A Unified Authentication Framework for JPEG2000

Zhishou Zhang[1], Gang Qiu[1], Qibin Sun[1], Xiao Lin[1]
[1]Institute for Infocomm Research
21 Heng Mui Keng Terrace, Singapore 119613
{zszhang, visgangq, qibin, linxiao}@i2r.a-star.edu.sg

Zhicheng Ni[2], Yun Q. Shi[2],
[2]New Jersey Institute of Technology
Newark, NJ 07102, USA
{zn2, shi}@njit.edu

Abstract

This paper proposes a unified authentication framework for JPEG2000 images, which consists of fragile, lossy and lossless authentication for different applications. The authentication strength can be specified using only one parameter called Lowest Authentication Bit-Rate (LABR), bringing much convenience to users. The lossy and lossless authentication could survive various incidental distortions while being able to allocate malicious attacks. In addition, with lossless authentication, the original image can be recovered after verification if no incidental distortion is introduced.

1. Introduction

JPEG2000 [2] is a new international image standard with many advanced features including lossy-to-lossless compression, better compression ratio, SNR and resolution scalability, Region of Interest (ROI) and so on. However, such coding flexibilities also pose the challenges on its new part (Part 8): security part called JPSEC [3]. In JPSEC, authentication is one of the main services being addressed. The JPSEC requirements on authentication are highlighted as follows.

- The authentication must be compliant with JPEG2000 Part 1 (core part). It cannot crash a JPEG2000 part-1 compliant decoder.
- The authentication must cover both data integrity and non-repudiation (i.e., source identification). A secure JPEG2000 file will allow for verification of integrity of the content. This includes semi-robust integrity verification, as well as mechanisms to optionally identify locations in the image content where the integrity is put into question.
- The authentication must protect whole code-stream, components, tiles, resolutions, subbands, quality layers, precincts, ROIs, and codeblocks.

Traditional digital signature techniques [4] (e.g., DSA or RSA) provide an effective and secure solution for data authentication, which covers both integrity protection and non-repudiation. Any one-bit change will make the protected data unauthentic, which is definitely advantageous for data as every bit of data is vital. Directly applying digital signature techniques to image provides a good protection. Such authentication on image is called fragile authentication. However, it works on image in an unreasonably strict way because one-bit change on image usually is trivial. For example, when images are exchanged between different entities, they are unavoidably experiencing incidental distortion introduced by image transcoding, unreliable carrier or multi-cycle compression, to name a few. Though incidental distortion makes image data change, usually it doesn't change the meaning of the image. Therefore, the fragility of traditional digital signature techniques limits their typical applications to images.

In this paper we propose a unified authentication system that can protect JPEG2000 image with different robustness modes (fragile, lossy and lossless). The whole framework is compliant with Public Key Infrastructure (PKI): After image signing, the signature together with the watermarked image is sent to the recipients. At the receiver site, the recipient can verify the authenticity of the image by using the image sender's public key and the signature. In our system, fragile mode is straightforward by employing the traditional crypto signature scheme. Lossy and Lossless modes are robust against the predefined image manipulations such as image format conversion or transcoding. In addition, lossy and lossless modes can allocate the attacked area, if the image is maliciously manipulated. Moreover, lossless mode is able to recover the original image after image verification if no incidental distortion is introduced. Finally, the authentication strength could be quantitatively specified by the parameter LABR. It means that all data/content of image above LABR will be protected. Thus it will bring users much convenience.

The proposed authentication system has been submitted to JPSEC, for consideration as a part of JPEG2000 standards [1].

0-7803-8603-5/04/$20.00

The paper is organized as follows. Section 2 presents the system description; Section 3 gives the experimental results; Section 4 summarizes this paper.

