Journal of ELECTRICAL ENGINEERING, VOL. 59, NO. 3, 2008, 131–138

ATTACKS ON DIGITAL WAVELET IMAGE WATERMARKS

Andreja Samčović * — **Ján Turán** **

In the last decade, a large number of schemes have been proposed for hiding copyright marks and other information in digital images. Watermarking is a potential method for protection of ownership rights on digital images. Any processing that may impair detection of the watermark or communication of the information conveyed by the watermark is in watermarking technology called an attack. This paper presents a number of attacks that enable the information hidden by them to be removed or otherwise rendered unusable. Also, some attacks are tested on a watermarking algorithm based on wavelets.

K e y w o r d s: watermarking, image, attacks, wavelets, signal processing

1 INTRODUCTION

With the growth of the Internet and the immediate availability of computing resources to everyone, "digitized property" can be reproduced and instantaneously distributed without loss of quality at basically no cost. Until now, intellectual property and value has always been bound to some physical container that could not be easily duplicated, thereby guaranteeing that the creator benefits from his work.

Clearly, there is business like the music or photography industry that can not adopt this paradigm since they trade basic content and therefore have to stick with traditional copyright enforcement to guarantee income. As audio, video and other works become available in digital form, it may be that the ease with which perfect copies can be made will lead to large-scale unauthorized copying which will undermine the music, film, book and software publishing industries.

The rapid evolution of digital technology makes the development of reliable and robust schemes for protecting digital still images, audio and video from piracy a matter of urgency. Piracy attacks include illegal access to transmitted data in networks, data content modification, production and retransmission of illegitimate copies. The impact of such attacks might be very large, booth in financial and security terms [1].

Networked multimedia systems have known rapid development and expansion, so that more and more information are transmitted digitally; the expansion will increase even more when advanced multimedia services will be widely available, such as electronic commerce, payper-view, video-on-demand, electronic newspapers, teleworking, teleconsultation, etc. However, authors, publishers and providers of multimedia data are reluctant to grant the distribution of their documents in a networked environment, because the ease of intercepting, copying and redistributing electronic data in their exact original form encourages copyright violation. It is crucial, thus, for the future development of networked multimedia systems, which robust methods are developed to protect the intellectual property rights of data owners against unauthorized copying and redistribution of the material made available on the network. Classical encryption systems do not completely solve the problem of unauthorized copying, because once encryption is removed from a document, there is no more control on its dissemination.

The use of digitally formatted image and video information is rapidly increasing with the development of multimedia broadcasting, network databases and electronic publishing. This evolution provides many advantages such as easy, fast and inexpensive duplication of products. However, it also increases the potential for unauthorized distribution of such information, and significantly increases the problems associated with enforcing copyright protection.

Among the multimedia data, images and video are certainly the most difficult ones to protect because of the numerous processing operations they may undergo. Many algorithms have recently been proposed for image and video copyright protection. Some techniques modify spatial/temporal data samples, while others modify transform coefficients. However, research on copyright protection of images is still in its early stages and none of the existing methods is totally efficient against attacks.

Data transmitted through network communication lines may be protected from unauthorized receivers by applying techniques based on cryptography. Only persons, who possess the appropriate private key, can decrypt the received data using a public algorithm implemented either in hardware or in software. Fast implementation of encryption-decryption algorithms is highly desirable.

* University of Belgrade, Faculty of Traffic and Transport Engineering, Vojvode Stepe 305, 11040 Belgrade, Serbia; andrej@sf.bg.ac.yu

** Technical University of Košice, Faculty of Electrical Engineering and Informatics, Park Komenského 13, 041 20 Košice, Slovakia; jan.turan@tuke.sk

ISSN 1335-3632

Data content manipulation can be performed for various legal or illegal purposes (compression, noise removal, malicious data modification). The modified product is not authentic with respect to the original one. Content verification can be performed by attaching digital signatures to the transmitted data. A digital signature is an encoded message that matches the content of a particular authentic digital product. Authenticity verification procedures are based on public algorithms and public keys. Any "worth nothing" modification performed in the product or in the signature data should cause verification failure.

One technical way to make law enforcement and copyright protection for digital media possible and practical is digital watermarking which is aimed to automatically detect and possibly also prosecute copyright infringement. Therefore, it has been significant recent research into "watermarking" (hiding copyright messages) and "fingerprinting" (hiding serial numbers or a set of characteristics that to distinguish an object from other similar objects); the idea is that the latter can be used to detect copyright violators and the former to prosecute them. In addition, a watermark may provide extra information and guarantee data integrity [2].

