IMAGE AUTHENTICATION AND RECOVERY USING WAVELET-BASED DUAL WATERMARKING

Radu Ovidiu PREDA[1], Ioana MARCU[2], Amelia CIOBANU[3]

In this paper a novel watermarking scheme for image authentication and recovery is presented. The algorithm can detect modified regions in images and is able to recover a good approximation of the original content of the tampered regions. For this purpose, two different watermarks have been used: a semi-fragile watermark for image authentication and a robust watermark for image recovery, both embedded in the Discrete Wavelet Transform domain. The proposed method achieves good image quality with mean Peak Signal-to-Noise Ratio values of the watermarked images of 42 dB and identifies image tampering of up to 20% of the original image.

Keywords: multimedia security, image forgery detection, digital watermarking, image authentication, image recovery, Discrete Wavelet Transform

1. Introduction

Digital content, such as images, video and audio can be easily copied and distributed through different communication channels. The availability of powerful signal processing tools makes it very difficult to guarantee the integrity of multimedia content. Digital images are used in legal disputes involving tampered pictures published in newspapers and magazines, accidents, political or celebrity scandals, etc. Under these circumstances, in order to prevent malicious, intentional tampering, image authentication has become a very important and challenging issue in the digital world. One of the best solutions for image authentication is digital watermarking, a process by which a user specified signal (watermark) is hidden or embedded in the original image.

A great number of scientific publications in this field only authenticate the content of digital images and are not able to reconstruct the original content [1-6]. Most techniques use fragile watermarks for authentication [3-7]. These watermarks can detect malicious altering of the image content, but are also destroyed even after the smallest unintentional modification, an undesired property in most applications. Compared to these methods, the technique

[1] Assoc. Prof., Telecommunications Dept., University POLITEHNICA of Bucharest, Romania, e-mail: radu@comm.pub.ro
[2] Lect., Telecommunications Dept., University POLITEHNICA of Bucharest, Romania
[3] Lect., Telecommunications Dept., University POLITEHNICA of Bucharest, Romania

proposed in this paper uses a semi-fragile authentication watermark, which is able to withstand a good degree of common image processing.

Many other semi-fragile authentication techniques use block-based approaches in the spatial or Discrete Cosine Transform (DCT) domain to detect the tampered regions [6, 8, 9]. Most of these schemes are vulnerable to counterfeiting attacks, like the Vector Quantization (VQ), and the tamper detection resolution is limited to the block size. Smaller block sizes and higher watermark payloads are necessary to improve the detection resolution, resulting in a considerable degradation of the image quality. To alleviate these problems, the technique proposed in this paper uses Wavelet coefficients permuted with a random key to embed the authentication watermark, protecting the scheme against local attacks. The embedding of the authentication watermark in the Wavelet domain also assures a better detection resolution than block-based methods.

Another desired property of an authentication scheme is the ability to recover the original content of the detected tampered regions. Only a small percentage of the existing algorithms are able to do this, because it comes with a trade-off: the use of a second watermark, the recovery watermark, an approximation of the original image with high payload, results in further degradation of the image quality [10-12]. Different recovery schemes try to reduce the payload of this watermark using compression. In [13], Chamlawi et al. use a highly compressed version of the original image as a recovery watermark, obtained by applying the DCT to the second level Wavelet approximation sub-band, and embed this watermark in some middle frequency Wavelet coefficients. This approach is fragile to any kind of image processing operation and also to large content altering modifications and is not able to recover the digest image. A recovery scheme with better results is proposed in [14], where the digest image is compressed using arithmetic coding and protected by applying a Bose-Chaudhuri-Hocquenghem (BCH) error correcting code. This watermark is embedded in the middle sub-band detail Wavelet coefficients using a Least Significant Bit (LSB) approach. The error correction code increases the watermark payload and degrades the image quality and, even if it is able to correct some errors produced by salt&pepper noise in the extracted arithmetic code, the LSB method is quite fragile to any modifications.

Most of the existing recovery schemes use either a fragile recovery watermark (highly compressed version of the original image) [13], [15, 16], or a fragile embedding strategy, like LSB embedding [4], [9], [14], [17]. Because the recovery strategy must be as robust as possible to any kind of modification of the image, these methods do not produce satisfactory results. The recovery algorithm proposed in this paper achieves not only good robustness to common signal processing operations, but also to large malicious tampering of the image.

