using a modulo arithmetic-

The author is currently with Dept. of Computer Engineering, Sejong University, Seoul, Korea.

978-0-7695-3744-3/09 $25.00 © 2009 IEEE
DOI 10.1109/IAS.2009.116

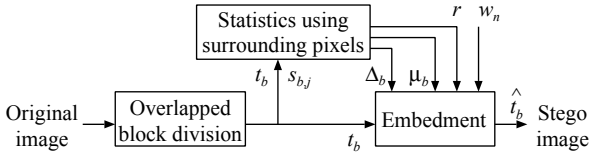


(a) Placement of blocks.

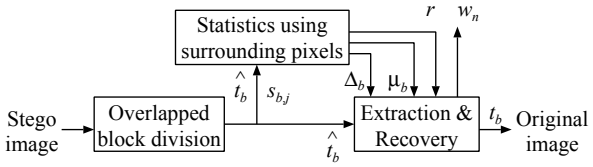


(b) A block.

Figure 1. Blocks for reversible information hiding based on the focused method [12].



(a) Data hiding.



(b) Hidden data extraction and image recovery.

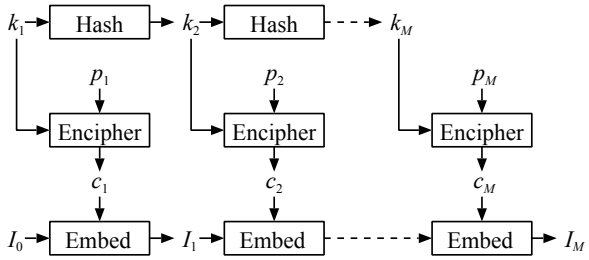
Figure 2. Reversible information hiding based on the focused method [12].

based equation and surrounding pixels $s_{b,j}$ where $j = 0,1,\ldots,7$ remain those original state (Fig. 1 (b)).

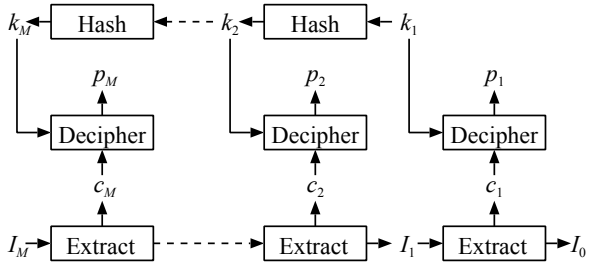
To distinguish whether t_b is able to convey hidden data bit w_n without loss of reversibility, i.e., t_b is usable, this algorithm uses single parameter r that is derived based on statistics of blocks such as μ_b, the average of $s_{b,j}$, and Δ_b, the difference between the maximum (or minimum) of $s_{b,j}$ and μ_b (Fig. 2). According to parameter r, this algorithm hides data bits to usable t_b's and remain unusable t_b's as is.

Though above mentioned strategy generally requires memorization of location map that indicates the pixel positions in which data are hidden, this algorithm estimates parameter r from a stego image that the image conveys hidden data. Therefore, this algorithm does not memorize any location map or parameter.

Furthermore, this algorithm is able to improve the capacity, the number of usable t_b's, by changing the size and shape of blocks and/or embedding equation [19], by applying reversible pre-process that changes statistics of blocks [20], and by increasing the data hiding density per block [21].



(a) Embedding.



(b) Extraction.

Figure 3. Proposed method (the depth of hierarchy is M).

3. Proposed Method

This section proposes a reversible information hiding method that is capable of hierarchical access control for embedded data. Figure 3 shows the system diagram of the proposed method.

In Fig. 3, an original image is I_0. Keys k_m's ($m = 1,2,\ldots,M$) are used to encipher M of plaintext information p_m's. The most important information that is accessible by only the privileged user is p_1, whereas p_M is the least important information that is opened to even the unprivileged user.

3.1. Embedding Algorithm

This section describes the algorithm to hide M of different information with different importance, $p_1, p_2, \ldots, p_m, \ldots, p_M$, into original image I_0 to form stego image I_M.

1) $m := 1$.
2) Encipher m-th most important plaintext information p_m by a certain cipher algorithm, $E()$, with L-length m-th key k_m to generate ciphertext information c_m, i.e., $c_m = E(p_m, k_m)$.
3) Embed c_m to image I_{m-1} by the reversible data hiding algorithm mentioned in Sect. 2 to form stego image I_m.
4) Apply certain one-way hash function $H()$ that outputs L-length hash to k_m to generate k_{m+1}, i.e., $k_{m+1} = H(k_m)$.

5) $m := m+1$. Continue to Step 2 unless $m > M$.

