International Journal of Smart Home
Vol.7, No.5 (2013), pp.115-124
http://dx.doi.org/10.14257/ijsh.2013.7.5.12

Digital Watermarking for Image Tamper Detection using Block-Wise Technique

Chan-Il Woo[1] and Seung-Dae Lee[2]
[1]*Department of Information and Communication Engineering, Seoil University, Seoul, Korea*
[2]*Department of Electronic Engineering, Namseoul University, Chungnam-do, Korea*
ciwoo@seoil.ac.kr, *seungdae@nsu.ac.kr*

Abstract

Fragile watermarking has the characteristics where the inserted watermark should be easily breakable for a trivial tampering of the image. So, fragile watermarking technique is proposed for the purpose of authentication or tamper detection. In this paper, we propose an efficient image tamper detection method using block-wise technique which is able to detect the tamper locations. In the proposed method, a digital signature is generated from the hash code of the blocks of the final level where the watermark is inserted and the blocks of the upper level where those blocks are included in the image division process and this signature is used as the watermark, which is randomly inserted into selected image blocks. As the result of experiment, the proposed method was confirmed to be able to detect the tampered parts of the image without testing the entire block of the watermarked image.

Keywords: *Fragile Watermarking, Image Authentication, Tamper Detection, Digital Signature*

1. Introduction

Growth of computer and network technology has led to tremendous opportunities for creation and distribution of digital media content. And the digital data is easy to be edited and illegal duplication, and thus the technology to resolve such issues is in demand [1, 2]. The Digital watermarking technique makes use of a data hiding scheme to insert some information in the image [3, 4]. Robust watermarks are useful for copyright and ownership assertion purposes. So, they cannot be easily removed and should resist such as cropping, filtering, etc. Fragile watermarks can be broken easily which means it's not totally immune from various attacks. However because fragile watermarking is very sensitive to any malicious alteration it can be very valuable for the purpose of authentication or tamper detection [5-8]. The digital watermarking can be divided into block-wise and pixel-wise techniques. Block-wise watermarking is dividing the image into specified non overlapping blocks for the purpose of tamper detection [9, 10].

Many fragile watermarking methods are proposed. And the method of inserting watermark by dividing the image into many blocks of small sizes is weak against attacks like cut-and-paste, and thus the methods to resolve such are being proposed [11-14].

In this paper, a method is proposed such that the digital signature generated by the hash code of the blocks at the last level where the watermark is inserted during the image division process and the upper level containing those blocks is used as the watermark, and the private key used in the digital signature is used to select the block location to insert watermark for effective detection of even tiny tampering of the image.

ISSN: 1975-4094 IJSH

2. Watermark Generation

In this paper, in case an intentional tampering or attack such as cut-and-paste is applied to the watermarked image, the following processes are executed to effectively and quickly detect such blocks.

2.1. Image Division for Watermark Generation and Insertion

The least significant bit(LSB) of the original image(256×256) is set to zero and the original image shall be divided into multiple levels as in Figure 1.

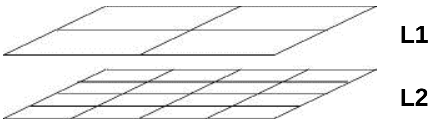


Figure 1. Per-Level Divided Image

In Figure 1, L_1 represents the quadrisection of the original image, and L_2 is the quadrisection of each part of L_1. As such, if the original image is continuously divided, L_3 and L_4 composed of blocks as in Figure 2 (a), (b) can be obtained. In Figure 2, the number in the block represents the block number.

Table 1 shows how four blocks of L_4 are included in one block of L_3. That is, when L_4 and L_3 are placed on top of each other, one L_3 block would fit four L_4 blocks.