The paper is organized as follows: in Sections 2 and 3 the proposed image authentication and recovery scheme is presented, including the block diagrams of the watermark embedder and decoder and the detailed steps of the algorithm. Section 4 contains the experimental results and performances of the proposed scheme in terms of image quality, detection, localization and recovery capability and robustness to common image processing operations. Conclusions are given in Section 5.

2. The proposed dual watermark encoding scheme

The block diagram of the embedding scheme, given in Figure 1, consists of two main blocks, for generating and embedding the two different watermarks, the authentication and recovery watermark. These procedures are described in the following.

2.1. Generation and embedding of the authentication watermark

The authentication watermark generation and embedding procedure is presented in the lower half on Figure 1 and is described in the following:

- A two level bi-dimensional Discrete Wavelet Transform (2D-DWT) is used to transform the original, grayscale image in the Wavelet domain.
- The detail Wavelet coefficients of the LH_2, HL_2 and HH_2 Wavelet sub-bands of the second Wavelet decomposition are selected for embedding the authentication watermark. By selecting higher resolution sub-bands for watermark embedding the algorithm achieves a better localization of intentional tampering.

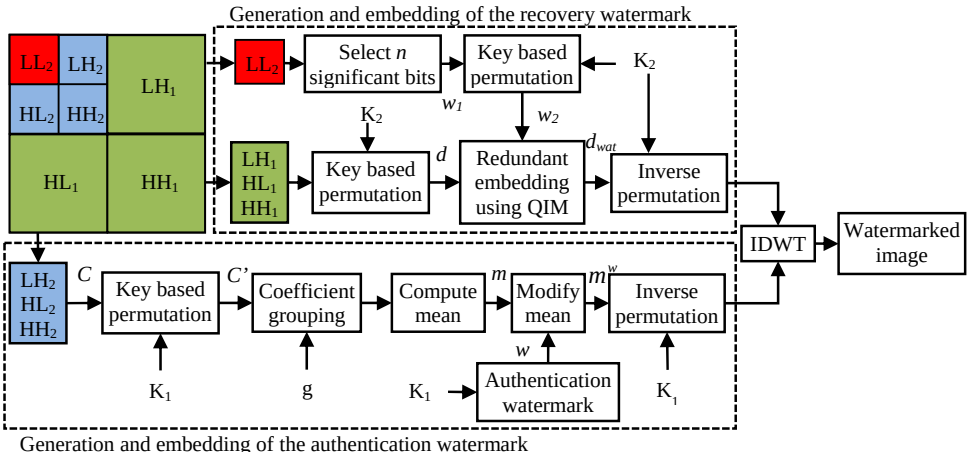

Fig. 1. The proposed watermark embedding scheme

- Vector C containing the Wavelet coefficients of the three sub-bands is randomly permuted with the use of a secret key K_1 into a vector C'. This permutation ensures the separation of coefficients from the same spatial location.
- C' Is divided into groups of g coefficients, where g controls the watermark capacity of the scheme. A bit of the authentication watermark will be embedded in every group of g coefficients. The use of a smaller group size will have a bigger watermark payload and thus a higher degradation of the image quality as an effect, but, on the other hand, it will not decrease the detection resolution.
- The authentication watermark is a binary random sequence w, generated based on a secret key K_1 and has the same length as the number of coefficient groups.
- The weighted mean m_i of a group i of permuted wavelet coefficients is calculated according to (1):

$$m_i = \sum_{j=1}^{d} (-1)^j \left| c_i(j) \right| \tag{1}$$

where $c_i(j)$ is the jth coefficient of group I and $(-1)^j$ is the weighting factor used to make the scheme more resilient against common image processing. Such unintentional alterations usually change the entire image content and do not modify the weighted mean.

- To embed a watermark bit w_i in a group of coefficients, the weighted mean m_i is quantized to the nearest even or odd quantization level according to the value of the corresponding watermark bit w_i, using (2).

$$m_i^w = \begin{cases} \lfloor m_i/Q \rfloor \cdot Q & if \ \bmod 2(\lfloor m_i/Q \rfloor) = w_i \\ \lfloor m_i/Q \rfloor \cdot Q + Q & if \ \bmod 2(\lfloor m_i/Q \rfloor) \neq w_i \end{cases}, \tag{2}$$

where m_i^w is the watermarked mean, mod2 is the remainder after division by 2 and $\lfloor . \rfloor$ is the integer part operator.

