International Journal of Image and Graphics
Vol. 5, No. 1 (2005) 1–14
© World Scientific Publishing Company

A CRYPTO SIGNATURE SCHEME FOR IMAGE AUTHENTICATION OVER WIRELESS CHANNEL

QIBIN SUN* and SHUIMING YE†
Institute for Infocomm Research,
21 Heng Mui Keng Terrace, 119613, Singapore
**qibin@i2r.a-star.edu.sg*
†*shuiming@i2r.a-star.edu.sg*

CHING-YUNG LIN
IBM T. J. Waston Research Center,
19 Skyline Dr., Hawthorne, NY 10532, USA
cylin@waston.ibm.com

SHIH-FU CHANG
Department of Electrical Engineering, Columbia University,
NY 10027, USA
sfchang@ee.columbia.edu

Received 27 October 2003
Revised 1 December 2003
Accepted 23 December 2003

With the ambient use of digital images and the increasing concern on their integrity and originality, consumers are facing an emergent need of authenticating degraded images despite lossy compression and packet loss. In this paper, we propose a scheme to meet this need by incorporating watermarking solution into traditional cryptographic signature scheme to make the digital signatures robust to these image degradations. Due to the unpredictable degradations, the pre-processing and block shuffling techniques are applied onto the image at the signing end to stabilize the feature extracted at the verification end. The proposed approach is compatible with traditional cryptographic signature scheme except that the original image needs to be watermarked in order to guarantee the robustness of its derived digital signature. We demonstrate the effectiveness of this proposed scheme through practical experimental results.

Keywords: Authentication; digital signature; watermark; packet loss; image transmission; error concealment.

1. Introduction

Our objective is to design a cryptographic (digital) signature scheme that allows two parties to exchange images while guaranteeing image integrity and non-repudiation from the image sender, over a lossy channel. We demand a cryptographic signature scheme working at semi-fragile level: some manipulations on the image will be considered acceptable (e.g. lossy compression and packet loss) while some are not allowable (e.g. content copy-paste). Here, integrity protection means that an image cannot be modified in such a way that its meaning is altered. Non-repudiation prevention means that once the image sender generates the cryptographic signature for an image, he cannot subsequently deny such a signing if both the signature and the image have been verified as authentic.

Note that at semi-fragile level, watermark-based approaches usually work for protecting the integrity of the image but not for preventing sender's repudiation.[1,2] Signature-based approaches can work on both the integrity protection of the image and the repudiation prevention of the sender, but prior robust digital signature is unavoidably very large because its size is usually proportional to the image size.[3–5] In order to solve these problems, efforts towards the combination of cryptographic signature and watermarking are being explored in these papers.[3,6,7] In Ref. 3, the author proposed to sign on the extracted/quantized features to form the signature and then either append to the image file or watermark into the image content. However, the variation of the features (e.g. quantization errors) makes crypto hash unavailable which still remains the security risks. Recently, a self-authentication-and-recovery image watermarking system was proposed.[6] In Ref. 7, we further extended Ref. 6 for working under PKI, by integrating feature extraction, error correction coding (ECC), watermarking and cryptographic signature into a unified framework.

In this paper, we propose a novel hybrid digital signature (DS) and watermarking system, which generates short and robust digital signatures based on the invariant message authentication codes (MACs). These MACs are obtained from the quantized original transform-domain coefficients and ECC-like embedded watermarks. The invariance of MACs is theoretically guaranteed if images are under lossy compression or other acceptable minor manipulations such as smoothing, brightness change, etc. Similar approach based on MACs for robust digital signature generation was proposed in Ref. 4. However, the MACs in Ref. 4 are only weakly invariant, which has some exceptional ambiguous cases when two coefficients are the same after manipulations. Because of these ambiguous cases, the whole MACs generated from the signing end has to be preserved in the receiving end. Thus, the size of digital signature is proportional to the image size. In this paper, we propose a method to generate the MACs that are strictly invariant in the signing end and the receiving end. Thus, hash function can be applied to significantly reduce the size of digital signature.

We further propose a cryptographic signature based authentication scheme robust to packet loss. The system generates only one fixed-length cryptographic signature (hundreds of bits) per image regardless of image size and packet loss. System robustness (i.e. to tolerate the distortions of packet loss) is achieved through an effective method based on error concealment concepts. System security (i.e. to prevent attacked images from passing authentication) is obtained by adopting

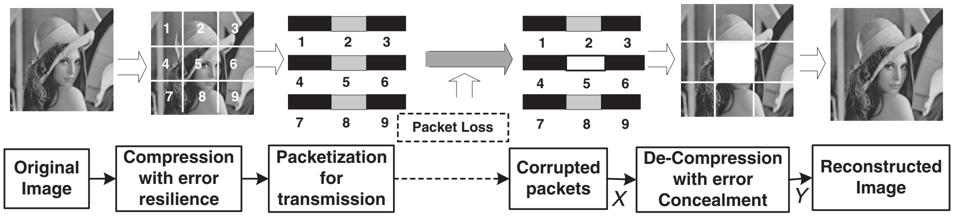

1 2 3
4 5 6
7 8 9
Packet Loss
Original Image
Compression with error resilience
Packetization for transmission
Corrupted packets
X
De-Compression with error Concealment
Y
Reconstructed Image

Fig. 1. Image transmission over lossy channel.

cryptographic hashing and signature scheme. We use watermarks to store ECC check information and allocate attacks. The Public Key Infrastructure (PKI)[9] is incorporated for addressing the authentication problems over various networks.