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64

(a) L_3 composed of 32×32 pixel blocks

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32

(b) L_4 composed of 16×16 pixel blocks

Figure 2. Image Divided into 32×32 and 16×16 Pixel Blocks

Table 1. L_4 Blocks include in L_3 Blocks

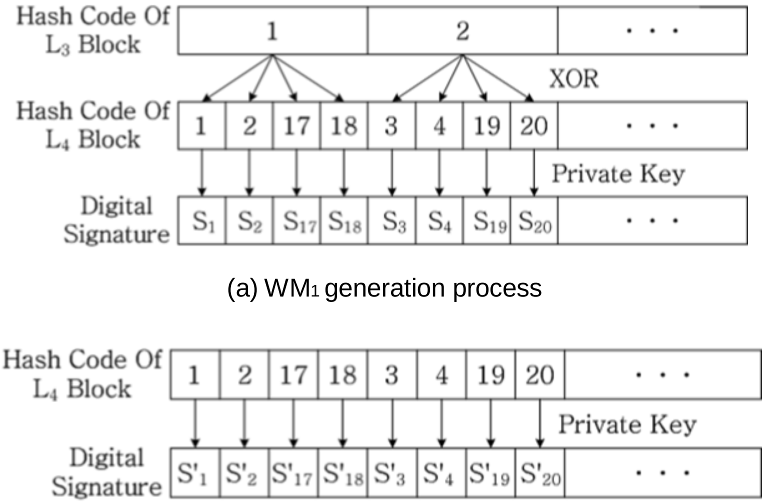
L_3 Block No.	L_4 Block No.
1	1, 2, 17, 18
2	3, 4, 19, 20
3	5, 6, 21, 22
4	7, 8, 23, 24
⋮	⋮

2.2. Watermark Generation

In this paper, two watermarks generated as follows will be inserted to the L_4 blocks divided to the pixel size 16×16.

1) First watermark (WM_1) generation: After performing XOR operation between the hash code for each block of L_3 and the hash code of the L_4 blocks included in this block, the result is enciphered with the private key to generate a digital signature (S_i). Performing such process repeatedly for all L_3 blocks, total of 256 digital signatures are generated, which are called the first watermarks (WM_1).

2) Second watermark (WM_2) generation: With the hash code for each L_4 block, a digital signature (S'_i) is generated. There will be total of 256 digital signatures for all L_4 blocks, and these shall be called the second watermarks (WM_2).



(a) WM_1 generation process

(b) WM_2 generation process

Figure 3. Watermark Generation Process

3) WM_1 and WM_2 generated in 1) and 2) shall each form a pair. The pair of WM_1 and WM_2 shall have S_1 of Figure 3 (a) and S'_1 of (b) form a single watermark pair, and S_2 and S'_2 shall form another pair. Repeating such would result in total of 256 pairs of watermarks.

3. Watermark Insertion and Extraction

3.1. Selection of Block for Watermark Insertion

The selection of block for insertion of watermark pair (WM_1, WM_2) will use the same block mapping equation (1) proposed by Lin et al [9] which uses the randomly selected key, but for the key value of equation (1), the prime number selected with the hash code of the private key in Figure 3 used in the digital signature generation is used to calculate the block to insert watermark.

$$X' = (\text{Key}\times X) \bmod N + 1 \quad (\mathbf{1})$$

Where, X' shows the L_4 block to insert watermark, and X(∈ {1, N}) shows the L_4 block used for watermark generation. And N shows the total number of L_4 blocks.

