A Watermarking-Based Authentication for Progressive Transmission Images

Piyu Tsai
Department of Computer Science and Information Engineering
National United University, Miaoli, Taiwan 360
pytsai@nuu.edu.tw

ABSTRACT

The image transmission over the Internet with progression is preferable and provided by most of image encoders such as SPIHT, EZW, JPEG 2000, etc. The progressive image transmission benefits the applications such as low-band channel or time-critical in which the transmission can be halted according to the user requirement. However, the received partial image should also be authenticated to ensure the transmission security. In this paper, a watermarking-based authentication scheme for progressive transmission images is proposed. The authentication code is extracted from the image content, which preserves the characteristic for progressive authentication. The authentication code embedding is incorporated to the multi-stage encoding. The embedded authentication code can be extracted progressively to authenticate the current received images. The experimental results show the validity of the proposed progressive images authentication. Furthermore, the size of the proposed authentication code is small, so that, the distortion of watermarked image is less.

1: INTRODUCTIONS

Digital information transmission over the open channel such as Internet always encounters the challenge of communication security. Image authentication scheme is proposed to solve the problem in which the integrity of the received image is authenticated. Several image authentication schemes have been proposed. In these schemes, they can be classified into the digital signature-based and the watermarking-based approaches. The digital signature-based approach attaches the authentication code either in the header of the image file or as an independent file. On the other hand, the watermarking-based approach embeds the authentication code into the image to be transmitted. The watermarking-based approach saves the space for authentication code but pays the degradation of the watermarked image. Generally, the watermarking-based approach is difficult to embed the authentication code and to preserve the image perspective.

Most of image authentication schemes [1-6] focus the authentication to the complete image. In other words, the authentication for the received partial image is not performed until the complete image is received. The complete image authentication restricts the applications of the progressive image transmission. After all, the progressive image transmission is useful on a time-critical or a low-band channel application in which the most important information is earlier transmitted as soon as possible and stopped once the received information is enough.

Few of progressive image authentication schemes [7] have been proposed. In 2003, Tsai *et al*. proposed a digital signature-based authentication based on set partitioning in hierarchical trees (SPIHT). The encoding stage numbers of discrete wavelet transformation (DWT) coefficients during the SPIHT multi-stage encoding are taken as the authentication code. The received partial image during the SPIHT multi-stage decoding can be authenticated according to the comparison result between the authentication code and the received partial image information. This scheme can locate the tampered area and distinguish the accepted operations from incident manipulations. In this scheme, the progressive image authentication is obtained. However, the space for authentication code is always concerned.

To improve the digital signature-based authentication, a watermarking-based authentication for progressive image is proposed in this paper. The authentication code contained the feature to verify the progressive image is extracted and embedded. The received progressive images can be authenticated progressively by the extracted authentication code. The rest of this paper is organized as follows. In Section 2, the proposed image authentication method will be described. Next, the experimental results will be shown in Section 3. Finally, some conclusions will be given in Section 4.

2: THE PROPOSED METHOD

The goal of the proposed method is to authenticate the received partial image that is not restricted to the completed image. Three main procedures: the authentication code generation, the embedding and the authentication procedures are included in this method.

2.1: THE AUTHENTICATION CODE GENERATION

In this procedure, the authentication code is first generated and then embedded into the image to be authenticated. To authenticate the progressive transmission images, the authentication code extracted from the feature of the image has to preserve the progressive information of the image. The authentication code embedding is based on multi-stage encoding/decoding algorithm in which images are transmitted and reconstructed and authenticated progressively.

To obtain the code for progressive image authentication, the DWT coefficients and the multi-stage encoding/decoding algorithm are explored. Three characteristics of the DWT coefficients are employed to generate the authentication code. The first characteristic is the stronger coefficient relationship between three sub-bands (LH: Low-High, HL: High-Low and HH: High-High). This relationship can be found when the image is modified. Any modification to an image will incur the change among three sub-bands. This characteristic indicates that one of three sub-bands can be selected to detect the image modification.