The paper is organized as follows. In Sec. 2, we briefly discuss the issues of authenticating data over lossy channel. In Sec. 3, we present a method for generating invariant MACs through watermarking. In Sec. 4, we describe the details of the authentication system, which is robust to packet loss. The experimental results and conclusions are shown in Secs. 5 and 6, respectively.

2. Authentication and Data Loss

Figure 1 illustrates the typical procedure of image transmission over a lossy channel (i.e. some data will be lost during transmission). Original image is encoded together with some error resilient techniques, block by block. The compressed bit-stream is then packetized for transmission. Assume the transmission channel is unreliable, some data packets will be lost before reaching the receiver (e.g. packets corresponding to block 5). Such loss will be known at the receiver end either by the transmission protocols (e.g. Real Time Protocol–RTP) or by content-based error detection techniques.[11,14] The corrupted image could be approximately recovered by error concealment techniques before displaying.

Refer to Fig. 1, at the receiver end, the authentication could be done either at point X or point Y, depending on applications. If we want to authenticate the corrupted image without error concealment, then we should conduct the authentication at point X; Otherwise, we should select point Y for authentication. The advantage for authenticating at point Y is that the concealed image is still securely reusable for other applications without re-doing error concealment every time.

Authenticating data over a lossy channel at point X has been studied in cryptography field.[8] In general, the idea is as follows: if a cryptographic hash of packet P_1 is appended to packet P_2 before signing P_2, then the signature on P_2 guarantees the authenticity of both P_1 and P_2. If P_1 is lost during transmission, the whole data-stream can still be authenticated because the hash value of lost packet P_1 can be obtained from the received packet P_2. However, directly applying this solution to image transmission has several drawbacks: (1) With the increase of Bit Error Rate (BER), the transmission payload will unavoidably increase; (2)

In image transmission, the importance and the size of packets varies in different environment. It may not be practical to generate hash functions from pre-defined fixed boundaries.

Once the image data are lost, the corresponding lost image parts could be approximated by its neighboring content based on various error concealment techniques. Considering different error concealment techniques only work well for particular type of image content (e.g. flat area, edge area, etc), digital watermarking has been successfully employed for selecting optimal error concealment technique.[13] Their basic idea is to analyze the important characteristics of the block to be processed such as its edge strength and embed it into other blocks as watermarks. If this block is corrupted during transmission, the best error concealment method can be selected and applied to this block adaptively based on the extracted watermarks.

To solve the drawbacks of solution,[8] here we propose a simple but effective approach to authenticate the corrupted image at point X, by combing the solution in Refs. 8 and 13. Refer to Fig. 1, instead of calculating the cryptographic hash value packet by packet, we calculate it in terms of image block. The computed hash value is watermarked into other blocks as watermarks. Later at the receiver end, assuming a block is corrupted by packet loss (e.g. block 5 in Fig. 1), its hash value can still be extracted from other blocks and the whole authentication can proceed successfully.

In the remaining sections we shall describe the idea of authenticating image at point B aiming at more practical applications.

3. Hybrid Digital Signature and Watermarking Scheme

In Ref. 6, Lin and Chang proposed a theorem for generating quantization-based invariant coefficients that are robust to distortions as long as later distortions are within the conceptually acceptable bounds. That theorem applies an HVS-based larger quantization step (Q) to make the updated coefficients be robust to later changes. In this novel method, instead of updating the original coefficients to make them invariant in the quantization domain, we do not change original coefficients but to store some auxiliary error control code (ECC) information in other places in order to generate message authentication codes in the quantization domain. We also describe in more detail about how to generate MACs from images and watermark ECCs in images.

3.1. *Invariant message authentication codes*

We denote a quantization process as follows. Assume that an original value is D, the quantization step size specified in the quantization table is Q, and the outputs of quantizer is quotient F (integer rounding) and remainder R respectively: $D/Q = F$, and $D\%Q = R = D - F * Q$. Suppose the incidental distortion introduced by

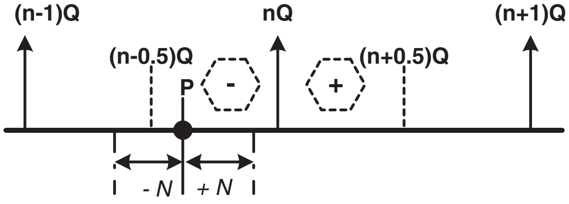


Fig. 2. Illustration on the concept of error correction.