2. System overview

Fig. 1 illustrates the proposed authentication system. Given a target Lowest Authentication Bit Rate (LABR) and authentication robustness mode (e.g., fragile, lossless or lossy), one digital signature is generated from the image content during JPEG2000 coding procedure. The image content can be protected in various granularities such as different subbands, different resolution levels, etc. If the required authentication mode is fragile, the traditional signature module is invoked to generate its corresponding signature. If the required authentication mode is lossless, the robust signature module with lossless data hidding function is invoked so that after signature verification, the image content can be exactly recovered. If transcoding has been applied to the image, the JPEG2000 image can still be verified but cannot be exactly recovered. If the required authentication mode is lossy, the robust signature module with lossy data hiding function is invoked to make the generated signature be robust to the incidental distortions. The final outputs are a JPEG2000 image (with watermark for lossy and lossless authentication and without watermark for fragile authentication) and its associated digital signature.

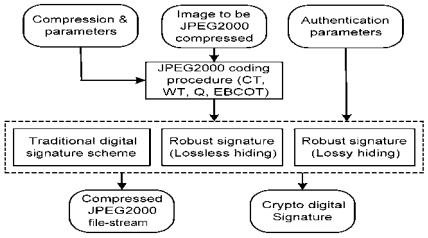


Fig. 1. System Diagram

Fragile authentication

Fragile mode is selected for protecting JPEG2000 code-streams. Fragile signing and verifying operations are quite straightforward, as shown in Fig. 2 and 3. During signing, the original image is encoded as per normal. While the codestream is formulated, its protected parts, as specified by LABR and other parameters, are extracted and fed to traditional hashing and signing operation. As result, a digital signature is generated. During verifying, while the codestream is parsed during decoding, its protected part, as specified by LABR and other parameters, is extracted and fed to traditional hashing and verifying operation, which returns the verification result: even one-bit change in the protected part will be deemed as unauthentic.

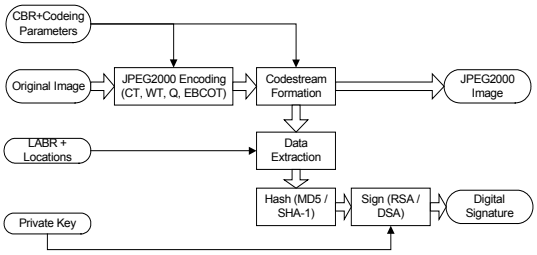


Fig. 2 Fragile sign operation

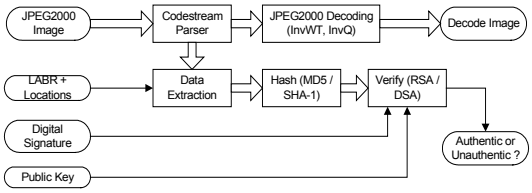


Fig. 3 Fragile verify operation

Lossy authentication

Lossy mode is usually selected for those applications demanding for more robustness such as wireless communication. Fig. 4 illustrates the basic ideas of lossy signing operation [5]. Firstly, the original image undergoes color and wavelet transformation, quantization, arithmetic coding and EBCOT, which are all basic procedures in JPEG2000 encoding. EBCOT process will find out for each coded block those bit-planes that are above LABR (i.e., they survive transcoding operation to LABR). Then, decision is made on which resolution level (X) is suitable for feature extraction and which resolution level (Y) for watermark embedding, based on Human Vision System (HVS). The block-based feature, F_i, is then encoded with selected Error Correction Coding (ECC) Scheme to generate codeword CW_i. The Parity Check Bits of CW_i, PCB_i, is used as a seed to formulate block based watermark W_i, which is then embedded into the corresponding block in LH or HH subband of Y. In addition, features from all blocks are concatenated and the resulted bit sequence is hashed by a cryptographic hashing function such as MD5 or SHA-1. The generated hash value can then be signed using the content sender's private key to form the crypto signature.

Fig. 5 illustrates the lossy verifying operation. The inputs to verifying operation are the received JPEG-2000 image (possibly undergone some incidental distortion or malicious attack), LABR, signature and public key. The codestream parser finds out for each

block those bit-planes above LABR, based on which we can decide the resolution level X for feature extraction and resolution Y for watermark extraction. Block-based feature extraction is the same to that in signing operation. Block-based watermark is extracted from each block in resolution Y. Note that if the input image is not JPEG2000 format, we have to repeat the operation that is the same as the signing to obtain the watermark and the features. Then combining features and PCBs from each block forms codeword, and the whole verification decision could be made orderly. Firstly, we calculate the syndrome of the codeword for each block to see whether any blocks are uncorrectable. If yes, then we claim the image is unauthentic and those blocks with uncorrectable codewords are attacked area. However, if all codewords are correctable (i.e. errors in any feature code are correctable by its PCB), all corrected codewords are concatenated into a bit sequence, which is then cryptographically hashed. The final verification result is concluded through a cryptographic verifying operation using supplied signature and public key.