This paper is organizes as follows. After the introduction, the main watermarking attacks are described. The next part deals with the wavelet transform, which can be applied in the field of watermarking. One additive watermarking wavelet algorithm is considered in the following part of the paper. Some simulation results are given, also. The conclusion finalizes the paper.

2 WATERMARKING ATTACKS

First of all, we have to distinguish two "reasons" or "purposes" for an attack against a watermark image:

- Hostile or malicious attacks, which are an attempt to weaken, remove or alter the watermark, and
- Coincidental attacks, which can occur during common image processing and are not aimed at tampering with the watermark.

Lossy image compression is considered the most common form of attack a watermarking scheme has to withstand. The harsh term "attack" can be easily justified: an efficient image compression has to suppress or discard perceptually irrelevant information — the invisible watermark. A wide range of attacks has been described in the literature [3]. The following four large categories of attacks can be invoked to penetrate a watermarking system:

- Removal attacks
- Geometrical attacks
- Cryptographic attacks
- Protocol attacks

Removal (simple) attacks attempt to separate and remove the watermark. If somebody tries to remove the watermark from the data, this is called a removal attack. The means employed most frequently are filter models taken from statistical signal theory. Denoising the marked image through median or high-pass filtering as well as nonlinear truncation or spatial watermark prediction are methods considered very likely to succeed. The goal is to add distortion to the host image in order to render the watermark undetectable or unreadable [4]. The attack is successful if the watermark cannot be detected anymore, but the image is still intelligible and can be used for a particular determined purpose. Many such attack operations have been proposed:

- Lossy image compression (JPEG, JPEG 2000)
- Addition of Gaussian noise
- Denoising
- Filtering
- Median filtering and blurring
- Signal enhancement (sharpening, contrast enhancement)

Compression: this is generally an unintentional attack, which appears very often in multimedia applications. Practically all images currently being distributed via Internet have been compressed. If the watermark is required to resist different levels of compression, it is usually advisable to perform the watermark embedding in the same domain where the compression takes place. For instance, the Discrete Cosine Transform (DCT) domain image watermarking is more robust to Joint Photograph Expert Group (JPEG) compression than the spatial-domain watermarking. Also, the Discrete Wavelet Domain (DWT)-domain watermarking is robust to JPEG 2000 compression [5].

Additive noise: a random signal with a given distribution (*eg* Gaussian, uniform, Poisson, Bernoulli) is added to the image unintentionally. In certain applications the additive noise may originate from Digital-to-Analog (D/A) and A/D converters, or as a consequence of transmission errors. However, an attacker may introduce perceptually shaped noise (image-dependent mask) with the maximum unnoticeable power. This will typically force to increase the threshold at which the correlation detector operates.

Denoising explores the idea that a watermark is an additive noise (which can be modeled statistically) relative to the original image. These attacks include: local median, midpoint, trimmed mean filtering, Wiener filtering, as well as hard and soft thresholding.

Filtering attacks are linear filtering: high-pass, low-pass, Gaussian and sharpening filtering, *etc.* Low-pass filtering, for instance doesn't introduce considerable degradation in watermarked images, but can dramatically affect the performance since spread-spectrum-like watermarks have non negligible high-frequency spectral contents. To design a watermark robust to a known group of filters that might be applied to the watermarked image, the watermark message should be designed in such a way to have most of its energy in the frequencies which filters change the least.

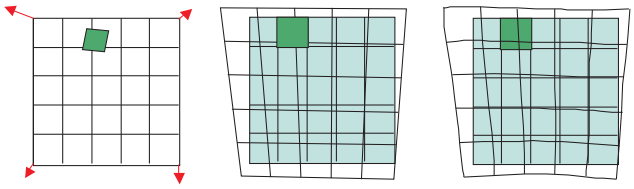

Fig. 1. StirMark application to still pictures

Statistical averaging: the aim of these attacks is retrieving the host image and/or watermark by statistical analysis of multiple marked data sets. An attacker may try to estimate the watermark and then to "unwatermark" the object by subtracting the estimation. This is dangerous if the watermark doesn't depend substantially on data. This is a good reason for using perceptual masks to create a watermark. In this group of attacks belong the averaging and collusion attacks. *Averaging attack* consists of averaging many instances of a given data set each time marked with a different watermark. In this way an estimate of the host data is computed and each of the watermarks is weakened. *Collusion attack* consists of averaging different host data containing the same watermark. The resulting signal may serve as a good estimate of the watermark, which can be used to remove it from the watermarked data.

