Watermarking for Multi-resolution Image Authentication

Piyu Tsai[1] , Yu-Chen Hu[2], Hsiu-Lien Yeh[3] and Wei-Kuan Shih[3]

[1]Department of Computer Science and Information Engineering
National United University, Miaoli, Taiwan, 36003
[2]Department of Computer Science and Information Management
Providence University, Taichung, Taiwan, 40006
[3]Institute of Information Systems and Applications
National Tsing Hua University, Hsinchu, Taiwan 30013
pytsai@nuu.edu.tw, ychu@pu.edu.tw, {hsiulien,wshih}@cs.nthu.edu.tw

Abstract

Progressive image transmission (PIT) provides multiple image resolutions that favors a time-critical or a low-band channel environment. In this paper, a PIT based watermarking for multi-resolution image authentication is proposed. The image content with progressive characteristic is taken as the authentication code. The authentication code is then embedded according to multi-resolution image encoding. The experimental results show the validity of the proposed scheme. Malicious operations are detected progressively from multi-resolution images. The significant tampering can be detected firstly and slight tampering is detected in the later authentication stages. Furthermore, the tampered locations can be located correctly.

Keywords: *Watermarking, progressive image transmission, image authentication*

1. Introduction

The multimedia digitalization and the Internet popularity promote the digital multimedia distribution. However, the security issues such as modification, interception, forgery, tampering as well as others are becoming more and more important. To deal with these issues, several approaches on how to authenticate digital multimedia are proposed [1, 2].

On the proposed approaches, they have digital signature-based and watermarking-based approaches. Digital signature-based authenticator can preserve the integrity of original multimedia but an extra space is required to store authentication code (AC). Watermarking-based authenticator modifies the multimedia content and extra space is not required [3].

On PIT, images can be reconstructed with multi-resolution. However, the low resolution images should also be authenticated to assure the transmission security. Most of current watermarking-based approach can only authenticate the fully reconstructed images. After all, PIT is useful on a time-critical or a low-band channel environment in which the important information can be transmitted as soon as possible.

A few of multi-resolution image authenticators have been proposed. In Groshois *et al.*'s scheme, each code-block employs hash function to generate a signature and appends to this code-block [3]. The attached signature and a new signature generated from the code-block are compared to authenticate the code-block. In Tsai *et al.*'s scheme, SPIHT encoding stage number is the AC [4]. The AC indicates a rough coefficient magnitude which is used to compare with the currently reconstructed coefficients magnitude to determine the authentication.

In Masmoudi and Bouhlel's scheme [5], the bit-stream of a certain resolution image is hashed and appended as AC. The new extracted AC and the appended AC is compared to determine image authentication. In Steinder *et al.*'s scheme, the wavelet-based and network-conscious concepts are incorporated to develop a blind digital image signature technique [6]. Each multi-resolution image can be authenticated in real time. In Huang *et al*.'s watermarking, the genetic algorithm is applied to DCT domain and JPEG spectral selection mode [7]. In Amiri *et al*.'s watermarking, discrete wavelet transformation (DWT) sub-bands of watermark are embedded into the corresponding DWT sub-bands [8].

In this paper, a multi-resolution images authenticator with a high precision is proposed. The rest of this paper is organized as follows. In Section 2, the proposed scheme is introduced. The experimental results are shown in Section 3. Finally, conclusions are given in Section 4.

2. The Propose Scheme

The proposed scheme extracts the most important image information to take as the AC. The AC is then progressively embedded and extracted to authenticate the multi-resolution images. The authentication code generation, embedding and authentication procedures are involved in this scheme.

2.1. The Authentication Code Generation

To develop an image authenticator, AC is first considered. In the proposed scheme, AC is extracted from the image content which contains the feature to authenticate the multi-resolution images. In addition, AC can be embedded into multi-resolution images. So, the size of the AC should be considered carefully.

On the above considerations, we observed that DWT decomposed the image into multi-levels. The coefficients in different levels hold the tree structure characteristics in which the root nodes preserve the most important energy. So, LL coefficients are selected as the AC.

To embed AC in image with imperceptibility, AC is further scaled. Finally, scaled AC is rearranged into bit planes. The first MSB of each LL coefficient is first embedded and extracted. And then, the second and the third MSB bit planes can be embedded/extracted, respectively. From that, AC can be embedded according to their importance.

An example shown in Table 1 illustrates the proposed AC generation. The scaled AC also indicates to rough coefficient magnitude. For example, the AC valued at 7 shown in Table 1(b) implies the corresponding coefficient magnitude is greater than or equal to 224. Similarly, AC valued at 3 indicates the corresponding magnitude is greater than or equal to 96 and less than 128.