The second characteristic is the tree structure of the sub-band coefficients. The DWT coefficients in a sub-band are structured with multi-levels. The multi-level structure holds the tree characteristic in which a high-level coefficient corresponds to many low-level coefficients. The tree structure characteristic can be found when the modification of an image is occurred. Once the modification of a tree coefficient is detected, the modification at the same tree coefficients can also be found. The tree structure characteristic implies that one of tree levels can be selected to represent the tree.

The third characteristic is the importance of each coefficient. An important coefficient always contains the more important information. It will be early encoded in the multi-stage encoding processing. In DWT coefficient, the larger the coefficient magnitude is, the more important the coefficient will be.

Based on these observations, the authentication code is composed of the high-level tree coefficients from one of three sub-bands. However, the size of the authentication code consists of DWT coefficients is so larger. The smaller size of the authentication code incurs the less modification and the higher perspective to the watermarked image. Therefore, reducing the size of the authentication code is further explored.

To reduce the authentication code size, the selected coefficients from a sub-band are quantized. The coefficient quantization is performed by the exponent operation. For example, a coefficient magnitude 278 will be quantized to 8 (i.e., $2^8 <= 278 < 2^9$). The quantization effectively reduces the authentication size. Furthermore, the multi-stage encoding is also concerned to reduce the authentication code size. In the multi-stage encoding, the main structure of an image is processed in the earlier stages and the refined image information is processed in the last stages. Generally, the information encoded in the earlier stages is not sufficient to identify an image. On the other hand, the refined image information contained the last stages may be discard for most of important information is received. Therefore, only the information encoded in the middle stages is selected as the authentication code. From that, the quantized authentication code is further scaled. An example shown in Table 1 illustrates the authentication code generation. The original DWT coefficients are shown in Table 1(a). The quantized authentication code by using the exponent operation is shown in Table 1(b). The scaled authentication code from Table 1(b) is shown in Table 1(c), in which the quantized values of 0,1and 2 are scaled to zero.

In this paper, the LH4 sub-band coefficients are extracted, quantized and scaled to generate the authentication code. The authentication code also still preserves the rough coefficient magnitude. For example, the authentication code valued at 2 shown in Table 1(c) implies the corresponding coefficient magnitude is greater than or equal to 16. Similarly, authentication code valued at 1 indicates the corresponding magnitude is greater than or equal to 8 and less than 16.

To perform the importance of the authentication code, the most significant bit of the authentication code is first extracted to form a MSB bit plane. And then, the second MSB forms another bit plane. The first and second MSB bit planes of the authentication code shown in Table 1(c) are composed of 1000000000000000 and 00110000000000000, respectively. The first MSB bit plane is more important than the second MSB bit plane. The more important MSB bit plane will be embedded than the second MSB bit plane.

Table 1. Example of the authentication code

26	7	13	10
-7	6	6	4
4	-4	4	-3
1	-2	-2	0

(a) Original

4	2	3	3
2	2	2	2
2	2	2	1
0	1	1	0

(b) Quantized

2	0	1	1
0	0	0	0
0	0	0	0
0	0	0	0

(c) Scaled

2.2: THE EMBEDDING PROCEDURE

Once the authentication code is generated, the embedding procedure based on the multi-stage encoding is performed. In the multi-stage encoding, the significant DWT coefficients will be first encoded according to the thresholds until all of information is encoded. Therefore, the authentication code should be embedded according to the importance of the authentication code and the encoding stages. The authentication code contained the important information

should be embedded in the earlier encoding stages in which the decoded image from the earlier decoding stages can be authenticated.

To achieve the progressive image authentication, the scaled authentication code from quantized coefficients is represented with binary form. The MSB bit plane of the binary authentication code is first embedded and then the second MSB bit plane is followed and so on. The first MSB bit plane of the authentication code carries the most important authentication information. They should be embedded into the coefficients, which are encoded in the earlier encoding stages. According to the importance of coefficient, the coefficients in the Low-Low (LL) sub-band preserve the lager magnitude. In other words, these coefficients are more important and will be encoded in the earlier stages. So, they are selected to carry the first MSB bit plane of the authentication code.

Each LL sub-band coefficient is selected to embed an authentication bit in which one bit of the coefficient (in binary form) is modified to match the embedding bit. For example, the coefficient magnitude is 63 and the embedding bit is 0. The coefficient magnitude is modified from 63 (111111 in binary) to 47 (101111 in binary) to embed the authentication bit in which the fifth LSB is changed from 1 to 0.