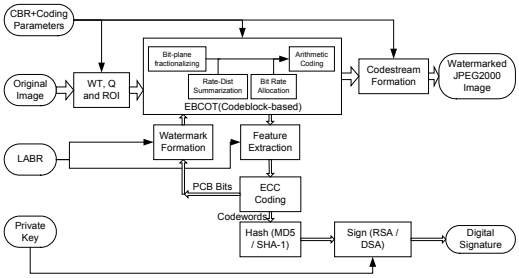


Fig. 4 Lossy signing operation

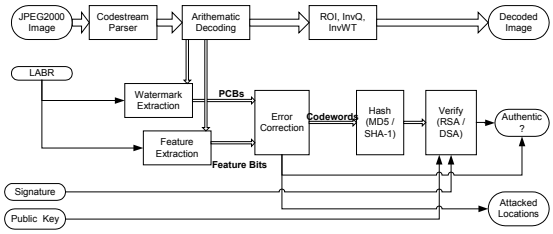


Fig. 5 Lossy verifying operation

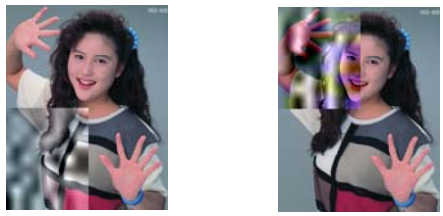
Lossless authentication

Lossless mode is usually selected for medical or remote imaging related applications where lossless recovery of the original image is required. Lossless signing operation is very similar to lossy signing operation (Fig. 4). The only difference lies in watermark embedding module. The lossless watermarking method used is novel [6], which doesn't use modulo 256 addition and hence doesn't generate annoying salt-pepper noise, and robust against image compression. The codeblock whose size is usually 64x64 is further divided into 8x8 blocks called patches. The coefficients in a patch are split into two subsets. Then we calculate the difference value α, which is defined as the arithmetic average of differences of coefficients in two respective subsets. Since in a patch, the coefficients are highly correlated, the difference value α is expected to be very close to zero. Furthermore, it has certain robustness against incidental distortions because α is based on all coefficients in the patch. Each patch is embedded with one bit. If 1 is to be embedded, we shift difference value α to right side or left side beyond a threshold, by adding or subtracting a fixed number from each coefficients within one subset. If 0 is to be embedded, the patch is intact. There are chances that the value α is originally beyond the threshold and a bit of binary 0 is to be embedded. In this case, we shift the value α further away beyond the threshold, and rely on ECC to correct the bit error, because the watermark bits are ECC encoded again before being embedded.

Lossless verifying operation is also similar to lossy one, with the exception of watermark extraction. The code block is divided in patches and difference value α of each patch is calculated in the same way as lossless sign. For each patch, if value α is beyond the threshold, a bit of "1" is extracted and the difference value is shifted back to its original position, which means that original coefficients are recovered. If the value α is inside the threshold, a bit of "0" is extracted and nothing needs to be done. Finally an ECC correction is applied on the extracted bit sequence to get the correct watermark bits.

3. Experiment results

Fragile authentication is the most restricted protection of the image; even a single-bit attack of the protected part will be deemed unauthentic. Fig. 6 is the verification result of an attacked image whose tile 0 (upper-left part) is protected (Totally 4 tiles).



a.) Tile 2 attacked, Authentic

b.) Tile 0 attacked, Unauthentic

Fig. 6 Fragile authentication testing results

In Fig. 7, a.) is the original image (640x512); b.) is watermarked image generated from lossy signing operation with LABR being 1 *bpp*. The PSNR between original and watermarked image is 42 dB. c.) is the attacked image with some text added near the woman's finger; d.) is the verified image with attacked area highlighted in red rectangle.