Table 1. Example of Authentication Code Generation

(a) LL Coefficients	(b) Scaled	(c) Binary
168, 190, 231, 30	5, 6, 7, 0	101, 110, 111, 000
195, 69, 80, 150	6, 2, 2, 4	110, 010, 010, 100
188, 82, 42, 110	5, 2, 1, 3	101, 010, 001, 011
157, 87, 36, 130	4, 2, 1, 4	100, 010, 001, 100

2.2 The Embedding Procedure

The embedding procedure inserts the AC bit plane into multi-resolution images according to PIT. Three AC bit planes will be embedded into HH, HL and LH sub-bands, respectively. To carry the authentication bit, each embedding coefficient will be modified. The embedding modification is determined according to the selected embedding bit. In the proposed embedding procedure, one of bits in embedding coefficient will be replaced by the embedded AC bit. To achieve multi-resolution image authentication, the more important AC bit planes are embedded into the earlier encoded bits. Similarly, the less important AC bit plane is inserted into the later encoded bits. After that, the more important authentication bit is embedded into the more important and the earlier encoded bits. Also, it can be extracted earlier to authenticate the earlier reconstructed low resolution images.

Furthermore, to reduce the embedding distortion, a compensation mechanism is incorporated. The compensation mechanism explores the relationship between embedded AC bit and the bits in the embedding coefficient. If the embedding bit (the fifth LSB) will be modified from 0 to 1 to match the AC bit, the first lower bit (the fourth LSB) will be set to 0.

In summary, AC is embedded into the multi-resolution images according to their importance. The low resolution image can be authenticated by the first extracted AC. The compensation mechanism is adopted to reduce the embedding distortion.

2.3 The Authentication Procedure

The authentication procedure is to verify the multi-resolution images integrity. In PIT, the image is reconstructed progressively from low resolution to high resolution. Each reconstructed low resolution image should be verified to assure the integrity. To verify multi-resolution image integrity, the embedded AC will be extracted from the low resolution images.

To authenticate the reconstructed multi-resolution images, the first embedded AC bit plane is extracted from HH coefficients. The embedding bit, which is the same as that of in embedding procedure, is extracted. If the second AC bit plane is not available, only the first AC bit plane is employed to verify the current reconstructed image. The first authentication bit plane implies the estimated coefficient magnitude (*est_mag*). Therefore, the LL coefficient magnitude in current reconstructed image is compared with *est_mag*. For example, the extracted AC bit value of 1 indicates that the *est_mag* is greater than or equal to 128 and bit value of 0 indicates the *est_mag* is less than 128. If the comparison result matches, the current reconstructed image is authenticated. The authentication of the first authentication bit can be formulated as in equation (1).

$$AC\_bit = \begin{cases} 1 & est\_mag \geq 128 \\ 0 & est\_mag < 128 \end{cases} \tag{1}$$

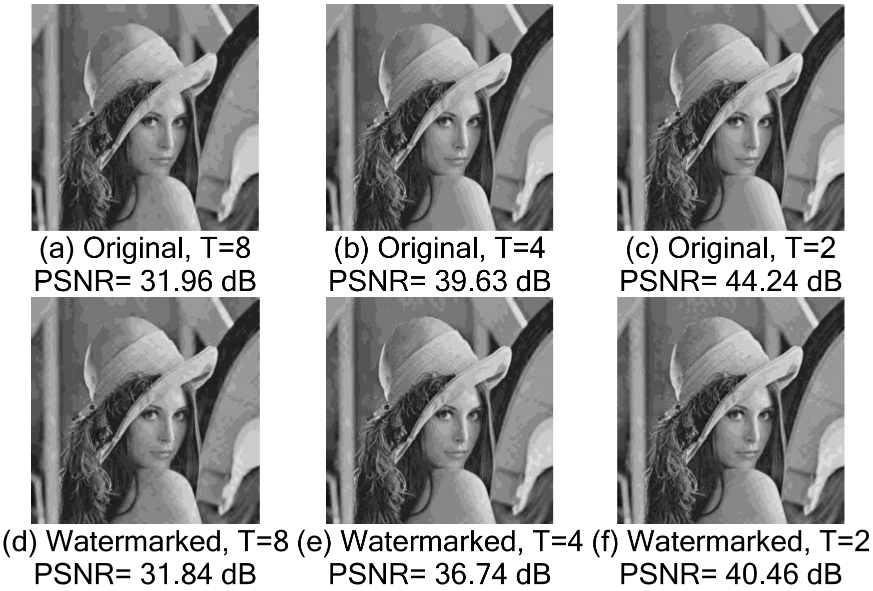
Once the current reconstructed low resolution image is authenticated, detailed image information is received to refine the rough image. When the second AC bit plane is received, the second AC bit plane can be extracted to verify the refined images. Similarly, the embedding bit in HL coefficient is examined to extract the embedded AC bit. Now, the AC is composed of the first and the second AC bit planes. This AC bits indicated *est_mag* will be more precise. For example, two AC bits valued at 3 $(11)_2$ indicates the *est_mag* is greater than or equal to 192, bits value of 2 indicates the *est_mag* is greater than or equal to 128 and less than 192. The coefficient comparison between the currently reconstructed coefficient and the *est_mag* authenticates the currently reconstructed image. The authentication of the first and the second AC bit planes can be formulated as in equation (2).