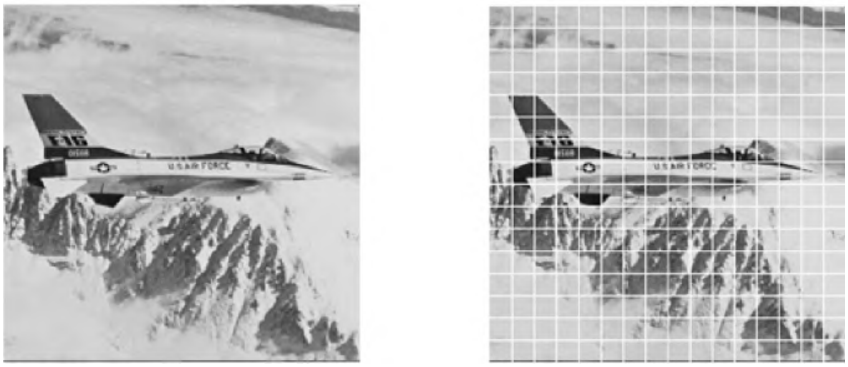
3.2. Watermark Extraction

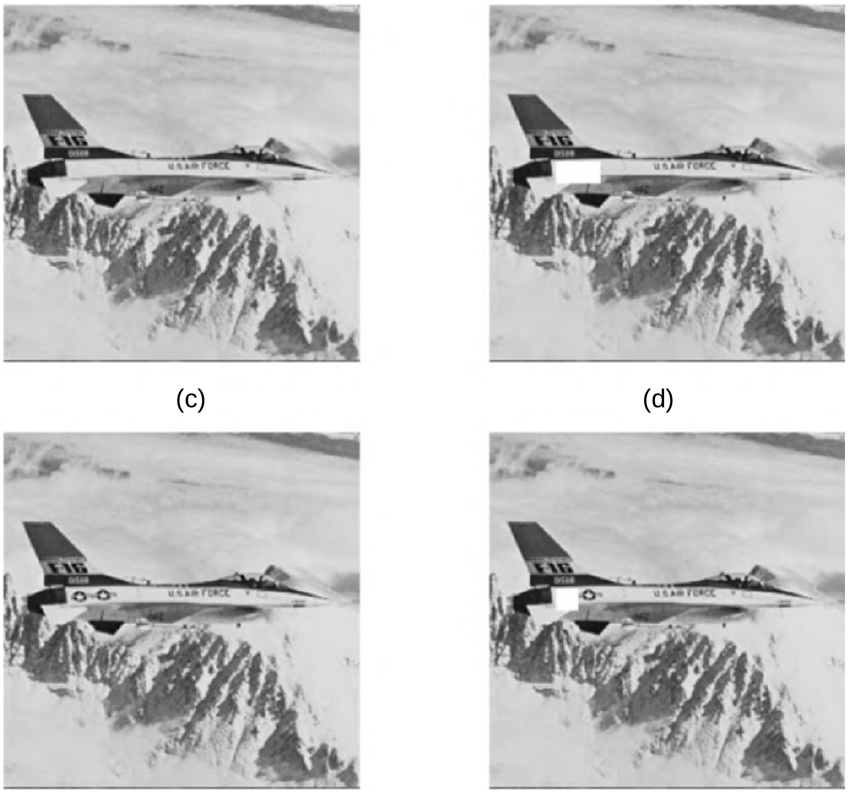
Watermark pairs are inserted to one of the all L_4 blocks. The reason for inserting two watermarks in the LSB of the L_4 block is to detect the tampered locks with minimal number of testing without testing all blocks of L_4 for detecting the presence of tampering in watermarked image, which is determined as follows.

1) The watermark generated as L_3 block 1 consists of 4 pairs as in (S_1, S'_1), (S_2, S'_2), (S_{17}, S'_{17}), (S_{18}, S'_{18}). Such watermark pair is inserted into 4 blocks in the L_4 image, and if the hash code and watermark earned by deciphering the extracted S_1 with the public key is the same as the hash code calculated in the same manner as the watermark generation process in the watermark-inserted image, then L_3 block 1 will be determined to have no tampering, and the three L_4 blocks with S_2, S_{17}, S_{18} inserted will also be determined to have to tampering. This is because S_1, S_2, S_{17}, S_{18} are related to the hash code of L_3 block 1, and due to the characteristics of hash function generating the hash code, the L_4 blocks (1, 2, 17, 18) included in L_3 block 1 are also determined to have no tampering.
2) In case the hash code deciphered with the extracted S_1 as the public key and the hash code calculated for S_1 generation are different, from the blocks inserted with the three watermark pairs of (S_2, S'_2), (S_{17}, S'_{17}), (S_{18}, S'_{18}), watermark pairs are extracted and deciphered for comparing and determining the presence of tampering. In conclusion, S_1, S_2, S_{17}, S_{18} are used as the watermark to determine the presence of tampering in L_3 block and S'_1, S'_2, S'_{17}, S'_{18} are used to determine the presence of tampering in L_4 blocks included in L_3 blocks.

4. Experiment and Result

The method suggested in this paper was experimented against the image of size 256×256.

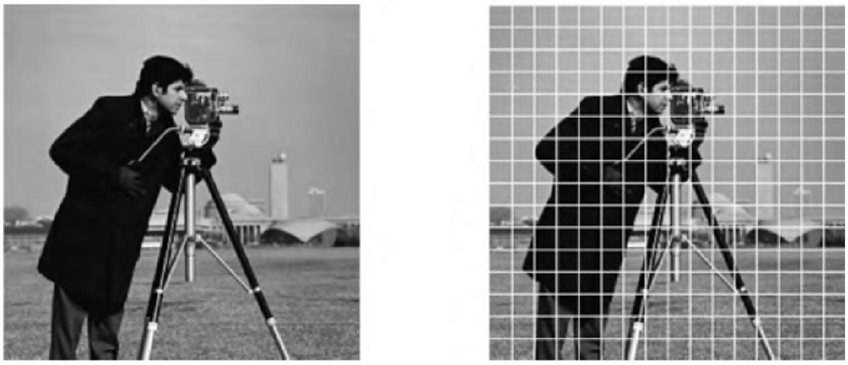

(a) (b)