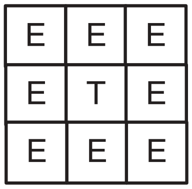
acceptable manipulations on the original coefficient D can be modeled as noise whose maximum absolute magnitude constraint is denoted as N.

Refering to Fig. 2, assuming a pre-determined $Q > 4N$ is known at both signing end and the receiving end. If the original value D is located at the point nQ, then no matter how this value is corrupted, if the distortion is in the acceptable bounds, the distorted value will still be in the range $((n - 0.5)Q, (n + 0.5)Q)$, and the quantized value using step size Q will remain unchanged as nQ before and after noise addition. However, if the original value D drops into the range of $((n - 0.5)Q, nQ)$ (the point **P** in Fig. 2), its quantized value (with step size Q) is still nQ before adding noise, but there is also a possibility that the noisy value could drop at the range $((n-1)Q, (n-0.5)Q)$ and will be quantized as $(n-1)Q$, not nQ, after adding noise. Thus the noise corruption will cause a different quantization result.

To avoid such a case, we propose an ECC-like procedure to record the sign of R. We want to push the points away from the quantization decision boundaries and create a margin of at least $Q/4$ so that the DCT value when contaminated later will not exceed the quantization decision boundaries. ECC codes are stored as watermarks (in other blocks) and can be retrieved by the authenticator.

We record an ECC bit "0" if the original value D drops between $((n-0.5)Q, nQ)$ (i.e. $R < 0$). In the authentication procedure, assume this value D has been corrupted. Add the value $0.25Q$ from the corrupted value, if we retrieve a watermark bit "0" indicating $R < 0$. Then, using the quantization step Q, we can obtain the same quantized value as nQ, which is the same as the original qnantized value. Similarly, if original value D is in $(nQ, (n + 0.5)Q)$ (i.e. $R > 0$), we record an ECC bit "1". In the authentication end, we subtract $0.25Q$ from the corrupted DCT value and obtain the same quantized value as nQ. Based on such an error correction procedure, all quantized values can be used to form message authentication codes (MACs) that will stay the same before and after distortion. These MACs can then be cryptographically hashed and encrypted to form cryptographic signature, which is short, fix-length and robust to signal distortion with acceptable manipulation bounds.

In prior discussions, the original value D, could be in the DCT domain, wavelet domain or original pixel domain, as long as the acceptable manipulation constraint



E	E	E
E	T	E
E	E	E

Fig. 3. Example of partitioning image blocks into **T** and **E**.

is predictable. As discussed in Ref. 10, several HVS models can be used to determine the setting of such constraints.

3.2. *MAC extraction and ECC watermarking*

Based on the method described in Sec. 2.1, a robust digital signature of image can be generated as follows. First, the image is partitioned and transformed into 8 × 8 blocks. Those blocks are further labeled as either **T** block or **E** block. We choose **T** blocks for extracting MACs and **E** blocks for watermarking. The selection and relations of **T** and **E** blocks can be specified by random seeds that are included in the digital signature.

For each **T** block, we pick up its DC and 3 ACs to generate MACs. These four coefficients are quantized by preset authentication strength matrix Q_a. These four bits are then watermarked into its corresponding **E** blocks. Assuming Q_a is used for generating features and watermarking while Q_c is for actual JPEG compression. In Ref. 6, the authors have proved that as long as Q_c is less than or equal to Q_a, the robustness of generated features as well as embedded watermarks is guaranteed. Based on this principle, we embed the watermark of **T** block by directly modifying some AC coefficients in **E**. A typical ratio of **T** and **E** blocks are 1:8. One example of partitioning blocks into **T** and **E** is shown in Fig. 3. Among eight **E** blocks of a **T** block, we only embed the watermark into those 3 blocks with highest AC energy (i.e. the most three textual blocks).

A one-way cryptographic hash function such as MD5 or SHA-1 is applied to the MACs concatenated from all **T** blocks. In addition to these hash values, other auxiliary information includes the size of image, and the authentication strength matrix (Q_a) are combined together and are encrypted using the image sender's private key to obtain the cryptographic signature.

4. Digital Signature Against Packet Loss

As discussed in Sec. 2, authenticating image data over lossy wireless channels derived from cryptographic techniques has its limits and drawback. In this section, we propose a novel solution based on the robust digital signatures generated from the MACs of the reconstructed degraded images via error concealment technique.

