Digital Watermarking Scheme Exploiting Non-deterministic Dependence for Image Authentication

Chang-Tsun Li and Yinyin Yuan

Department of Computer Science
University of Warwick
Coventry, CV4 7AL, UK
{ctli, yina@dcs.warwick.ac.uk}

ABSTRACT

Watermarking schemes for authentication purposes are characterized by three factors namely security, resolution of tamper localization, and embedding distortion. Since the requirements of high security, high localization resolution, and low distortion cannot be fulfilled simultaneously, the relative importance of a particular factor is application-dependent. Moreover, block-wise dependence is recognized as a key requirement for fragile watermarking schemes to thwart the Holliman-Memon counterfeiting attack. However, it has also been observed that deterministic dependence is still susceptible to transplantation attack or even simple cover-up attack. This work is intended to propose a fragile watermarking scheme for image authentication, which exploits non-deterministic dependence and provides the users with freedom of making trade-offs among the three factors according to the needs of their applications.

Keywords - fragile watermarking, image authentication, integrity verification, multimedia security

1. INTRODUCTION

In recent years, researchers have spent enormous amount of effort investigating digital watermarking schemes to meet the needs of copyright protection and authentication of multimedia. Usually, the schemes for copyright protection [2, 12, 14] are typically *robust* in the sense that the embedded watermark is expected to be preserved provided the host media is still valuable after manipulation. On the contrary, the schemes for authentication and verification of content integrity [1, 3-9, 11, 15, 16] are usually (*semi*) *fragile* in the sense that, when attacked, the embedded watermark should be entirely or locally destroyed, depending on whether the attack is a global or local tampering, so that alarms can be raised when wrong watermark is extracted. This work is intended to address the issues of fragile watermarking schemes and to propose a novel scheme for authentication purposes.

Fragile watermarking schemes for authentication purposes often find their applications in medical, forensic, broadcasting, and military applications where content verification and identity authentication are of the main concern. It is desirable that the watermarking scheme should not only be able to verify the authenticity and content integrity of the image, but also to locate the positions where tampering has taken place so that possible intention of the attacker can be interpreted. It is also important that the embedding operation should not introduce noticeable distortion to the host image. Therefore, fragile watermarking schemes are characterized by three factors namely security, resolution of tamper localization, and embedding distortion.

While low distortion and high resolution of tamper localization are important, the key concern of an authentication scheme is security. A fragile watermarking scheme must show no security gaps to attacks such as cover-up / cut-and-paste [1] and the Holliman-Memon counterfeiting attack [6] (also known as birthday attack [1], vector quantization attack [16], or collage attack [3, 4]).

Cover-up attack is the operation of cutting one region / block of the image and pasting it somewhere in the same or another image. The Holliman-Memon counterfeiting attack / birthday attack is devised on the basis of the so-called birthday paradox [13, Appendix 8.A]. According to birthday paradox, using a hash function that produces a bit string of length l, the probability of finding at least two blocks that hash to the same output is greater than 0.5 whenever roughly $2^{l/2}$ watermarked blocks are available. The idea of the attack is to forge a new watermarked image (a collage) from a number of authenticated images watermarked with the same key and watermark / logo by combining portions of various authenticated images while maintaining their relative positions in the forged version. Fridrich *et al.* [3, 4] showed that, provided a larger number of images watermarked with the same key are available, counterfeiting is possible even when the logo is not known to the attacker.