- The weighted mean m_i of every group i of coefficients is changed to the watermarked mean m_i^w by modifying the Wavelet coefficient $c_{i,\max}(j)$ of the highest magnitude. The random permutation ensures that every group has at least one coefficient with high magnitude. Coefficient $c_{i,\max}(j)$ is modified using (3):

$$c_{i,\max}^w(j) = c_{i,\max}(j) + (-1)^j \cdot sign(c_{i,\max}(j)) \cdot (m_i^w - m_i), \tag{3}$$

with $c_{i,\max}^w(j)$ being the watermarked coefficient and

$$sign(x) = \begin{cases} -1, & if\ x \le 0 \\ 1, & if\ x > 0 \end{cases} \quad (4)$$

- The Wavelet coefficients are shuffled back to their original position using the inverse permutation with the same secret key K_1, obtaining the new watermarked sub-bands LH_2^w, HL_2^w and HH_2^w.

2.2. Generation and embedding of the recovery watermark

The generation and embedding of the recovery watermark are performed in the upper part of Figure 1. The following steps are performed:

- The LL_2 approximation sub-band, is used as the recovery watermark, also called the digest image. It is a reduced version of the original image.
- To further reduce the watermark payload, only the first n most significant bits of every wavelet coefficient from LL_2 are used for embedding. Let w_1 denote the binary watermark vector of length l_{wat}, given in (5), where $M \times N$ is the resolution of the image.

$$l_{wat} = nMN / 16 \quad (5)$$

- To increase the security of the algorithm the vector w_1 is shuffled using a random permutation based on the secret key K_2, obtaining the permuted binary watermark w_2.
- The detail Wavelet coefficients of the LH_1, HL_1 and HH_1 sub-bands are used for embedding the recovery watermark. For security reasons, they are shuffled using a third key K_3, obtaining the vector d of shuffled coefficients of size l_{coef}:

$$l_{coef} = 3MN / 4 \quad (6)$$

- Each bit of the recovery watermark w_2 is redundantly embedded into every coefficient of a group of h coefficients of vector d, where h is obtained using (7):

$$h = \lfloor l_{coef} / l_{wat} \rfloor = \lfloor 12 / n \rfloor \quad (7)$$

- A watermark bit is embedded into a Wavelet coefficient using a Quantization Index Modulation approach, as shown in (8), where d_{wat} is the vector of watermarked coefficients.

$$d_{wat}(ij) = \left\lfloor \frac{d(ij)}{Q} \right\rfloor \cdot Q + \frac{Q}{2} \cdot w_2(i),\ i = \overline{1, l_{wat}},\ j = \overline{1, h} \quad (8)$$

- After the entire watermark has been embedded, an inverse permutation of the watermarked coefficients is done, ensuring that a watermark bit is spread in the entire image. Let LH_1^w, HL_1^w and HH_1^w denote the wavelet sub-bands containing the recovery watermark.

- To obtain the watermarked image, the Inverse 2D-IDWT is applied two times, first on the coefficients of the LL_2, LH_2^w, HL_2^w and HH_2^w sub-bands, obtaining the approximation sub-band LL_1^w, and the second time on the coefficients of the LL_1^w, LH_1^w, HL_1^w and HH_1^w sub-bands.

3. The proposed watermark retrieval scheme

A block diagram of the watermark decoder is given in Figure 2. The upper part of the figure contains the image recovery system and the bottom part contains the blocks to authenticate the image and localize possible intentional tampering.

3.2. Retrieval of the authentication watermark and image authentication

The extraction process of the authentication watermark and the steps for image authentication are described in the following:

- First, the test image undergoes a 2D-DWT decomposition.
- The LH_2, HL_2 and HH_2 Wavelet sub-bands are used to extract the authentication watermark.
- With the use of the secret key K_1, the same random permutation from the encoder side is performed on the vector of watermarked wavelet coefficients.
- The weighted mean m_i' of every group of g coefficients is calculated using (1).