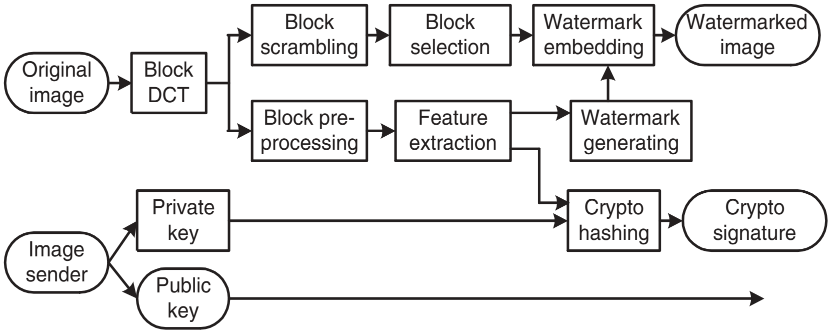


Fig. 4. The diagram of image signing.

Error concealment techniques are usually applied by either using contextual relationship of adjacent blocks,[11] or through embedded watermarking information.[12,13] In Ref. 11, Ye *et al.* conceal packet loss errors by exploring the contextual relationship between the damaged image blocks and their non-damaged neighboring blocks, which is a common solution in image and video transmission.[14] Our proposition is based on the error concealment technique in Ref. 11 with an additional block shuffling method in order to evenly distribute the corrupted blocks, and a preprocessing process to guarantee the invariance of the reconstructed images message authentication codes.

4.1. *Image signature procedure*

The image signing procedure is shown in Fig. 4. Given the image to be sent, the user generates a cryptographic signature by performing the following signing process on the image orderly: (1) Perform block-based pre-processing. (2) Extract the DCT features and generate the watermarks; Shuffle image blocks and select the blocks for watermarking. (3) Embed the watermarks and obtain the watermarked image. (4) Cryptographically hash the extracted features, generate the cryptographic signature by the image sender's private key. (5) Send the watermarked image and its associated cryptographic signature to the recipients.

Block shuffling

An original image is partitioned into 8×8 blocks. Those blocks are further labeled as either **T** block or **E** block. All **E** blocks are shuffled by a random number seed RGN. The final bit-stream is assembled in this shuffled block order before transmission. The reasons doing so are as follows. Firstly we want to ensure that most damaged blocks caused by packet loss are isolated. Such techniques have already been adopted in Ref. 11 and 14 to achieve a better result of error concealment. Secondly such shuffling makes the watermarks from those smooth blocks still embeddable. The shuffled blocks are labeled as $\mathbf{E}'$. We choose $\mathbf{T}$ blocks for extracting content-based features (MACs) and $\mathbf{E}/\mathbf{E}'$ blocks for watermarking.

Preprocessing

At the image signing section, it is impossible to know which blocks will be damaged in advance (i.e. which packets will be lost during the transmission is unknown). However, only two cases exist: either $\mathbf{T}$ is damaged or $\mathbf{E}$ is damaged. If it is an $\mathbf{E}$ block, it will affect the correctness of watermark extraction. If it is a $\mathbf{T}$ block, it will affect the stability of MAC extraction because $\mathbf{T}$ has to be reconstructed at the receiver site by the error concealment methods. Usually such reconstruction is just a roughly approximated version of original $\mathbf{T}$ and eventually affects either system robustness or system security because a large Q has to be set for feature extraction in order to tolerate a large N. Therefore some preprocessing is required. Assuming $\mathbf{T}$ is lost during transmission and is reconstructed by our error concealment algorithm,[11] denoted as $\mathbf{T}'$. We check the distortion between $\mathbf{T}$ and $\mathbf{T}'$. If it is greater than our preset N, we then recursively modify $\mathbf{T}$ with decreasing difference values on randomly selected coefficients until the modified coefficients can generate the same MACs as in $\mathbf{T}'$. In the worst situation, if this recursive method results in worse visible quality than that of $\mathbf{T}'$, the system can choose to directly replace $\mathbf{T}$ by $\mathbf{T}'$ as the signing end.

Note that the digital signature as described in Sec. 2.2 has to include the random number RGN for block shuffling.

4.2. *Image authentication procedure*

The image authentication procedure is shown in Fig. 5. Given the degraded image and its associated digital signature, the proposed solution authenticates both the integrity and the source of the received image by performing the following process on the image orderly: (1) Perform content-adaptive error concealment, if some blocks are damaged; (2) Extract message authentication codes and watermark respectively; (3) Correct the perturbations in the extracted feature set by

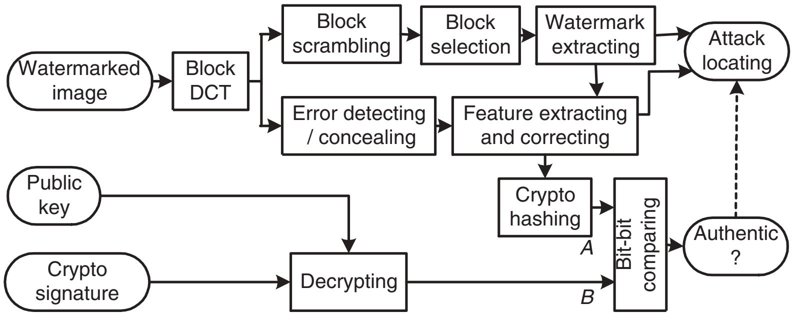


Fig. 5. The diagram of image authentication.