$$AC\_bits = \begin{cases} 11 & est\_mag \geq 192 \\ 10 & 128 \leq est\_mag < 192 \\ 01 & 64 \leq est\_mag < 128 \\ 00 & est\_mag < 64 \end{cases} \quad (2)$$

If further refine image information is received, the third AC bit plane can be extracted from LH sub-band. Now, all of AC is available and a more precision *est_mag* is indicated. The comparison result determines whether the multi-resolution image is authenticated or not. Since the reconstructed images can be authenticated from low resolution to high resolution, the significant tampering will be detected in low resolution authentication procedure and slight modification will be located in high resolution authentication procedure.

3. Experimental Results

Several simulations were implemented to evaluate the proposed performance. Test gray-level images of 512×512 pixels were taken as the test images. These images were decomposed into four levels by using CDF 9/7 transformation. Then, AC is generated in which the first three MSBs of LL coefficients were extracted. The size of the AC is related to the selected number of coefficients and scales. In this simulation, 1024 LL coefficients and 8 scales were employed and 3072 AC bits will be embedded.



(a) Original, T=8
PSNR= 31.96 dB

(b) Original, T=4
PSNR= 39.63 dB

(c) Original, T=2
PSNR= 44.24 dB

(d) Watermarked, T=8
PSNR= 31.84 dB

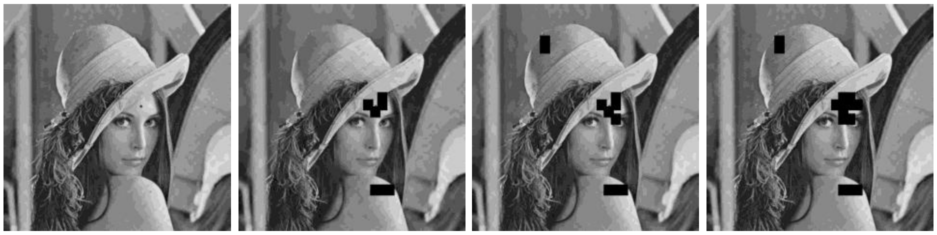
(e) Watermarked, T=4
PSNR= 36.74 dB

(f) Watermarked, T=2
PSNR= 40.46 dB

Figure 1. The Multi-resolution Original and Watermarked Images “Lena”

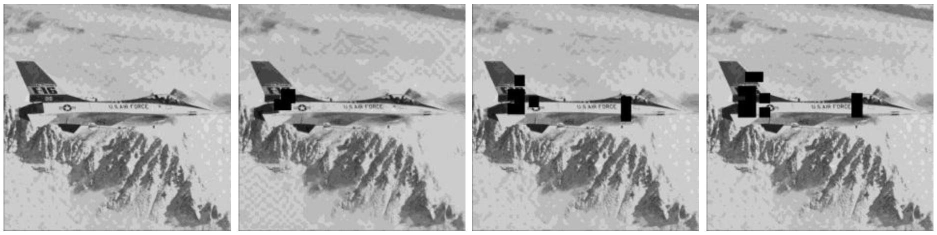
To evaluate the proposed scheme performance, the multi-resolution encoding images and watermarked images were simulated according to PIT. Three AC bit planes were embedded into HH_4, HL_4 and LH_4 sub-bands in encoding thresholds (T) 8, 4 and 2, respectively. The simulation results were shown in Figure 1. By comparing Figures 1(a) and 1(d), it is noted that the embedding distortion is only about 0.12 dB. The embedding distortion is about 2.89 dB and 3.78 dB when the second and third authentication bit planes were embedded, respectively. From Figure 1(f), it indicated that the proposed embedding caused distortion is less and the watermarked image preserves a good imperceptibility.