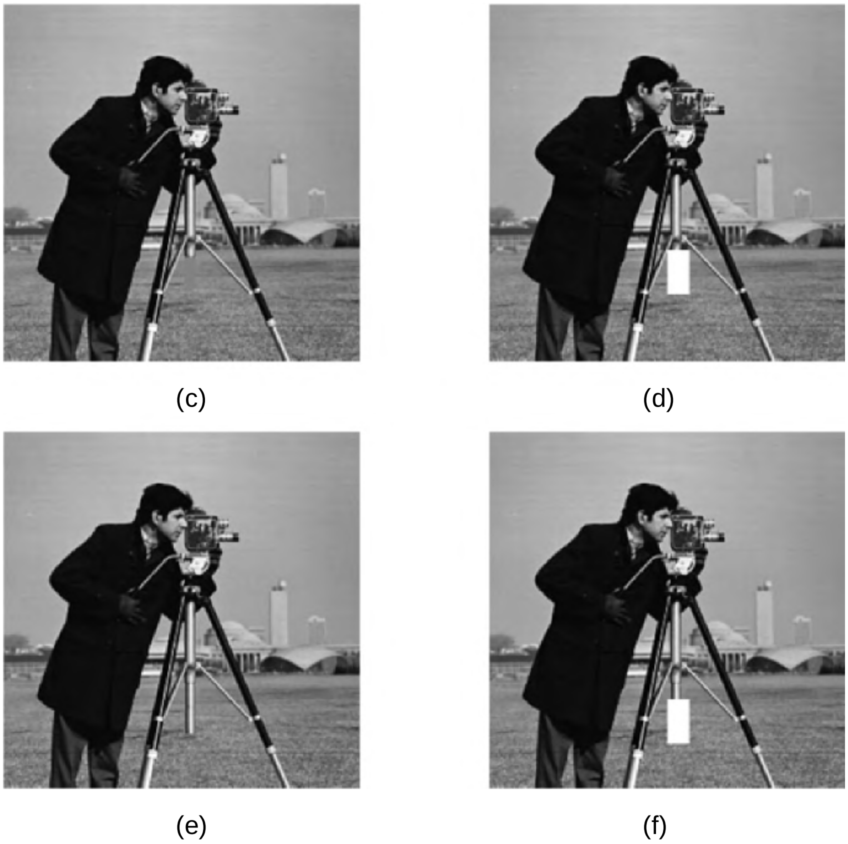
(c) (d)

(e) (f)

Figure 4. (a) The Watermarked Airplane, (b) Image Divided into 16×16 Pixels, (c) Tampered Airplane, (d) Detected Erroneous Regions, (e) Airplane with a Part of the Image Duplicated, (f) Airplane with a Duplicated Part Detected



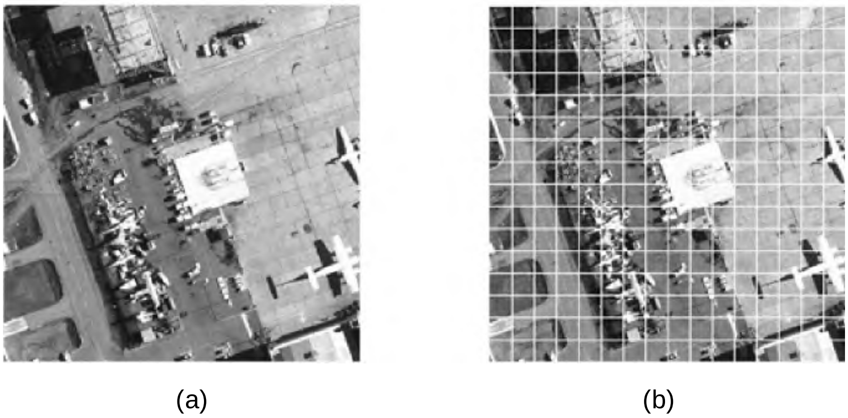
(a) (b)