Once the first MSB bit plane of the authentication code is embedded, the second MSB bit plane embedding can be performed. To avoid the embedded authentication code is influenced by the followed authentication code embedding, the coefficients in HL4 sub-band are selected to carry the second MSB bit plane. Similarly, one bit of each HL4 sub-band coefficient is modified to embed one authentication bit. However, the location of the embedding bit in HL4 sub-band is lower than that of in LL sub-band. This is because the lower bits are generally encoded in the latter encoding stages. For example, the second MSB bit plane of the authentication code can be embedded into the fourth bit of the HL4 coefficient, which is lower than the fifth bit in the first MSB bit plane embedding. Similarly, the different sub-band coefficients with lower embedding bits can be selected to embed the residual authentication bits.

However, the embedded authentication bits might be modified by acceptable image processing such as compression, blurring, etc. To distinguish the acceptable processing from malicious manipulation, the robustness is explored. The locations of coefficient bits that are lower than the embedding bit are further considered. For example, an original coefficient magnitude is modified from 63 (111111 in binary) to 47 (101111 in binary) for embedding an authentication bit 0. If the acceptable image processing caused the magnitude is modified from 47 to 48 (110000 in binary). In this case, the embedded bit is easily removed. So, the bits lower than the embedding bit should also be considered. If the value of the embedding bit is modified from 1 to 0, the value of the next lower bit is set to 1 and the other lower bit values are set to 0. On this consideration, the coefficient magnitude is modified from 63 to 40 (from 111111 to 101000 in binary) in which the fifth LSB is the embedding bit and the fourth LSB is set to 1 and the remained lower bits (from the first to third LSBs) are set to 0. On the other hand, if the value of the embedding bit is 1, the coefficient magnitude is modified from 63 to 48 (111111 to 110000 in binary). On this robustness consideration, the embedding bit will not be removed by the little modification. On the contrary, the significant modification caused by the malicious manipulation will be detected according to the modified embedded bit.

In summary, the authentication code is extracted from the content of the image and reformed according to its importance. The most important authentication code is first embedded in the earlier encoding stages. And then, the less important authentication code is embedded in the last encoding stages. From that, the earlier decoded image can be authenticated by the authentication code, which is extracted from the earlier decoded image.

2.3: THE AUTHENTICATION PROCEDURE

In the authentication procedure, the embedded authentication code is extracted from the received image to verify the content of the progressive decoded image. Based on the multi-stage encoding/decoding algorithm, the progressive decoded image can be authenticated when the embedded authentication code is received. Because the first MSB bit plane of the authentication code is first embedded in the earlier encoding stages, so it will be extracted in the earlier decoding stages. Once the authentication code is extracted, the current decoded image can be authenticated. If the current decoded image is authenticated, the next decoding stage can be done. Otherwise, the decoding processing is halted for the malicious manipulation is detected and the decoded image is unauthenticated. The authentication can be performed once the authentication bit is extracted. In other words, the multi-stage decoded image can be authenticated progressively.

In the authentication processing, the image is reconstructed progressively according to the multi-stage decoding. Once the embedded first MSB bit plane is received and extracted, the first authentication processing can be performed. The first MSB bit plane of the authentication code can be used to verify the coefficient magnitude in the LH4 sub-band. The authentication processing compares the authentication bit and the current reconstructed magnitude in LH4 sub-band. Because the authentication bit preserves the characteristic to indicate the rough coefficient magnitude, so, the comparison between the rough magnitude and the reconstructed magnitude of the corresponding coefficient can be used to authenticate the current decoded image. If the comparison result indicates that the malicious operation is detected, the position of the tampered area can be located and the transmission is halted. Otherwise, the current decoded

image is authenticated. However, the current authentication processing only verifies the current decoded image. The refined information will be received in the following stages and the further authentication should be performed when the further authentication code is extracted.