Block-wise dependence is accepted as an essential requirement to combat the Holliman-Memon counterfeiting attack / birthday attack [1, 3-11, 15]. However, it has also been shown that with deterministic dependence, i.e., the information involved or dependent upon is deterministic, is susceptible to 'transplantation attack' or even simple cover-up attack [1, 8-10]. The 'transplantation attack' derived by Barreto *et al*. [1] works as follows. Let $f'_A \rightarrow f'_B$ denote that the hashing or the calculation of some sort of signature of block f'_B depends on the information about f'_A. Now, for two arbitrary images, f' and f'', with block f'_A identical to f''_A, f'_B identical to f''_B, and f'_C identical to f''_C, but f'_X not identical to f''_X, if the following dependence relationships exist

$$\ldots \rightarrow f'_A \rightarrow f'_X \rightarrow f'_B \rightarrow f'_C \rightarrow \ldots$$

$$\ldots \rightarrow f''_A \rightarrow f''_X \rightarrow f''_B \rightarrow f''_C \rightarrow \ldots$$

then the block pairs (f'_X, f'_B) and (f''_X, f''_B) can be swapped without being detected by schemes such as [15, 17] adopting deterministic dependence. Merely increasing the number of dependencies could

not thwart this type of transplantation attack. For example, let $f_A \leftrightarrow f_B$ denote that the hashing of each block depends on the information about the other. Now if the following dependence relationships exist

$$\cdots \leftrightarrow f'_A \leftrightarrow f'_B \leftrightarrow f'_X \leftrightarrow f'_C \leftrightarrow f'_D \leftrightarrow \cdots$$

$$\cdots \leftrightarrow f''_A \leftrightarrow f''_B \leftrightarrow f''_X \leftrightarrow f''_C \leftrightarrow f''_D \leftrightarrow \cdots,$$

the triplets (f'_B ,f'_X , f'_C) and (f''_B ,f''_X , f''_C) are interchangeable without raising alarm if block f'_D is also identical to f''_D. In the light of the threat posed by the transplantation attack, non-deterministic dependence has to be imposed as a key requirement on the watermarking schemes. This is one of the key motivations of this work

Since the requirements of high security, high resolution of tamper localization, and low embedding distortion cannot be fulfilled simultaneously, the relative importance of a particular factor is application-dependent. It is therefore desirable to provide the users with the flexibility of making trade-offs among the three factors to suit the needs of their application. This is another key motivation behind the proposed scheme.

The rest of this work is organized as follows. The merits and limitations of some related works are reviewed and discussed in Sec. II. A new scheme is proposed and analyzed in Sec. III. Experiments are conducted in Sec. IV to test the proposed scheme. Finally, conclusions are drawn in Sec. V.

2. RELATED WORKS

Generally speaking, fragile watermarking schemes can be classified into three categories according to the level of dependence on the contextual information.

Level 1: Schemes such as the Yeung-Minzter [17] and Wong's schemes [15], in which embedding process does not involve any dependence information, fall into this category. The lack of block-wise dependence in these schemes makes forgery an easy task. For example, a fake image with valid watermark can be constructed by swapping blocks of the authentic images in a database, which are watermarked with the same scheme using the same watermark or key.

Level 2: Schemes such as [7] and the hash block chaining scheme (HBC1) of [1] that exploit deterministic dependence by making the signature relying on the contextual information from the neighboring pixels/blocks belong to this category. Watermarked with this type of scheme, when an image block is subjected to the Holliman-Memon counterfeiting attack, the watermark detector would not be able to derive valid signature or watermark from the blocks dependent on the attacked one and, as a result, alarms in association with those blocks could be raised. For example, in [7], Li *et al.* proposed to use a binary feature map extracted from the underlying image as watermark and divide the watermark into blocks. Then the right half of each watermark block is replaced with the right half of the next block in zigzag scanning path before encrypting and embedding into the LSBs of the image. Nevertheless, the dependence with deterministic context is still susceptible to the transplantation attack.

Level 3: Schemes such as [5, 8, 9] and HBC2 of [1] that place randomly chosen parameters as well as the contextual information from the neighboring blocks to form a non-deterministic signature are of this level. By involving random/non-deterministic parameters in the dependence context, the signature of two identical image blocks will be different, thus, providing further resistance against transplantation attack.