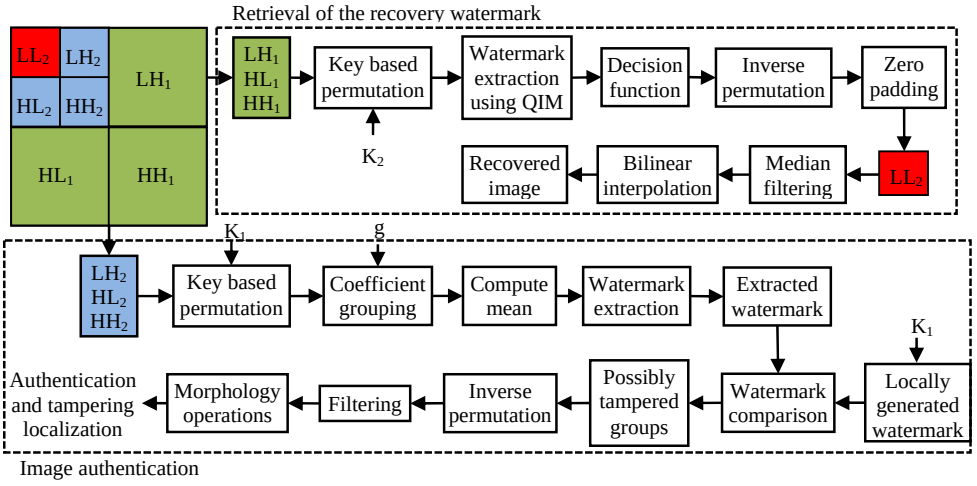

Fig. 2. The proposed watermark decoder and image authentication scheme

- From every mean a watermark bit w_i' is extracted using (9).

$$w_i' = \text{round}\left(\frac{m_i'}{Q}\right) \bmod 2 \tag{9}$$

- Using the secret key K_1, the original watermark w is locally generated and compared to the extracted one. If they match, the image is declared as authentic. If not, the following steps will determine the authenticity and the location of possible tampering.
- If a bit w_i' of the extracted watermark does not match the original one w_i, all coefficients of group i are considered as potentially tampered.
- After permuting all coefficients back to their original position using the secret key K_1, the potentially tampered coefficients should be spread all over the second level detail Wavelet sub-bands. A high density of potentially tampered coefficients should indicate that the corresponding region has been tampered with. Authentic regions, on the other hand, should only contain isolated flagged coefficients, distributed like random noise. These coefficients are false positives and should be considered as authentic.
- As a result, the sub-bands LH_2', HL_2' and HH_2' will contain flagged and non-flagged coefficients. Let **A** be the binary authentication matrix of size $(M/2^2)\times(N/2^2)$, the same size as any of the three sub-bands. If there is a potentially tampered coefficient at position (x, y) in any of the three sub-bands, $\mathbf{A}(x, y)$ will be set to 1.
- To remove the isolated '1' bits from **A**, the authentication matrix will be filtered using both a noise removal filter and successive mathematical morphology operations with a disk of a radius of one pixel as the structural element. The authentication matrix should now contain only regions of clustered flagged positions and should correctly indicate the tampered locations.
- To locate the regions that have actually been tampered with, the flagged positions in matrix **A** are mapped back to the spatial domain.

Every position in authentication matrix **A** of size $(M/2^2)\times(N/2^2)$ indicates an actual region of size 4×4 pixels in the image, which is the maximum detection resolution of this scheme. The quantization step size Q, the filter size and the size of the structural element used for the arithmetic morphology operations can be modified to improve the sensitivity of the tampering detection.

3.2. Retrieval of the recovery watermark

- First, the three detail Wavelet sub-bands LH_1', HL_1' and HH_1' of the first Wavelet decomposition are selected.
- A random permutation with key K_3 of these coefficients is performed on the selected Wavelet coefficients, obtaining a vector d' of shuffled coefficients.
- From every coefficient of vector d', a watermark bit is extracted according to (10), where $w_h'(i)$ is the extracted bit.

$$w_h'(i) = \text{round}\left(\frac{2d'(i)}{Q}\right) \bmod 2,\ i = \overline{1, l_{coef}} \tag{10}$$

- The vector w_h' is divided into groups of h coefficients. The watermark bit $w'(j)$ corresponding to the group j is obtained by majority voting, as in (11):

$$w'(j) = \begin{cases} 0, & \text{if } \sum_{k=h(j-1)+1}^{hj} w_h'(k) \le \frac{h}{2} \\ 1, & \text{if } \sum_{k=h(j-1)+1}^{hj} w_h'(k) > \frac{h}{2} \end{cases}, \quad j = \overline{1, l_{wat}}. \tag{11}$$