This algorithm generates stego image I_M that conveys M of different information. It is noted that all keys k_m $(m = 1,\ldots,M)$ have the identical length L.

3.2. Extraction Algorithm

This section describes the extraction algorithm under the condition a user receives L-length key k_μ to access $(M-\mu+1)$ of less important information among M of different information.

1) $m := \mu$.
2) Apply one-way hash function $H()$ to k_m to generate k_{m+1}, i.e., $k_{m+1} = H(k_m)$.
3) $m := m+1$. Continue to Step 2 unless $m > M$.
4) Extract m-th ciphertext c_m and recover image I_{m-1} from stego image I_m by the reversible data hiding algorithm mentioned in Sect. 2.
5) Decipher c_m by decipher algorithm $D()$, corresponding to encipher algorithm $E()$, with key k_m to obtain plaintext information p_m, i.e., $c_m = D(c_m, k_m)$.
6) $m := m-1$. Continue to Step 4 unless $m < \mu$.
7) Extract m-th cipertext c_m and recover image I_{m-1} from stego image I_m by the reversible data hiding algorithm.
8) $m := m-1$. Continue to Step 7 unless $m = 0$.

By this algorithm, the user who receives k_μ can access $(M-\mu+1)$ of less important information $p_M, p_{M-1}, \ldots, p_\mu$ and original image I_0.

Moreover, if any p_m is meaningless information, users can find stego image I_M is tampered.

3.3. Features

This section focuses the most important feature of the proposed method, namely, the hierarchical access controllability.

As described in Sect. 3.1, the proposed method cascadingly hides different information to one image in the order according to the importance of information. Since the proposed method utilizes the reversible information hiding scheme, a set of hidden data extraction and image recovery takes a user back to the previous stage of data hiding transition as described in Sect. 3.2. This enables that the least important information p_M opened to all hierarchy is firstly extracted, whereas the extraction of the most important information p_1 for the privileged user is the last. That is, accessing to the most important information is the hardest among all information by hiding strategy.

(a) I_1. PSNR: 60.65 dB (b) I_2. PSNR: 54.09 dB

Figure 4. Stego images (depth of hierarchy $M = 2$, ciphertext c_m are 2048-bits long).

Moreover, each information to be hidden, p_m, is enciphered with the corresponding key, k_m, i.e., different keys are assigned to different information, as described in Sect. 3.1. A user, therefore, is required keys $k_M, k_{M-1}, \ldots, k_\mu$ to access $(M-\mu+1)$ of least important information $p_M, p_{M-1}, \ldots, p_\mu$ in addition to extract ciphertext information $c_M, c_{M-1}, \ldots, c_\mu$ from stego images $I_M, I_{M-1}, \ldots, c_\mu$ as described in Sect. 3.2. In the proposed method, all L-length keys are subordinately generated from one managed key by L-length one-way hash function $H()$, where

$$k_M = H(k_{M-1}) = H^2(k_{M-2}) = H^{M-1}(k_1). \quad (1)$$

Thanks to $H()$, a user who receives key k_μ obtains $(M-\mu+1)$ of keys $k_\mu, k_{\mu+1}, \ldots, k_M$ but cannot obtain $(\mu-1)$ of keys $k_{\mu-1}, k_{\mu-2}, \ldots, k_1$. That is, this user cannot access $(\mu-1)$ of more important information, $p_1, p_2, \ldots, p_{\mu-1}$, beyond his/her right.

With these two properties, the proposed method can serve hierarchical access controllable reversible information hiding.

It is noteworthy that the cascading key generation using a one-way hash function [17] needs to manage only one key and to deliver only one key to a user, even M different keys are required as mentioned above. Consequently, this key generation mechanism simultaneously reduces the cost for managing keys and for delivery keys.

4. Experimental Results

Though any arbitrary one-way hash function and any arbitrary cipher algorithm can be used in the proposed method, this paper uses SHA-256 [22] and blowfish [23] as the hash function and the cipher algorithm, respectively.

Figure 4 shows stego images I_1 and I_2 for 8-bits grayscale image "lena," where depth of hierarchy $M =$

2. Ciphertext c_m consists of 2048 bits in each depth. It is confirmed that accessing plaintext information is limited by keys, but all user who receives a key can access the least important information and the original image.

5. Conclusions

This paper has proposed a reversible information hiding method that is capable of hierarchical control of access to hidden data. The proposed method hides data multiple times in which each hidden data are different and are enciphered with different keys. This method manages only one key and the other keys are subordinately generated from the managed key by a one-way hash function. These two features makes the proposed method be capable to hierarchical access control. The proposed method also serve image tamper detection.