However, one common limitation of the three categories of schemes is that they do not provide the users with the flexibility of making trade-offs among security, resolution of tamper localization,

and embedding distortion to meet the needs of their application. Moreover, the scheme of [5] is not able to detect the cropping on the right and/or from the bottom of the watermarked image because none of the pixels on the right or below the pixel to be watermarked is involved in the watermarking process. Li and Yang proposed a 1-D neighborhood forming strategy [9] to tackle this problem by involving x pixels ahead of the pixel to be marked in the zigzag order because the direction of the zigzag-scanning path is not constant. However, one disadvantage of the scheme is that the process of turning off the false alarms is not efficient due to the variable shape of the dependence neighborhood.

3. PROPOSED WORK

In this work we propose a new scheme in attempt to overcome the aforementioned problems. The proposed scheme can be employed for watermarking color and gray scale images. Without loss of generality, throughout the rest of this work we will assume that we are working with gray scale images with 8 bits per pixel. Symbols are defined as follows.

f: the original image of M pixels with the gray scale of its ith pixel denoted as $f(i)$

b: the number of watermarkable bits of each pixel

f': the image received by the watermark detector.

w: the secret-key generated watermark image of the same dimensions as the original image f, with the gray scale of its ith pixel denoted as $w(i)$ that consist of only b bits (i.e., $w(i) \in [0, 2^b\text{-}1]$, $b < 8$)

w': the extracted watermark image by the decoder with the gray scale of its ith pixel denoted as $w'(i)$

$N(i)$: the square dependence neighborhood centered at pixel i of an image consisting of $k \times k$

pixels including pixel i itself

$S(i)$: the secret non-deterministic dependence information of pixel i extracted from $N(i)$ according to Eq. (1) expressed as follows:

$$S(i) = \sum_{j \in N(i)} (-1)^{w(i)+w(j)} \left\lfloor \frac{f(j)}{2^b} \right\rfloor \quad (1)$$

Note that performing the *floor* function $\lfloor \bullet \rfloor$ after dividing $f(i)$ by 2^b is intended to involve only the $8 - b$ bits of $f(i)$, which are not affected throughout the embedding process, in the calculation of $S(i)$.

D: the binary *difference map* between w and w' with its ith pixel denoted as $D(i)$ ($D(i) \in \{0, 255\}$) indicating whether $w(i)$ and $w'(i)$ are different. Wherever the watermarked image is manipulated, noises are shown in the corresponding portion of the difference map D.

A: the binary *authenticity map* with its ith pixel denoted as $A(i)$ ($A(i) \in \{0, 255\}$) created by turning the false alarms and missed alarms (false authenticity) of D off and on, respectively.

3.1 Watermark Embedding Algorithm

Step_e 1. Specify the number of watermarkable bits b of each pixel and the size ($k \times k$ pixels) of $N(i)$ agreed with the watermark detector.

Step_e 2. Generate a watermark image w of the same dimensions as the original image f with the secret key shared with the watermark detector

Step_e 3. For each pixel i of the original image f

Step_e 3.1. Calculate the secret dependence information $S(i)$ according to Eq. (1)

Step_e 3.2. Use $S(i)$ as the seed of a random number generator to generate an integer $v(i)$ in the range of $[0, 2^b\text{-}1]$

Step$_e$ 3.3. Adjust the b least significant bits of $f(i)$ so that

$$v(i) \oplus (f(i) \bmod 2^b) = w(i), \tag{2}$$

where $\oplus$ is the symbol of EXCLUSIVR-OR operation.

An example of the embedding operation in Step$_e$ 3.3 is as follows: Suppose $b = 2$ (i.e. we allow 2 LSBs to be watermarked), $v(i) = 2 = (10)_2$, $w(i) = 0 = (00)_2$, $f(i) = 129 = (10000001)_2$. Then the left-hand side of Eq. (2) is

$$\begin{aligned} v(i) \oplus (f(i) \bmod 2^b) &= (10)_2 \oplus (129 \bmod 2^2) \\ &= (10)_2 \oplus (01)_2 \\ &= (11)_2 \end{aligned}$$

, which is not equal to $w(i)$ on the right-hand side of Eq.(2). In order to embed the watermark by satisfying Eq. (2), $f(i)$ has to be changed from 129 to 130. This can be proved by substituting 130 for $f(i)$ in Eq. (2). Note if the original $f(i)$ satisfies Eq. (2) no change to $f(i)$ is necessary.