- The inverse permutation with key K_2 of vector w' is performed, obtaining w''.
- The binary sequence w'' is divided into groups of n bits and every group is padded with $8-n$ zeroes. Every group of 8 bits represents an extracted Wavelet coefficient of the digest image (LL_2 sub-band). After reordering the coefficients, the recovered image LL_2' of resolution $M \times N / 16$ is obtained.
- To remove the error pixels that could appear in LL_2' because of intentional tampering of the image, a median filter of size 3x3 can be applied.
- Finally, the recovered digest image is obtained by bilinear interpolation of the improved version of LL_2'.

The security of the authentication and recovery system is ensured by three secret keys used to control the generation of the authentication watermark and the random permutations of Wavelet coefficients. There can be distinct keys for these three operations or a single key. An attacker has to know the secret key(s) in order to generate the correct coefficient permutation or a duplicate of the original authentication watermark. Unlike most block-based methods, where the authentication of a block depends only on the content of the block itself, the proposed scheme is rendered immune to the VQ attack by selecting the coefficients of a group randomly from all over the Wavelet sub-bands.

4. Experimental results

We have used 100 images of resolution 512×512 pixels to test the algorithm in terms of quality of the watermarked images, detection and localization capability of the tampering, quality of the recovered images and robustness to common image processing operations.

In Table 1 the image quality and decoding results of the proposed method are shown for different quantization step sizes Q and different group sizes g, where PSNR is the mean Peak Signal to Noise Ratio for 100 test images and BER is the mean decoding Bit Error Rate of the extracted authentication watermark, compared to the original one. The biorthogonal 4.4 Wavelet family has been used, but it can be replaced with any other wavelet family, with minimal impact on the resulting image quality and detection results. The PSNR has good values, above 40 dB, except *for* Q=12, where the mean PSNR drops to 37 dB. For every combination of parameters the authentication watermark can be extracted successfully without any errors.

Next, we have tested the capacity of the proposed approach to detect intentional tampering of the image and recover the tampered regions. For this purpose, we have replaced a region of different sizes of the watermarked image with a region of the same size from another image. This was done for every image in the database. The sizes of the tampered blocks were $16 \times 16, 32 \times 32, 64 \times 64, 128 \times 128$ and 192×192 pixels. After the tampering, the authentication watermark is extracted from the tampered image and the authentication algorithm returns the positions of the tampered regions.

One of the major contributions of this proposed technique is the capability to repair the tampered regions. When a tampered region is detected, the recovery algorithm will recover the content of this region. These unauthentic parts of the image are replaced with the corresponding regions of the recovered digest image.

Table 1

Mean PSNR and BER values

Q	d	PSNR	BER
4	4	46,99	0%
	8	47,51	0%
	12	47,70	0%
8	4	40,95	0%
	8	41,47	0%
	12	41,66	0%
12	4	37,41	0%
	8	37,92	0%
	12	38,11	0%

To measure the image quality of the reconstructed images, we have calculated the mean PSNR values of these images compared to the original ones. The results are shown in Table 2, where all PSNR values are mean values for 100 images. Table 2 also contains the false negative rate (FNR), the percentage of tampered images declared as authentic. We can see, that for small tampering and some embedding parameters, like g=4 and Q=12 we get a small percentage of false negatives, but for most parameters, this percentage is zero.

Fig. 3 shows two examples of image authentication and restoration. The first image is the popular "Lena" grayscale image of size 512×512 pixels and the second image is another test image of resolution 768×512 pixels. Fig. 3a shows the watermarked images using a quantization step size of Q=8 and a group size of g=4. After embedding the watermarked, the "Lena" image has been modified by replacing a region of 64×64 pixels with another region of the same size from the same image (Fig. 3b, left image). The second image has been modified by replacing the face of the woman in the top left region with another woman's face and by removing the beer can and extending the background (Fig. 3b, right image). In Fig. 3c the results of the authentication process are presented, where the white regions denote the detected unauthentic part of the images. The reconstructed images are shown in Fig. 3d. We can see that the proposed algorithm is sensitive to malicious manipulations. It is able to correctly detect the tampered region of the image and to recover the missing information with acceptable quality.