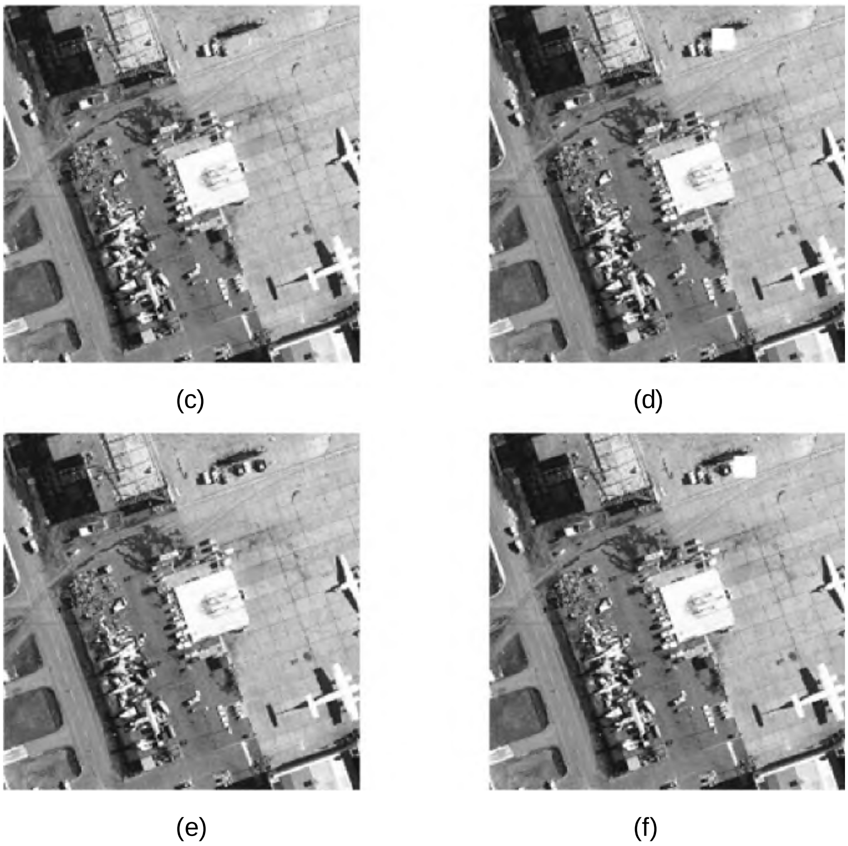
(c) (d)

(e) (f)

Figure 5. (a) The Watermarked Camera, (b) Image Divided into 16×16 Pixels, (c) Tampered Camera, (d) Detected Erroneous Regions, (e) Camera with a Part of the Image Duplicated, (f) Camera with a Duplicated Part Detected



(a) (b)



(c) (d)

(e) (f)

Figure 6. (a) The Watermarked Airfield, (b) Image Divided into 16×16 Pixels, (c) Tampered Airfield, (d) Detected Erroneous Regions, (e) Airfield with a Part of the Image Duplicated, (f) Airfield with a Duplicated Part Detected

Figure 4, 5 and 6 (c) are the image with a part of the watermarked Airplane, Camera and Airfield image deleted, and (e) shows the copy of a part of the watermarked image. Figure 4, 5 and 6 (d) and (f) shows the result of the tampered blocks in (c) and (e) images being detected.

As the result of the experiment, it was confirmed that by testing the hash code of L_3 blocks rather than all blocks of L_4, and testing the L_4 blocks only if there is a discrepancy, the tampered blocks could be detected faster.

5. Conclusion

In this paper, the image block-wise watermarking method was proposed by using digital signature. For the proposed method, it was confirmed that the tampered blocks could be detected faster by testing the hash code of the upper level first without testing all inserted blocks with watermarks inserted. For future research subject, there should be more research on watermark insertion/extraction according to block size.

Acknowledgments

Funding for this paper was provided by Namseoul University.

References

[1] P. Katzenbeisser, “Information Hiding Techniques for Steganography and Digital Watermarking”, Artech House, **(1999)**.

[2] P. W. Wong, “A Public Key Watermark for Image Verification and Authentication”, Proceedings of IEEE International Conference Image Processing, http://www.oifii.org/uag-ird/image-change-detection/igarss/ public-key-watermark.pdf, **(1998)**, pp. 428-429.

[3] B. Surekha and D. N. Swamy, “A Spatial Domain Public Image Watermarking”, International Journal of Security and its Applications, http://www.sersc.org/journals/IJSIA/vol5_no1_ 2011/1.pdf, vol. 5, no. 1, **(2011)**, pp. 1-12.