3.2 Watermark Detection Algorithm

Step$_d$ 1. Specify the number of watermarkable bits b of each pixel and the size ($k \times k$ pixels) of $N(i)$ agreed with the watermark embedder.

Step$_d$ 2. Generate a watermark image w of the same dimensions as the received image f' with the secret key shared with the watermark embedder

Step$_d$ 3. For each pixel i of the received image f'

Step$_d$ 3.1. Calculate the secret dependence information $S(i)$ according to Eq. (1) based on the

received image f'

Step$_d$ 3.2. Use $S(i)$ as the seed of a random number generator to generate an integer $v(i)$ in the range of $[0, 2^b-1]$

Step$_d$ 3.3. Extract watermark bit $w'(i)$ according to Eq. (3) defined as follows

$$w'(i) = v(i) \oplus (f'(i) \bmod 2^b) \tag{3}$$

Step$_d$ 3.4. Calculate the *binary* difference $D(i)$ between $w(i)$ and the extracted watermark $w'(i)$ using Eq. (4)

$$D(i) = \begin{cases} 0 & , w'(i) = w(i) \\ 255 & , \text{Otherwise} \end{cases} \tag{4}$$

Step$_d$ 4. Turn on/off the missed alarms/false alarms according to Eq (5) to create the *authenticity map A* such that

$$A(i) = \begin{cases} 0 & , Black(i) > \alpha |N(i)| \\ 255 & , Black(i) \le \alpha |N(i)| \end{cases} \tag{5}$$

where $|N(i)|$ is the cardinality or size of $N(i)$ and *Black(i)* is a function returning the number of *black* pixels (the pixels with gray scale equal to 0) in the neighborhood $N(i)$ of pixel i of the difference map D and $1/2^b < \alpha \le 1$. Appropriately chosen value of α makes the noisy areas shrink while filling up the interior of them. The purpose of this post-processing step is detailed in the next subsection.

3.3 Algorithm Analyses

3.3.1 Post-processing

There are two possible authentication errors namely *false alarm* and *false authenticity* (*missed alarm*) in the difference map D. The false alarm is the result of the involvement of $N(i)$ and appear outside the actual tampered area making it looks bigger than it actually is. This is because, for any authentic pixel i, if any one of its neighbors in $N(i)$ is tampered with, pixel i will be deemed inauthentic with a probability of $1- 1/2^b$. Therefore, the larger the dependence neighborhood $N(i)$ is, the lower the resolution of tamper localization becomes. Reducing the size of $N(i)$ would increase the resolution of tamper localization. However, this is achieved at the expense of security since smaller dependence neighborhood provides lower security. It is therefore desirable to turn the false alarms off in order to improve the localization accuracy without reducing the size of $N(i)$ and compromising the security.

On the other hand, according to Eq. (1), tampering the watermarked image changes $S(i)$. However, according to Eq. (3), for each individual pixel i, new $S(i)$ could still produce the same/correct $w'(i)$ with a probability of $1/2^b$. (Note that for the schemes reported in [1, 4, 5, 7, 9, 10, 15-17] this probability is as high as 0.5 because they only watermark the least significant bit, i.e., $b = 1$.) Although turning the missed alarms on does not make significant contribution, it could make the tampered areas look more 'solid', thus, creating clearer indication of tampering.

Step_d 4 of the watermark-detecting algorithm is intended to serve the purpose of turning the false alarms and missed alarms (false authenticity) off and on, respectively.