the extracted watermark based on the Error Correction Coding (ECC) concept; (4) Cryptographicgraphically hash the corrected feature set, obtain a short and fixed-length bit stream A; (5) Decrypt the signature by using the sender's public key and obtain another bit stream B; (6) Bit-bit compare A and B; Deem the image authentic if they are the same; Otherwise (7) Locate the possible attacks by correlating the extracted feature and the watermark.

Error detection and concealment

A summary of the content-based error concealment proposed in Ref. 11 is as follows. First, the damaged image blocks are detected by exploring the contextual information in images, such as their consistency and edge continuity. The statistical characteristics of missing blocks are then estimated based on the types of their surrounding blocks (e.g. smoothness, texture and edge). Finally different error concealment strategies are applied to different types of blocks to achieve better visual quality: Linear Interpolation method is used for smooth blocks, DCT Coefficient Prediction is used for textural blocks, and Directional Interpolation is applied to edge blocks.

Attack locating

If the image is verified as unauthentic, the attacked locations may be detected by correlating between the extracted watermarks and the remainders of DCT features quantized by Q_a. This advantage could help in further convincing the authentication results. Note that some false alarms may exist because of (1) Other incidental distortions, (2) The size of the attacked areas (i.e. the attack must be greater than one image block 8×8) and (3) The randomness of the quantization on DCT coefficients. This may be acceptable because the major system performances are system robustness (i.e. the image distorted by acceptable manipulations should be authentic) and system security (i.e. the image distorted by malicious attacks should be unauthentic). Moreover, such false alarms can be further reduced by removing isolated detected blocks, as shown in Fig. 8(f).

5. Experiments

We simulated the packet loss based on the Rayleigh model which is commonly used for wireless lossy channel. The attack simulation was done either before or after packet loss. Whole simulation procedure is shown in Fig. 6.

Figure 7 shows the merits of using block shuffling before image transmission on the stability of extracted features (MACs), by comparing the DCT value difference between original and concealed. Figure 7(c) is the histogram without block shuffling [the corrupted image is shown in Fig. 7(a)] and Fig. 7(d) is with block shuffling [the corrupted image is shown in Fig. 7(b)]. The number of DCT coefficients having small difference in Fig. 7(d) is much smaller than that in

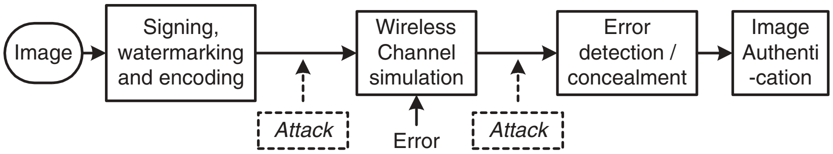
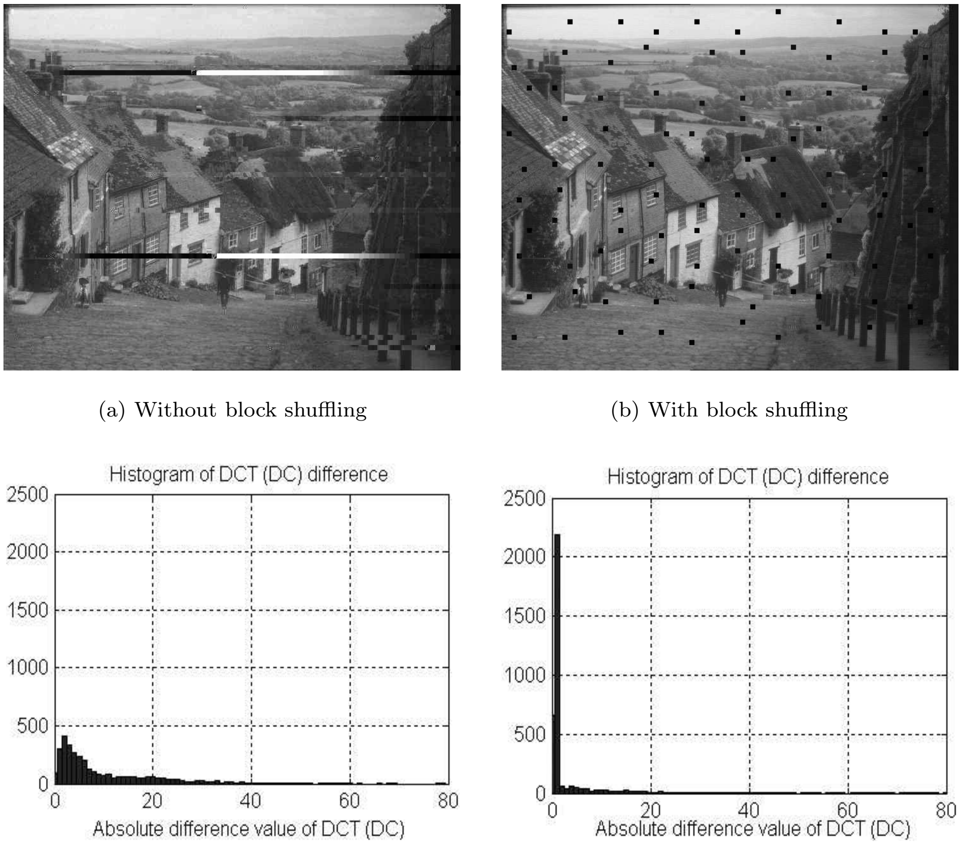