Table 2

Mean PSNR values of the recovered images and false negative rate for different tampering

Q	g	Size of the tampered region									
		16×16		32×32		64×64		128×128		192×192	
		PSNR (dB)	FNR (%)	PSNR (dB)	FNR (%)	PSNR (dB)	FNR (%)	PSNR (dB)	FNR (%)	PSNR (dB)	FNR (%)
4	4	44,18	0,00	41,79	0,00	38,74	0,00	33,27	0,00	29,31	0,00
	8	44,31	0,00	42,21	0,00	38,62	0,00	31,49	0,00	23,13	0,00
	12	44,08	0,00	41,92	0,00	38,56	0,00	23,49	0,00	23,13	0,00
8	4	39,73	10,00	38,57	3,33	37,04	0,00	32,77	0,00	29,03	0,00
	8	40,28	0,00	39,20	0,00	37,27	0,00	32,04	0,00	23,21	0,00
	12	40,45	0,00	39,18	0,00	37,08	0,00	26,89	0,00	23,14	0,00
12	4	36,55	13,33	35,98	3,33	34,97	0,00	31,45	0,00	28,30	0,00
	8	37,26	10,00	36,51	0,00	34,84	0,00	31,62	0,00	23,74	0,00
	12	37,45	10,00	36,61	0,00	35,13	0,00	27,87	0,00	23,19	0,00

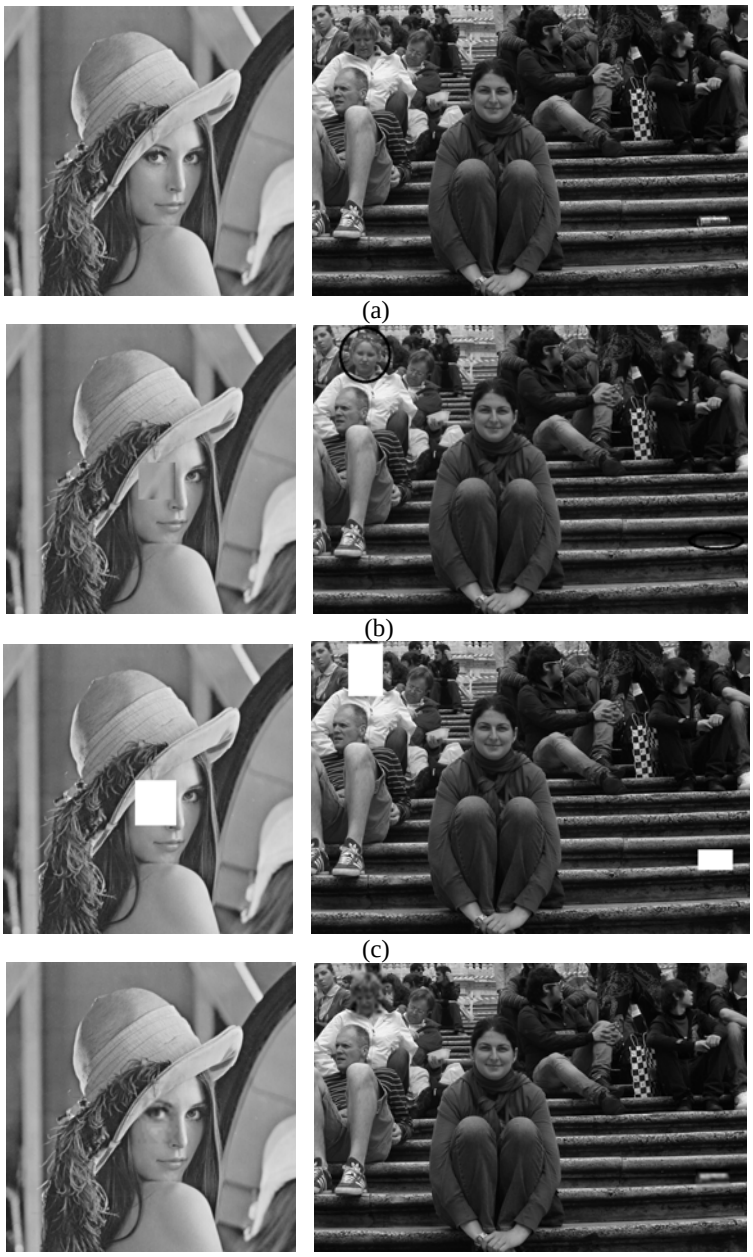

Fig. 3. (a) watermarked images for g=4 and Q=8, (b) tampered images, (b) authenticated images, (d) reconstructed images

Next we have tested the robustness of the proposed technique to mild image processing operations. The authentication watermark is a semi-fragile

watermark, which should be robust to common signal processing operations that preserve the image content, while still being able to detect content altering modification in the image.