3.3.2 Balancing security, resolution, and distortion

Embedding more bits into each pixel would certainly introduce more distortion to the watermarked image. However, this also introduces more secret information into the media thus providing higher security. In the cases where the user requires higher resolution of tamper localization and could afford higher distortion, the requirement can be met by watermarking more bits per pixel (i.e., using greater value of b in the algorithm) and involving smaller dependence neighborhood $N(i)$ without compromising the security. Another advantage of using greater value for b is that the probability of missing alarm is lower ($1/2^b$).

3.3.3 Calculating dependence information

There are various ways for calculating $S(i)$. For example, Barreto *et al*. proposed to hash the gray scales of the pixels with the dependence neighborhood appended with some random numbers [1]. In this work, we propose to calculate $S(i)$ according to Eq (1). With the inclusion of $w(i)$ and $w(j)$ in Eq (1), even two identical dependence neighborhoods would yield different $S(i)$s because their corresponding watermarks are different. This feature makes the proposed algorithm immune to transplantation attack without resorting to the relatively compute-intensive hashing operation as in [1]. At first glance, manipulating any one of 8 - b most significant bits (MSBs) of $f(i)$ makes no difference in the result of the operation of $f(i)$ mod 2^b in Eq. (2) and therefore could defeat the proposed scheme. However, this is not true because the 8- b MSBs of $f(i)$ have already been involved in the calculation of $S(i)$ in Eq. (1), which in turn generates $v(i)$ used in Eq. (2). Therefore, this kind of attack will not pass the authentication.

4. EXPERIMENTS

To demonstrate the imperceptibility of the proposed scheme we applied the scheme to four test images and listed the embedding distortion (PSNR) measured in dB in Table 1. We can see that even when $b = 3$ (i.e. we allow the first 3 LSBs to be watermarked), the PSNRs are still higher than 37.9 dB. This feature is visualized in Figure 1. Figure 1(a) shows the original image of F16 while Figure 1(b), 1(c), and 1(d) show the images watermarked with the proposed scheme with the size of the neighborhood $N(i)$ equal to 5 × 5 pixels and the number of watermarkable bits b equal to 1, 2, and 3, respectively. In all cases, the distortion is not noticeable to human visual system (PSNR equal to 51.1, 44.2, and 37.9 dB, respectively).

Figure 2(a) illustrates the attacked version of the watermarked image ($b = 1$) of Figure 1(b) with the characters on the fuselage of the jet fighter removed. Figure 2(b) highlights the exact corresponding region, the 'ground truth', which has actually been tampered with. The difference map D in Figure 2(c) indicates the authentication result with the size of the neighborhood $N(i)$ equal to 5 × 5 before post-processing. Figure 2(d) illustrates the final *authenticity map A* after post-processing with α equal to 0.7. The difference map D in Figure 2(e) indicates the authentication result with the size of the neighborhood $N(i)$ equal to 9 × 9 before post-processing. Figure 2(f) illustrates the final *authenticity map A* after post-processing with α equal to 0.7.

Figure 3 shows the authentication results with the number of watermarkable bits $b = 3$ subjected to the same local manipulation applied to Figure 2(a). Figure 3(a) is the difference map D with the size of the neighborhood $N(i)$ equal to 3 × 3. Figure 3(b) illustrates the *authenticity map A* after the post-processing was applied to Figure 3(a) with $\alpha = 0.25$. Figure 3(c) demonstrates the difference map D with $N(i)$ equal to 9 × 9. The *authenticity map A* after post-processing with α =

0.25. We can see the difference in terms of the resolution of tamper localization between Figure 3(a) and (c). By comparing the difference between Figure 3(c) and (d), the significant improvement on the resolution of tamper localization made by the post-processing in $Step_d$ 4 can be clearly seen.