Image
Signing, watermarking and encoding
Attack
Wireless Channel simulation
Error
Attack
Error detection / concealment
Image Authenti -cation

Fig. 6. The flowchart of the experimental simulation.



(a) Without block shuffling

(b) With block shuffling

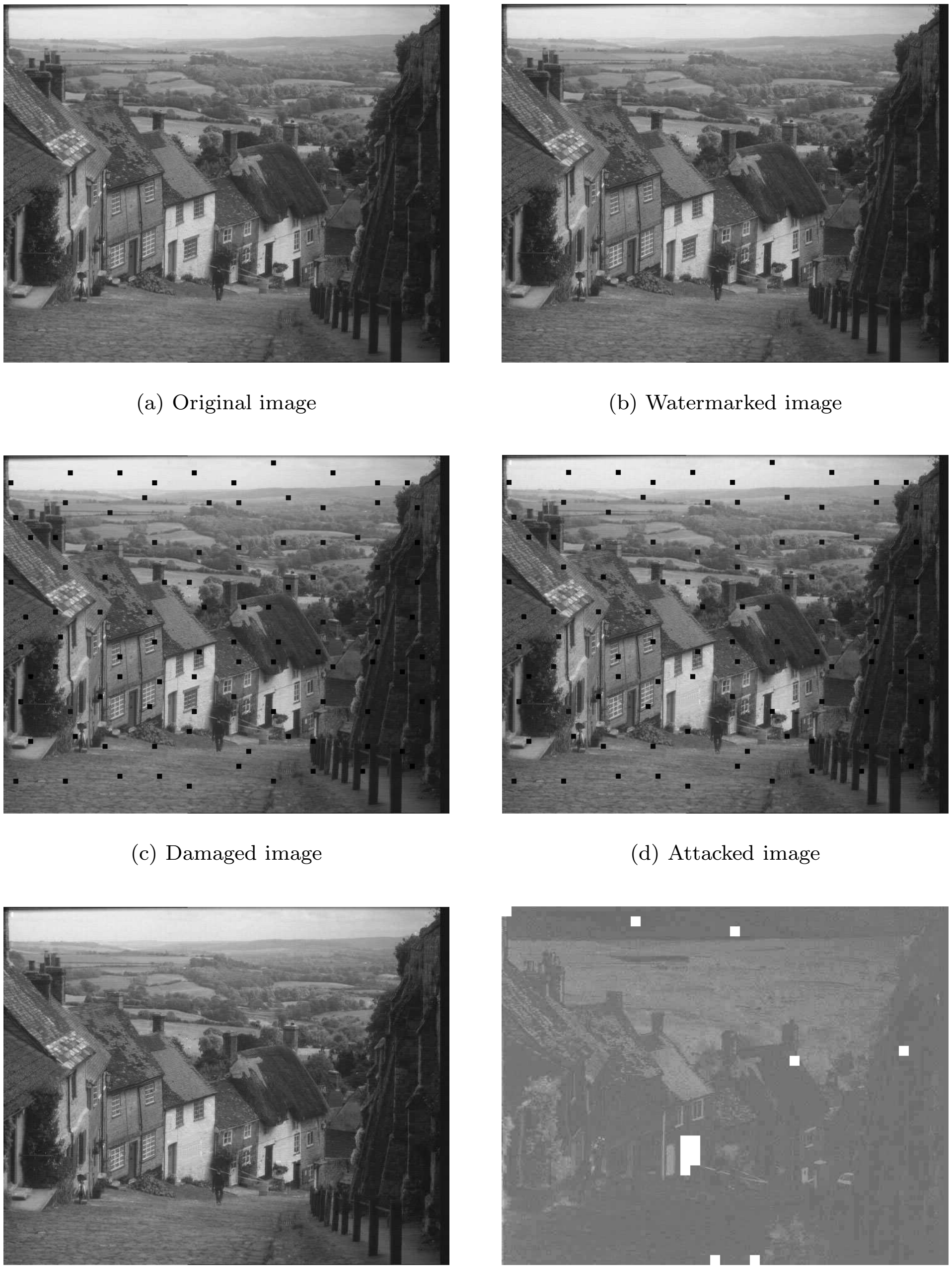
(c) DCT without block shuffling

(d) DCT with block shuffling

Fig. 7. Corrupted image without/with block shuffling.