To demonstrate this property, two scenarios have been used. First, the original images have been watermarked using the best choice for the embedding parameters (g=4, Q=8) and were modified using the following image processing operations: brightening/darkening (luminance of 40); addition of Gaussian noise of mean 0 and variance 30×10^{-6}; addition of "salt&pepper" noise, where 0.1% of the image pixels were modified; JPEG compression with a quality factor of 85.

Then, the modified images have been authenticated and the false positive rate (FPR) has been experimentally determined for the database of 100 test images. The FPR is the percentage of authentic images that have been declared as unauthentic. Table 3 shows the results for g=4 and Q=8, where all PSNR values in the table are mean values of the watermarked images after applying the image processing operations.

For the second scenario, the images have been watermarked, modified by replacing a region of 64x64 pixels and finally, an image processing operation has been applied. Then, the images have been authenticated, the recovery watermark has been extracted and the original content of the unauthentic regions has been reconstructed. The PSNR values from Table 3 are mean values for the reconstructed images, compared to the original ones. We have also experimentally determined the false negative rates, which are also given in Table 2. The algorithm was able to successfully detect every content altering modification (FPR=0), but a small percentage of authentic images, that have been affected by Gaussian noise, salt&pepper noise and JPEG compression have been falsely declared as unauthentic.

The proposed method has also been compared to two other approaches. Table 4 gives a summary of this comparison. The main advantages of this method, compared to the other techniques, are the good image quality, the good detection resolution of 4x4 pixels for a small payload of the authentication watermark and the robustness to common image processing operations.

Table 3

Robustness of the proposed scheme to common image processing operations

Brightening				Gaussian noise				Salt&pepper noise				JPEG Compression			
No tamp.		64x64		No tamp.		64x64		No tamp.		64x64		No tamp.		64x64	
PSNR (dB)	FPR (%)	PSNR (dB)	FNR (%)	PSNR (dB)	FPR (%)	PSNR (dB)	FNR (%)	PSNR (dB)	FPR (%)	PSNR (dB)	FNR (%)	PSNR (dB)	FPR (%)	PSNR (dB)	FNR (%)
40,95	0,00	21,62	0,00	40,95	6,67	30,86	0,00	40,95	10	32,52	0,00	40,95	6,67	24,45	0,00

Table 4

Comparison to other techniques

Technique	Image quality for average parameters	Detection resolution	Robustness to common image processing	Image recovery possible after removing
[13]	36,65 dB	4x4	Yes (only authentication watermark)	Up to 5% of original
[14]	39,88 dB	8x8	Only to salt&pepper noise	Up to 10% of original
Proposed	39,73 dB	4x4	Yes (both authentication and recovery watermarks)	Up to 20% of original

5. Conclusions

In this paper a novel Wavelet-based image authentication and recovery scheme using two watermarks has been proposed. The algorithm is blind, semi-fragile, is able to detect and locate malicious tampering in digital images and recover a good estimate of the original content even if the watermarked image has been tampered with to a degree of 20%.

The proposed method achieves high tampering detection resolution and high image quality compared to other state of the art techniques. The watermarking scheme is protected against local attacks, like the Vector Quantization attack, by randomizing the position of Wavelet coefficients used for embedding with the use of a private key. The embedded authentication and recovery watermarks are also resilient against mild common image processing operations, like brightening, addition of Gaussian and "salt&pepper" noise, and JPEG compression, while still being able to detect intentional tampering with good accuracy.

Acknowledgement

This work has been funded by the Sectoral Operational Programme Human Resources Development 2007-2013 of the Ministry of European Funds through the Financial Agreements POSDRU/159/1.5/S/134398 and POSDRU/159/1.5/S/132397.