To demonstrate the proposed scheme's capability of thwarting the vector quantization attack, we first watermarked four images: 1) the original image of Lena; 2) image of Lena with the LSB plane flipped. (d) image of Lena with the second LSB plane flipped; 4) image of Lena with the 2 LSB planes flipped. An image as shown in Figure 4(a) is then forged with its four quadrants taken from the four watermarked images. The difference map in Figure 4(b) shows that the image in Figure 4(a) is actually a fake. The reason the "noise cross" appear in the difference map is because that along the boundaries of the four quadrants, wrong pixels enters the dependence neighborhood of the pixels to be authenticated, which disturb the dependence relationship. The noises appearing along the borders of the difference map is due to the fact that when establishing the dependence neighborhood we allow the image to "wrap around", i.e. the pixels along the left (upper) border of the image are treated as neighbors of the pixels along the right (bottom) border, and vice versa. This feature of "wrap around" allows the scheme to put up resistance against cropping attack.

5. CONCLUSIONS

In this work, we reviewed some previous watermarking schemes to identify their merits and limitations. Based on their limitations and given the challenges fragile watermarking schemes face, we propose a simple yet powerful scheme with its security relying on non-deterministic dependence information. Effectiveness of this scheme is shown in the experiments. The main merits of the proposed scheme are:

- It can resist the existing attacks such as cut-and-paste, the Holliman-Memon counterfeiting

attack, and transplantation attack due to the merit of non-deterministic dependence.

- The balance between security, tamper localization, and embedding distortion can be adjusted by varying the size of the neighbourhood and the number of watermarkable bits according to the needs of the applications.
- The post-processing scheme offers a way of enhancing localization resolution without compromising security.
- Involving the neighbouring pixels in all directions in the dependence neighbourhood centred at the pixel to be marked allows the scheme to detect cropping on any sides of the image along any directions.

6. REFERENCES

[1] P. S. L. M. Barreto, H. Y. Kim, and V. Rijmen, "Toward secure public-key block-wise fragile authentication watermarking," in *IEE Proceedings - Vision, Image and Signal Processing*, 148(2), 57 – 62 (2002).

[2] A. G. Bors and I. Pitas, "Image watermarking using block site selection and dct domain constraints," *Optics Express*, 3(12), 512-522 (1998).

[3] J. Fridrich, M. Goljan, and N. Memon, "Cryptanalysis of the yeung–mintzer fragile watermarking technique," *Journal of Electronic Imaging*, 11(2), 262-274 (2002).

[4] J. Fridrich, "Security of fragile authentication watermarks with localization," in *Proc. SPIE Security and Watermarking of Multimedia Contents*, VI, 691-700 (2002).

[5] J Fridrich, M. Goljan and A.C. Baldoza, "New fragile authentication watermark for images," in *Proc. IEEE International Conference on Image Processing*, 694-697 (2000).

[6] M. Holliman and N. Memon, “Counterfeiting attacks on oblivious block-wise independent invisible watermarking schemes,” *IEEE Trans. Image Processing,* vol. 9, no. 3, pp. 432-441, March 2000.

[7] C.-T. Li, D. C. Lou, and T. H. Chen, “Image authenticity and integrity verification via content-based watermarks and a public key cryptosystem,” in *Proc. IEEE Int. Conf. Image Processing,* vol. III, Vancouver, Canada, Sept. 2000, pp. 694-697.

[8] C.-T. Li, “Digital fragile watermarking scheme for authentication of jpeg images,” *IEE Proceedings - Vision, Image, and Signal Processing*, 151(6), 460 – 466 (2004).

[9] C.-T. Li and F.-M. Yang, "One-dimensional neighborhood forming strategy for fragile watermarking," *Journal of Electronic Imaging*, 12(2), 284-291 (2003).

[10] C.-T. Li, "Digital watermarking for multimedia authentication," in *Digital Watermarking for Digital Media*, ed. by J. Seitz, Idea Group Publishing (2005).

[11] A. H. Ouda and M. R. El-Sakka, “Localization and security enhancement of block-based image authentication,” in *Proc. IEEE Int. Conf. Image Processing*, I, 673-676 (2005).

[12] J.-M. Shieh, D.-C. Lou, and M.-C. Chang, “Highly robust watermarking scheme based on surrounding mean value relationship,” *Optical Engineering*, 44,(6), 897-907 (2005)

[13] W. Stallings, *Cryptography and network security – Principles and practice,* Prentice Hall, (1998).