[4] M. Hussain and M. Hussain, “Information Hiding Using Edge Boundaries of Objects”, International Journal of Security and its Applications, http://www.sersc.org/journals/IJSIA/vol5_ no3_ 2011/1.pdf, vol. 5, no. 3, **(2011)**, pp. 1-10.

[5] M. U. Celik, G. Sharma, A. M. Tekalp and E. Saber, “Localized Lossless Authentication Watermark (LAW)”, Proceeding of SPIE-IS &T Electronic Imaging, http://www.ece.rochester.edu/~gsharma/papers/ei2003Lawpaper.pdf, vol. 5020, **(2003)**, pp. 689-698.

[6] I. J. Cox and J. P. M. G. Linnarts, “Public Watermarks and Resistance to Tampering”, IEEE International Conference Image Processing, http://www.sps.ele.tue.nl/members/J.P.Linnartz/papers/articles/ icip.pdf, vol. 3, **(1997)**.

[7] P. Dong, J. G. Brankov, Y. Yang and F. Davoine, “Digital Watermarking Robust to Geometric Distortions”, IEEE Transaction on Image Processing, http://www.cmlab.csie.ntu.edu.tw/~ipr/ipr2005/ data/material /Digital%20Watermarking%20Robust%20to%20Geometric%20Distortions.pdf, vol. 14, no. 12, **(2005)** pp. 2140-2150.

[8] P. Tsai, Y.-C. Hu, H.-L. Yeh and W.-K. Shih, “Watermarking for Multi-Resolution Image Authentication”, International Journal of Security and its Applications, http://www.sersc.org/journals/IJSIA/vol6_no2_2012/ 18.pdf, vol. 6, no. 2, **(2012)**, pp. 161-166.

[9] S. Dadkhah, A. Abd Manaf and S. Sadeghi, “Efficient Digital Image Authentication and Tamper Localization Technique using 3 LSB Watermarking”, International Journal of Computer Science Issues, http://ijcsi.org/papers/IJCSI-9-1-2-1-8.pdf, vol. 9, no. 2, **(2012)**.

[10] P. L. Lin, C. K. Hsieh and P. W. Huang, “A Hierarchical Digital Watermarking Method for Image Tamper Detection and Recovery”, Pattern Recognition, http://www.sciencedirect.com/science/article/pii/ S0031320305000890, vol. 38, **(2005)**, pp. 2519-2529.

[11] C. C. Chien, K. C. Fan and S. W. Wang, “A Wavelet-Based Public Key Image Authentication Watermarking”, Proceeding of IEEE 37th Annual 2003 International, http://ieeexplore.ieee.org/ stamp/stamp.jsp?arnumber=01297579, **(2003)**, pp. 321-324.

[12] P. W. Wong and N. Memon, “Secret and Public Key Authentication Schemes that Resist Vector Quantization Attack”, Proceeding of SPIE 3971, vol. 75, **(2002)**, pp. 417-427.

[13] M. Holliman and N. Memon, “Counterfeiting Attacks on Oblivious Block-Wise Independent Invisible Watermarking Schemes”, IEEE Transaction on Image Processing, ieeexplore.ieee.org/iel5/83/17937/ 00826780.pdf, vol. 9, no. 3, **(2000)**, pp. 432-441.

[14] A. Singh, S. Tiwari and S. Kumar Singh, “Face Tampering Detection from Single Face Image using Gradient Method”, International Journal of Security and its Applications, http://www.sersc.org/journals/IJSIA/vol7_no1_2013/3.pdf, vol. 7, no. 1, **(2013)**, pp. 17-30.

Authors

Chan-Il Woo received the B.S., M.S., and Ph.D. degree in electronic engineering from Dankook University, Seoul, Korea, in 1993, 1995 and 2003, respectively. From 1995 to 1997, he worked as a researcher at LG Innotek Co., Ltd, Korea. He is an associate professor in the information and communication engineering department at Seoil University, Seoul, Korea. His research interests include information security and digital watermarking.

Seung-Dae Lee Seung-Dae Lee is a professor in the department of electronic engineering at Namseoul University, Chungnam-do in Korea. His research interests focus in wire and wireless communication and information security. He received the B.S., M.S. degree in electronic engineering from Dankook University, and obtained his Ph.D. degree in communication engineering from Dankook University, Seoul, Korea in 1999.