Since the authentication can be preformed stage by stage, the progressive decoded image is verified from rough to detail. The significant modification can be located in the earlier authentication stages. The slight modification is detected in the last authentication stages when the detailed image information is received. Once the first authentication processing is authenticated, the following refined image is reconstructed. The second MSB bit plane is extracted when the coefficients in HL4 sub-band are available. Similar authentication processing is performed to authenticate the detailed image. In this authentication processing, the first and the second authentication bits are combined to further verify the more detailed image information. From that, the progressive decoded image can be authenticated progressively.

3: EXPERIMENTAL RESULTS

Several experiments were performed to evaluate the validity of the proposed method. A set of gray-level test images of 512×512 pixels were used in the experiments. These test images are first transformed into four-level DWT coefficients using the Haar transformation. The magnitude of LH4 sub-band coefficient is selected and quantized by the exponent operation. The quantized magnitude is further scaled to form the authentication code. In this experiment, four scaled authentication code (with 2-bit binary) is employed. The first and the second MSBs of the authentication code are embedded into LL and HL4 sub-bands, respectively.

The distribution of coefficient magnitude among LL, LH4, HL4 and HH4 sub-bands was explored to find out the authentication code. The results of the number of coefficient magnitudes among sub-bands with different thresholds were shown in Table 2. In Table 2, it can be seen that more of larger magnitudes are encountered in LL sub-band. On the other hand, most of HH4 coefficient magnitudes are small. The distribution in LH4 and HL4 sub-bands is normal. So, both of LH4 and HL4 sub-bands are suitable to generate the authentication code.

From the authentication code generation, the size of the authentication code is determined according to the selected sub-bands and the number of scales. Table 3 listed the sizes of the authentication code with different sub-bands and scales. From Table 3, it is shown that the authentication code size is adaptive. The larger the authentication code size is, the more precise of the authentication will be. In this experiment, LH4 sub-band and four scales are selected. The size of the authentication code is 2048 (1024×2) bits. The small size of the authentication code benefits the embedding procedure and the quality of the watermarked images.

The images shown in Fig. 1 are used to illustrate the characteristic of the multi-stage encoding/decoding. The resolution of the reconstructed images is determined by encoding/decoding stages in which predefined thresholds (TH) are employed. For example, the image resolution shown in Fig. 1(b) is higher than that of in Fig. 1(a). This is because a lower TH is employed in Fig. 1(b) and more detailed information is used to reconstruct the image. Similarly, the image shown in Fig. 1(e) is more detailed than that of in Fig. 1(f). In multi-stage transmission, once the information to reconstruct the image is enough, the transmission can be halted. In other words, the remained transmission stages are usually omitted. However, the authentication of the received partial image is also required for security.

To evaluate the validity of the proposed progressive image authentication method, several experiments were performed. The experimental results were shown in Fig. 2. The watermarked image of the first MSBs of the authentication code embedded in threshold (TH) 64 was shown in Fig. 2(a) with PSNR 27.74 dB. The second MSBs was embedded during the encoding of threshold (TH) 32. The watermarked image was shown in Fig. 2(b) with PSNR 30.42 dB. By comparing the PSNR between Figs. 1(c), 1(d) and 2(a), 2(b), it is shown that the degradation of the watermarked image is near ignored. After this encoding process, all of the authentication code was embedded into the watermarked image. The following encoding stages were performed sequentially and the complete watermarked image was shown in Fig. 2(c) with PSNR 37.08 dB. The tampered image was created in which the watermarked image shown in Fig. 2(c) was modified. In Fig. 2(d), two dots were inserted into the image Lena's arm and hair with different significances. The authentication results using Fig. 2(d) were shown in Figs. 2(e) and 2(f), respectively. When the first MSBs authentication code were received and extracted, the authentication processing was performed immediately. The authentication result was shown in Fig. 2(e). From Fig. 2(e), it is noted that only the significant modification in Lena's arm is located.

When further detailed image information is received, the second MSB authentication code can be extracted. All of extracted authentication bits (the first and the second MSBs) were combined to perform the more precise authentication. The authentication result was shown in Fig. 2(f). In Fig. 2(f), both of tampered areas were correctly located even though the insignificant modification in Lena's hair. From these experimental results, it is shown that the proposed progressive image authentication is achieved.