[14] K. Su, D. Kundur and D. Hatzinakos, “Spatially localized image-dependent watermarking for statistical invisibility and collusion resistance,” *IEEE Trans. on Multimedia*, 7(1), 52 - 66 (2005).

[15]P. W. Wong and N. Memon, "Secret and public key image watermarking schemes for image authentication and ownership verification," *IEEE Trans. On Image Processing,* 10(10), 1593 - 1601 (2001).

[16]P. W. Wong and N. Memon, "Secret and public key authentication watermarking schemes that resist vector quantization attack," in *Proc. SPIE Security and Watermarking of Multimedia Contents* II*,* 40-47 (2000).

[17]M. Yeung and F. Minzter, "Invisible watermarking for image verification," *Journal of Electronic Imaging*, 7(3), 578-591 (1998).

BIOGHRAPHIES

Chang-Tsun Li received the B.S. degree in electrical engineering from Chung-Cheng Institute of Technology (CCIT), National Defense University, Taiwan, in 1987, the M.S. degree in computer science from U. S. Naval Postgraduate School, U.S.A., in 1992, and the Ph.D. degree in computer science from the University of Warwick, U.K., in 1998. He was an associate professor during 1999-2002 in the Department of Electrical Engineering at CCIT and a visiting professor in the Department of Computer Science at U.S. Naval Postgraduate School in the second half of 2001. He is currently a lecturer in the Department of Computer Science at the University of Warwick, U.K. His research interests include image processing, pattern recognition, computer vision, multimedia security, and content-based image retrieval.

Yinyin Yuan received her master degree from the University of Warwick in 2005 and her Bachelor degree from the University of Science and Technology of China in 2003, both in the discipline of Computer Science. She is now a PhD candidate in the Department of Computer Science, University of Warwick. Her research interests are in the fields of digital watermarking, medical image processing and genomic signal processing.

Table 1. Embedding distortion measured in PSNR inflicted on the test images with different number of watermarkable bits *b*.

b	PSNR(dB)			
	F16	Mandrill	Lena	Camera man
1	51.1476	51.1773	51.1370	51.1565
2	44.1531	44.1349	44.1489	44.1536
3	37.9072	37.9180	37.8996	37.9522

FIGURE CAPTIONS

Figure 1. (a) The original image (b) The watermarked image with the number of watermarkable bits $b = 1$ and PSNR at 51.1 dB. (c) The watermarked image with $b = 2$ and PSNR at 44.1 dB. (d) The watermarked image with $b = 3$ and PSNR at 37.9 dB. The size of $N(i)$ is equal to 5×5 pixels in all cases.

Figure. 2. (a) The tampered version of Figure 1(b) with the characters on the jet fighter removed. (b) The actual region tampered with. (c) The difference map D with the size of the neighborhood $N(i)$ equal to 5×5. (d) The *authenticity map A* after post-processing with $\alpha = 0.7$. (e) The difference map D with the size of the neighborhood $N(i)$ equal to 9×9. (f) The *authenticity map A* after post-processing with $\alpha = 0.7$.

Figure 3. Authentication results with the number of watermarkable bits $b = 3$ subjected to the same local manipulation as shown in Figure 2(b). (a) The difference map D with the size of the neighborhood $N(i)$ equal to 3×3. (b) The *authenticity map A* after post-processing with $\alpha = 0.25$. (c) The difference map D with the size of the neighborhood $N(i)$ equal to 9×9. (d) The *authenticity map A* after post-processing with $\alpha = 0.25$.

Figure 4. Vector quantization attack. (a) A forged image with its four quadrants taken from four slightly different and authentic images watermarked with the proposed scheme. (b) Difference map shows that the image is actually a collage made of four blocks taken from different images.

F16
U.S.AIR FORCE

F16
U.S.AIR FORCE

F16
U.S.AIR FORCE

F16
U.S.AIR FORCE