Fig. 7(c). Such improvement allows us to choose smaller Q_a given the same Q_c, which consequently improves system security with fewer false negative on missing manipulations.

Figure 8 shows some experimental results. Figure 8(a) is the original image with the size of 768×512. Figure 8(b) is the watermarked image compressed with JPEG quality factor $8^{PhotoShop}$ (i.e. $Q_c = QF8$), the robustness of authentication and



(a) Original image

(b) Watermarked image

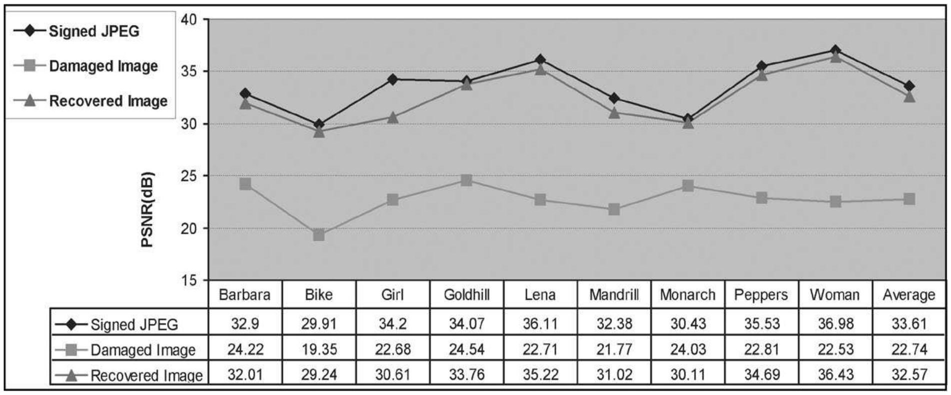
(c) Damaged image

(d) Attacked image

(e) Recovered image

(f) Detected attacks

Fig. 8. The examples of test results.



	Barbara	Bike	Girl	Goldhill	Lena	Mandrill	Monarch	Peppers	Woman	Average
Signed JPEG	32.9	29.91	34.2	34.07	36.11	32.38	30.43	35.53	36.98	33.61
Damaged Image	24.22	19.35	22.68	24.54	22.71	21.77	24.03	22.81	22.53	22.74
Recovered Image	32.01	29.24	30.61	33.76	35.22	31.02	30.11	34.69	36.43	32.57

Fig. 9. Image quality evaluation in terms of PSNR.

watermarking is set to JPEG quality factor 7 (i.e. $Q_a = QF7$). Figure 8(c) is the damaged image due to packet loss (The BER is $3 * 10^{-4}$). We have tested that the corrupted image below the BER of $3 * 10^{-3}$ can still pass the authentication after error concealment. Note that some damaged blocks may not be detected and therefore escape from being concealed. However, such missing data did not affect the authentication. This is because we set the same distortion measure for both pre-processing at the signing end and error concealment at the receiver end. Figure 8(d) is the attacked image on the damaged image (one window in the image center was removed and the location was filled with its surrounding image content). Figure 8(e) is the recovered image obtained by applying our error concealment techniques.[11] Figure 8(f) shows the detected attacked location. Due to packet loss and its subsequent error concealment, some false detected locations occur and are also shown in Fig. 8(f).

The image quality is also measured in terms of PSNR, as shown in Fig. 9. We use eight images for our test: Barbara, Bike, Girl, Goldhill, Lena, Mandrill, Monarch, Peppers, Women. Their sizes vary from 256 × 256 to 768 × 512. The first row shows the PSNR results between original images and watermarked images compressed with JPEG Quality Factor $8^{PhotoShop}$. The second row is the PSNR results between the original images and the corrupted images due to packet loss. The third row shows the PSNR results between original images and the recovered images. We see that the quality of the damaged images recovered by our error concealment method is very close to the original watermarked image.

6. Conclusion

We presented a semi-fragile authentication solution robust to packet loss. ECC and watermarking are incorporated into traditional crypto signature scheme to enhance the system robustness. Pre-processing and block shuffling techniques are adopted to stabilize the features for signature generation and verification. The system generates only one cryptographic signature regardless of the image size. The whole system could be incorporated into current PKIs, and thus can be more easily adopted by existing data authentication systems. Preliminary experiments have shown the effectiveness of this system. In the future, we will conduct more tests on the quality of watermarked images and discuss the deployment issues of this technique.