References

[1] M. Barni, F. Pérez-González, M.L. Miller, F. Bartolini, J.J. Eggers, I.J. Cox, P. Moulin, N. Memon, and T. Kalker, "What is the future for watermarking? (Part I)," *IEEE Signal Process. Mag.*, vol.20, no.5, pp.55–59, 2003.

[2] R. Samtani, "Ongoing innovation in digital watermarking," *IEEE Computer*, vol.42, no.3, pp.92–94, Mar. 2009.

[3] H. Berghel and L. O'Gorman, "Protecting ownership rights through digital watermarking," *IEEE Computer*, vol.29, no.7, pp.101–103, July 1996.

[4] M. Barni, F. Pérez-González, M.L. Miller, F. Bartolini, J.J. Eggers, I.J. Cox, P. Moulin, N. Memon, and T. Kalker, "What is the future for watermarking? (Part II)," *IEEE Signal Process. Mag.*, vol.20, no.6, pp.53–59, 2003.

[5] M. Fujiyoshi, Y. Seki, H. Kobayashi, and H. Kiya, "Modulo arithmetic-based image watermarking and its theoretical analysis of image-quality," in *Proc. IEEE ICIP*, 2005, pp.I-969–I-972.

[6] C. De Vleeschouwer, J.-F. Delaigle, and B. Macq, "Circular interpretation of bijective transformations in lossless watermarking for media asset management," *IEEE Trans. Multimedia*, vol.5, pp.97–105, Mar. 2003.

[7] M.U. Celik, G. Sharma, A.M. Tekalp, and E. Saber, "Lossless generalized-LSB data embedding," *IEEE Trans. Image Process.*, vol.14, pp.253–266, Feb. 2005.

[8] J. Fridrich, M. Goljan, and R. Du, "Lossless data embedding — new paradigm in digital watermarking," *EURASIP J. Applied Signal Process.*, vol.2002, pp.185–196, Feb. 2002.

[9] J. Tian, "Reversible data embedding using a difference expansion," *IEEE Trans. Circuit Syst. Video Technol.*, vol.13, pp.890–896, Aug. 2003.

[10] H.J. Kim, V. Sachnev, Y.Q. Shi, J. Nam, and H.-G. Choo, "A novel difference expansion transform for reversible data embedding," *IEEE Trans. Inf. Forensics Security*, vol.3, pp.456–465, Sep. 2008.

[11] Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," *IEEE Trans. Circuit Syst. Video Technol.*, vol.16, pp.354–362, Mar. 2006.

[12] S. Han, M. Fujiyoshi, and H. Kiya, "A reversible image authentication method free from location map and parameter memorization," in *Proc. IWAIT*, 2009.

[13] S. Weng, Y. Zhao, J.-S. Pan, and R. Ni, "A novel reversible watermarking based on an integer transform," in *Proc. IEEE ICIP*, 2007, pp.III-241–III-244.

[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, pp.1042–1049, Apr. 2006.

[15] S. Han, M. Fujiyoshi, and H. Kiya, "An efficient reversible image authentication method," *IEICE Trans. Fundamentals*, vol.E91-A, pp.1907–1914, Aug. 2008.

[16] B.B. Zhu, M.D. Swanson, and S. Li, "Encryption and authentication for scalable multimedia: current state of the art and challenges," in *Proc. SPIE*, vol.5601, 2004, pp.157–170.

[17] Y. Wu, D. Ma, and R.H. Deng, "Progressive protection of JPEG 2000 codestreams," in *Proc. IEEE ICIP*, 2004, pp.3447–3450.

[18] M. Fujiyoshi, S. Imaizumi, and H. Kiya, "Encryption of composite multimedia contents for access control," *IEICE Trans. Fundamentals*, vol.E90-A, pp.590–596, Mar. 2007.

[19] M. Fujiyoshi, S. Sato, H.L. Jin, and H. Kiya, "A location-map free reversible data hiding method using block-based single parameter," in *Proc. IEEE ICIP*, 2007, pp.III-257–III-260.

[20] H.L. Jin, M. Fujiyoshi, and H. Kiya, "On improvement of the reversible data hiding method by reversibly adaptive modulation of statistics," *IEICE Trans. Fundamentals*, vol.J91-A, pp.823–827, Aug. 2008.

[21] M. Ono, M. Fujiyoshi, and H. Kiya, "Image quality improvement of the reversible data hiding method based on high-density embedding," in *Proc. IEICE ESS Soc. Conf.*, 2008, p.64.

[22] "Secure hash standard," NIST FIPS 180-2, Aug. 2002, http://csrc.nist.gov/publications/fips/fips180-2/fips180-2withchangenotice.pdf

[23] B. Schneier, "Description of a new variable-length key, 64-bit block cipher," in *Proc. FSE*, 1996, pp.191–204.