Table 2. The magnitude distribution among sub-bands with different thresholds (TH)

Thresholds / Images	TH≧1024				256≦TH＜1024				64≦TH＜256				32≦TH＜64			
	LL	LH4	HL4	HH4	LL	LH4	HL4	HH4	LL	LH4	HL4	HH4	LL	LH4	HL4	HH4
Airplane	1021	1	0	0	3	95	77	11	0	272	231	194	0	184	128	140
Lena	898	0	0	0	126	49	169	36	0	254	359	192	0	155	123	143
Girl	904	0	0	0	117	75	79	10	3	325	337	226	0	163	171	209
Toys	510	14	32	0	514	82	87	19	0	267	194	137	0	85	50	74
Peppers	873	3	0	0	145	98	155	23	6	336	351	236	0	175	189	139
Baboon	998	0	0	0	26	43	49	7	0	387	459	313	0	230	231	277

Table 3. The sizes (unit: bit) of the authentication code with different sub-bands and scales

No. of scales / Sub-bands	LH4	LH3	LH2	LH1
2	1024	4096	16384	65536
4	2048	8192	32768	131072
8	3072	12288	49152	196608
16	4096	16384	65536	262144

(a) Reconstructed, TH=256, PSNR=22.24dB (b) Reconstructed, TH=128, PSNR=25.00dB (c) Reconstructed, TH=64, PSNR=27.86dB

(d) Reconstructed, TH=32, PSNR=31.11dB (e) Reconstructed, TH=16, PSNR=34.82dB (f) Reconstructed, TH=8, PSNR=38.94dB

Fig. 1. The progressively reconstructed images with different thresholds

(a) Watermarked, TH = 64, PSNR=27.74dB (b) Watermarked, TH= 32, PSNR=30.42dB (c) Watermarked, TH = 1, PSNR=37.08dB

(d) Tampered, TH = 1 (e) Detected, TH= 64 (f) Detected, TH= 32

Fig. 2. The tampered and detected progressive images

4: CONCLUSIONS

In this paper, a progressive image authentication method is presented. A multi-stage decoded image can be authenticated progressively. The authentication code is directly embedded into the transmitted image such that the extra space for authentication code is avoided. The size of the authentication code is adaptive and can be determined by the number of scales and the selected hierarchical sub-bands.

The positions of the tampered areas can be located according to the degree of the malicious. The significant tampered area can be located in the earlier authentication. The slight malicious will be detected in the following authentication. The results show the validity of progressive images authentication with small authentication size.

In the future researches, more of authentication stages will be explored to verify the variant resolution images. And then, the famous multi-stage encoding algorithms such as EZW, SPIHT and JPEG 2000, etc. will be studied in which the progressive image authentication can be employed.

Acknowledgement: This paper was supported by National Science Council under NSC grant 94-2213-E-239-008.

REFERENCES

1. Eggers, J., and Girod, B.: Blind Watermarking Applied to Image Authentication. Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing ICASSP ‘01, Salt Lake City, UT, May (2001) 1977-1980.
2. Celik, M. U., Sharma, G., Saber, E., and Tekalp, A. M.: Hierarchical Watermarking for Secure Image Authentication with Localization. IEEE Transactions on Image Processing, Vol. 11, 6(2002) 585-594.
3. Queluz, M. P.: Authentication of Digital Images and Video: Generic Models and a New Contribution. Signal Processing: Image Communication, Vol.16, (2001) 461-475.
4. Lin, C. Y., and Chang, S. F.: A Robust Image Authentication Method Distinguishing JPEG Compression from Malicious Manipulation. IEEE Transactions on Circuits and Systems of Video Technology, Vol. 11, 2(2001) 153-168.
5. Xie, L., Arce, G. R., and Graveman, R. F.: Approximate Image Message Authentication Codes. IEEE Transactions on Multimedia, vol. 3, 2(2001) 242-252.
6. Tsai, P., and Hu, Y. C.: A Watermark-Based Authentication with Malicious Detection and Recovery. The Fifth International Conference on Information, Communications & Signal Processing (ICICS 2005), Bangkok, Thailand. (2005) 865-869.
7. Tsai, P., Hu, Y. C., and Chang, C. C: Using Set Partitioning in Hierarchical Trees to Authenticate Digital images. Signal Processing: Image Communication, Vol. 18, (2003), pp. 813-822.