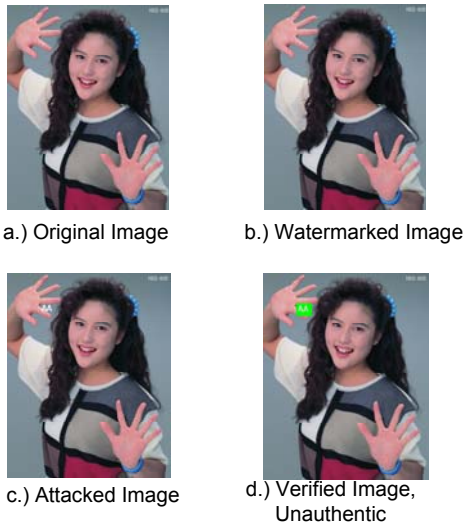


Fig. 7 Lossy authentication results

For lossless authentication, the same image (as in Fig. 7 a.) is used for testing. In Fig. 8, a.) is the watermarked image generated from lossless signing operation with LABR being 4 *bpp*; b.) is the recovered image after lossless verify operation. The PSNR between watermarked and original image is 45 dB, and the PSNR between recovered and original image is infinity which means the original image can be recovered.

Fig. 8 Lossless authentication results

Fig. 9 and Fig. 10 compare the image quality and file size before and after signing. The image is encoded with 9x7 filter (with and without lossy watermark) and 5x3 filter (with and without lossless watermark) respectively. We can see that the image quality drops slightly with watermark embedded and no significant difference between the image sizes. More detailed testing results are given in [1].

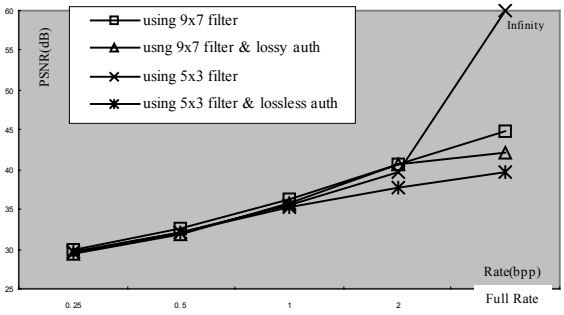


Fig. 9 PSNR comparison of "woman" images

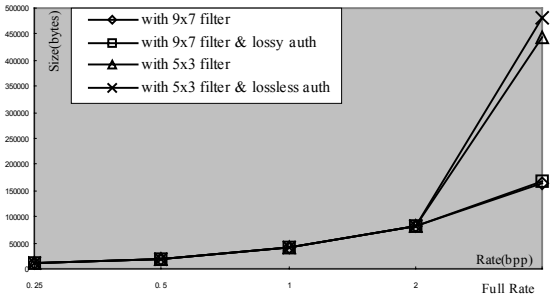


Fig. 10 File size of "woman" images

4. Conclusion

In this paper, we have proposed an authentication system for different applications by employing different modes (fragile, lossy and lossless). The framework provides a systematic and quantitative way for authenticating JPEG2000 image in terms of LABR. In addition, it is fully compatible with JPEG2000 coding and traditional crypto schemes.

10. References

[1] Z. Zhang, G. Qiu, Q. Sun, X. Lin Z. Ni, Y. Q. Shi, "A Unified Authentication Framework for JPEG2000: System Description and Experiment Results", ISO/IEC JTC 1/SC29/WG1 N3074.

[2] JPEG2000 Part 1: Core coding system, ISO/IEC 15444-1:2000.

[3] JPSEC workdraft version 2, ISO/IEC JTC 1/SC29/WG1 N3055.

[4] B. Schneier, Applied Cryptography, Wiley, 1996.

[5] Q. Sun, S.-F. Chang, M. Kurato and M. Suto, "A Quantitive Semi-Fragile JPEG2000 Image Authentication System", ICIP2002, Rochester, USA

[6] Z. Ni and Y. Q. Shi, "A Novel Lossless Data Hiding Algorithm And Its Application In Authentication of JPEG2000 Images", Technical Report, July 2003.