To authenticate the multi-resolution images, the watermarked image shown in Figure 1(f) was tampered with. The tampered images were shown in Figure 2(a) in which four dots with different contrasts were inserted. The tampered images were reconstructed with different resolutions. Each resolution image was verified and the tampered areas were detected and marked. The authentication results were shown in Figures 2(b-d). From the result, it is shown that the tampered areas were located from different resolution images. Another simulation shown in Figure 3 also demonstrated the same result in which text "F-16" with different contrasts was inserted into three locations and the number 8 in airplane number was removed in Figure 3(a). The tampered areas were detected progressively according to their significance.



(a) Tampered, T= 2 (c) Detected, T= 8 (c) Detected, T= 4 (d) Detected, T= 2

Figure 2. The tampered and detected images "Lena"



(a) Tampered, T= 2 (c) Detected, T= 8 (c) Detected, T= 4 (d) Detected, T= 2

Figure 3. The Tampered and Detected Images "Airplane"

4. Conclusions

In this paper, a watermarking for multi-resolution images authentication is presented. The size of the AC can be determined according to the embedding distortion and the authentication precision. The experimental results show that the reconstructed low and high resolution images can be authenticated according to the extracted AC bits. Furthermore, the significant tampered areas can be detected and located in low resolution images and slight tampered can be located from high resolution images.

Acknowledgements

This research was supported by the National Science Council, Taiwan, R.O.C. under contract NSC 100-2221-E-239-030.

References

[1] C. Y. Lin and S. F. Chang, "A Robust Image Authentication Method Distinguishing JPEG Compression from Malicious Manipulation", IEEE Transactions on Circuits and Systems for Video Technology, **(2001)**, pp. 153-168.

[2] Q. Sun and S. F. Chang, "A Secure and Robust Digital Signature Scheme for JPEG2000 Image Authentication, IEEE Transactions on Multimedia, Vol. 7, **(2005)**, pp. 480-494.

[3] R. Groshois, P. Gerhelot and T. Ehrahimi, "Authentication and Access Control in the JPEG 2000 Compressed Domain", SPIE, **(2001)**, pp. 95-104.

[4] P. Tsai, Y. C. Hu and C. C. Chang, "Using Set Partitioning in Hierarchical Trees to Authenticate Digital Images", Signal Processing: Image Communication, Vol. 18, **(2003)**, pp. 813-822.

[5] A. Masmoudi and M. S. Bouhlel, "A Proposal for Progressive Authentication and Data Integrity of JPEG2000 Codestreams", IEEE International Conference on Information and Communication Technologies. **(2006)**.

[6] M. Steinder, S. Iren and P. D. Amer, "Progressively Authenticated Image Transmission", IEEE International Conference on Military Communications (MILCOM), **(1999)**.

[7] H. C. Huang, J. S. Pan, C. S., Shieh and F. H. Wang, "Progressive Watermarking Techniques with Genetic Algorithms", IEEE International Carnahan Conference on Security Technology, **(2003)**, pp. 62-65.

[8] M. D. Amiri, H. Danyali and Z. A. Bahram, "An Adaptive Robust and Multiresolution Image Watermarking for Progressive Wavelet Image Coding", International Conference on Wireless Communications Networking and Mobile Computing (WiCOM), **(2010)**, pp. 1-4.

Authors

Piyu Tsai received his M.S. degree in computer science in 1990 from Texas A&M University USA and Ph. D. degree in computer science and information engineering in 2003 from National Chung Cheng University, Taiwan. He is currently a professor of the department of computer science and information engineering at National United University, Taiwan. His research interests include multimedia security, data engineering and signal processing.

Chen-Yu Hu received his PhD. degree in computer science and information engineering from National Chung Cheng University, Taiwan in 1999. Currently, Dr. Hu is a professor in the Department of Computer Science and Information Management, Providence University, Taiwan. He servers as the Editor-in-Chief of International Journal of Image Processing since 2009. Also, he is the managing editor of Journal of Information Assurance & Security. His research interests include image and signal processing, data compression, information hiding, and data engineering.

Hsiu-Lien Yeh joined in 2009 for her Ph.D in information security from National Tsing Hua University, Hsinchu, Taiwan. Her research interests include cryptography, information security, multimedia security, information hiding, and image compression.

Wei-Kuan Shih is a Professor at the Department of Computer Science, National Tsing Hua University. He completed his Ph.D. degree at the University of Illinois, Urbana- Champaign. His current research interests include real-time systems, wireless systems, Internet technology, multimedia systems, and information security.