R E F E R E N C E S

[1] *H. M. Al-Otum*, Semi-fragile watermarking for grayscale image authentication and tamper detection based on an adjusted expanded-bit multiscale quantization-based technique, Journal of Visual Communication and Image Representation, vol. 25, issue 5, pp. 1064-1081, 2014.

[2] *R. O. Preda*, Semi-fragile watermarking for image authentication with sensitive tamper localization in the wavelet domain, Measurement, vol. 46, issue 1, pp. 367-373, 2013.

[3] *S. Bravo-Solorio, L. Gan, A. K. Nandi, and M. F. Aburdene*, Secure private fragile watermarking scheme with improved tampering localisation accuracy, Information Security, IET, vol. 4, pp. 137-148, 2010.

[4] *H. Kuo-Ming, C. Ting-Wen, S. Wen-Kai, and K. Chia-Nan*, Automatic image authentication and recovery using multiple watermarks, 2012 8th International Conference on Information Science and Digital Content Technology (ICIDT), pp. 730-735, 2012.

[5] *K. Wei-Chin, C. Te-Chih, W. Hsin-Lung, and C. Jen-Chun*, A Fragile Watermarking Scheme for Image Authentication with Tamper Detection and Localization, Fourth International Conference on Genetic and Evolutionary Computing (ICGEC), pp. 638-641, 2010.

[6] *A. T. S. Ho, Z. Xunzhan, S. Jun, and P. Marziliano*, Fragile Watermarking Based on Encoding of the Zeroes of the Z-Transform, IEEE Transactions on Information Forensics and Security, vol. 3, pp. 567-569, 2008.

[7] *C. Qin, C.-C. Chang, and P.-Y. Chen*, Self-embedding fragile watermarking with restoration capability based on adaptive bit allocation mechanism, Signal Processing, vol. 92, pp. 1137-1150, 2012.

[8] *H. He, J. Zhang, and F. Chen*, Adjacent-block based statistical detection method for self-embedding watermarking techniques, Signal Processing, vol. 89, issue 8, pp. 1557–1566, 2009.

[9] *A. M. Hassan, A. Al-Hamadi, B. Michaelis, Y. M. Y. Hasan, and M. A. A. Wahab*, Secure Self-Recovery Image Authentication Using Randomly-Sized Blocks, 2010 20th International Conference on Pattern Recognition (ICPR), pp. 1445-1448, 2010.

[10] *S. D. Lin, J. H. Lin, and C. Y. Chen*, A ROI-based semi-fragile watermarking for image tamper detection and recovery, International Journal of Innovative Computing, Information and Control, vol. 7, pp. 6875-6888, 2011.

[11] *P. Korus, J. Bialas, and A. Dziech*, Towards Practical Self-Embedding for JPEG-Compressed Digital Images, Multimedia, IEEE Transactions on, vol. 17, pp. 157-170, 2015.

[12] *S. Agreste and L. Puccio*, Wavelet-based watermarking algorithms: theory, applications and critical aspects, International Journal of Computer Mathematics, vol. 88, pp. 1885-1895, 2011.

[13] *R. Chamlawi, A. Khan, and I. Usman*, Dual Watermarking Method for Secure Image Authentication and Recovery, IEEE 13th International Multitopic Conference, INMIC 2009, pp. 1-4, Dec. 2009.

[14] *J. A. Mendoza-Noriega, B. M. Kurkoski, M. Nakano-Miytake and H. Perez-Mean*, Image Authentication and Recovery Using BCH Error-Correcting Codes, International Journal of Computers, vol. 5, no. 1, pp. 26-33, 2011.

[15] *X. Wang, D. Zhang, and X. Guo*, "Authentication and recovery of images using standard deviation", Journal of Electronic Imaging, vol. 22 (3), 033012, 2013.

[16] *R. Ullah, A. Khan, and A. S. Malik*, Dual-purpose semi-fragile watermark: Authentication and recovery of digital images, Computers and Electrical Engineering, vol. 39, pp. 2019-2030, 2013.

[17] *S. Som, S. Palit, K. Dey, D. Sarkar, J. Sarkar, and K. Sarkar*, A DWT-based Digital Watermarking Scheme for Image Tamper Detection, Localization, and Restoration, in Applied Computation and Security Systems. vol. 305, pp. 17-37, 2015.