References

1. D. Kundur and D. Hatzinakos, "Digital watermarking for telltale tamper-proofing and authentication," *Proc. of the IEEE* **87**(7), 11670-1180 (1999).
2. C.-S. Lu and H.-Y. M. Liao, "Multipurpose watermarking for image authentication and protection," *IEEE Transactions on Image Processing* **10**(10), 1579–1592 (2001).
3. C. W. Wu, "On the design of content-based multimedia authentication systems," *IEEE Transacitons on Multimedia* **4**, 385–393 (2002).
4. C.-Y. Lin and S.-F. Chang, "A robust image authentication method surviving JPEG lossy compression," *SPIE Security and Watermarking of Multimedia Content* (January 1998).
5. L. Xie, G. R. Arce, and R. F. Graveman, "Approximate image message authentication codes," *IEEE Transacitons on Multimedia* **3**(2), 242–252 (2001).
6. C.-Y. Lin and S.-F. Chang, "SARI: Self-authenticaiton-and-recovery image system," *ACM Multimedia* (2001).
7. Q. Sun, S.-F. Chang, M. Kurato, and M. Suto, "A new semi-fragile image authentication framework combining ECC and PKI infrastructure," *ISCAS2002*, Phoneix, USA (2002).
8. P. Golle and N. Modadugu, "Authenticating streamed data in the presence of random packet loss," *Proc. of the NDSS Symposium* (2001). In http://cryptographic.stanford.edu/ pgolle.
9. B. Schneier, *Applied Cryptographicgraphy* (New York, Wiley, 1996).
10. C.-Y. Lin and S.-F. Chang, "Zero-error information hiding capacity for digital images," *Proc. of ICIP* (October 2001).
11. S. Ye, X. Lin, and Q. Sun, "Content based error detection and concealment for image transmission over wireless channel," *ISCAS2003* (May 2003), Thailand.
12. C.-Y. Lin, D. Sow, and S.-F. Chang, "Using self-authentication-and-recovery images for error concealment in wireless environments," *SPIE ITCom* (August 2001).
13. P. Yin, H. Yu, and B. Liu, "Error concealment using data hiding," *International Conference on Acoustic, Speech and Signal Processing, 2001*, Salt Lake City, UT, USA (2001).
14. Y. Wang and Q. Zhu, "Error control and concealment for video communication: A review," *Proc. of the IEEE* **86**(5), 974–997 (1998).

Qibin Sun received his MS and Doctoral degrees, both in Electrical Engineering, from the University of Science and Technology of China, Anhui, China, in 1988 and 1997, respectively.

Since 1996, he is with the Institute for InfoComm Research, Singapore, where he is responsible for industrial as well as academic research projects in the area of face recognition, media security, image and video analysis. He worked in Columbia University during 2000–2001, as a research scientist.

Shuiming Ye received the Master degree and Bachelor degree in 2002 and 1999, respectively, in the department of Electronical Engineering of the Tsinghua University, China.

He is currently pursuing the PhD degree in the School of Computer, National University of Singapore, Singapore. His research interests include multimedia security, transmission and
1 processing.

Ching-Yung Lin received the BS and MS degrees from the National Taiwan University in 1991 and 1993, respectively, and his PhD degree from Columbia University in 2000, all in Electrical Engineering.

Since 2000, he has been a Research Staff Member in IBM T. J. Watson Research Center, New York. His current research interests include multimedia understanding and multimedia security. Dr. Lin is the author/co-author of 60 journal articles, conference papers, and public release software. He holds three US patents and seven pending patents in the fields of multimedia security and multimedia understanding.

Shih-Fu Chang (http://www.ee.columbia.edu/ sfchang) is currently a Professor at the Department of Electrical Engineering of Columbia University. He leads Columbia University's Digital Video/Multimedia Lab (http://www.ee.columbia.edu/dvmm) and ADVENT industry-university consortium, conducting research in multimedia indexing, pervasive media, and media rights management. In addition to developing new theories and algorithms, he is also interested in applying video technology to various domains, such as a video digital library currently funded by the 5-year NSF DLI-2 initiative, a Digital News project, and a live sports video filtering project. Through collaboration with industry partners, his group has made major contributions to the development of MPEG-7 multimedia description schemes and the TREC video benchmark events. Dr. Chang actively participates in professional activities. He served as a general co-chair of ACM 8th Multimedia Conference 2000 and will participate as a Conference Co-Chair in IEEE ICME 2004. He has been a consultant in several media technology companies, and a Distinguished Lecturer in IEEE Society of Circuits and Systems. He has received a Young Investigator Award from Navy ONR, a Faculty Development Award from IBM, a CAREER Award from National Science Foundation, and three Best Paper Awards from IEEE, ACM, and SPIE in the areas of multimedia indexing and manipulation. He has also supervised
3 several research works receiving best student paper awards in recent years.