Geometrical attacks. These attacks are not aimed at removing the watermark, but try to either destroy it or disable its detection. They attempt to break the correlation detection between the extracted and the original watermark sequence, where the image is subjected to translation, rotation, scaling and/or cropping. This can be accomplished by "shuffing" the pixels. The values of corresponding pixels in the attacked and the original image are the same. However, their location has changed. These attacks can be subdivided into attacks applying general affine transformations and attacks based on projective transformation. *Cropping* is a very common attack since in many cases the attacker is interested in a small portion of the watermarked object, such as parts of a certain picture or frames of video sequence. With this in mind, in order to survive, the watermark needs to be spread over the dimensions where this attack takes place.

StirMark is a program which can be used to apply different types of attacks. One specific attack introduces nonlinear distortion via random "bending" into the image. This system introduced random bilinear geometric distortions as an innovative attack against image watermarks. Following this attack and after evaluating some watermarking software, it became clear that although many of the seriously proposed schemes could survive basic manipulations — that is, manipulations that can be done easily with standard tools, such as rotation, shearing, resampling, resizing and lossy compression — they would not cope with combinations with them. StirMark is a generic tool developed for simple robustness testing of image marking algorithms. In its simplest version, StirMark simulates a resampling process, *ie* it introduces the same kind of errors into an image as printing it on a high quality printer and then scanning it again with a high quality scanner, which is shown in Fig. 1. The first drawing in the picture corresponds to the original picture; the others show the picture after StirMark has been applied — without and with bending and randomization. It applies a minor geometric distortion: the image is slightly stretched, sheared, shifted and/or rotated by an unnoticeable random amount, and then resampled by using either bi-linear or Nyquist interpolation. In addition, a transfer function that introduces a small and smoothly distributed error into all sample values is applied. This emulates the small non-linear analog/digital converter imperfection typically found in scanners and display devices. StirMark introduces a practically unnoticeable quality loss in the image if it is applied only once. However, after a few iterated applications, the image degradation becomes noticeable.

The StirMark system is today a public automated benchmark evaluation service. The attacks which are included in the benchmark are cropping, JPEG, median cut, add noise, remove lines, affine transform, self-similarity, convolution and random bilinear geometric distortion. For each attack, it tests whether a message was correctly decoded or not.

For those unfamiliar with digital signal processing, we shall now summarize briefly the main computation steps. Apart from a few simple operations such as rotations by 90 or 180 degrees, reflection and mirroring, image manipulation usually requires resampling when destination pixels don't line up with source pixels. In theory, one first generates a continuous image from the digital one, then modifies the continuous image, finally samples this to create a new digital image. In practice, however, we compute the inverse transform of a new pixel and evaluate the reconstruction function at that point.

There are numerous reconstruction filters. In a first version of the software, a linear interpolation was used but, as foreseen, this tended to blur the image too much, making the validity of the watermark removal arguable. Then the sinc function is implemented as a reconstruction filter, which gives theoretically perfect reconstruction for photo images and can be described as follows. This gives very much better results than the simple filter. An example of the removal of a watermark is given in Fig. 2, which shows the Kings' College Chapel in Cambridge, England. The image (a) is the watermarked image. The StirMark attack is applied in Fig. 2 (b)and tested the presence of the watermark.

The StirMark benchmark has now been established as an evaluation tool for image watermarking robustness. The general design concept is divided into three main parts: (1) the test library with the evaluation algorithms, evaluation profiles for the different requirements from the applications, and the multimedia database; (2) benchmarking application with the marking scheme library and

(a) (b)

Fig. 2. Example of the StirMark attack on the watermarked image

the quality metrics; and (3) the results database with a Web server as Web interface for Web-based evaluation. The main idea is to encapsulate the test algorithms from the benchmarking to allow continuous development of new attacks independent of the actual available profiles integrated into the whole application. Furthermore, for offline testing, the test library can be used as a stand-alone evaluation tool without using the Web evaluation service. The actual implementation for image benchmarking covers the test library as a stand-alone tool and the Web service in the overall architecture design.

Mosaic attack. This point is emphasized by a "presentation" attack, which is of quite general applicability and which possesses the initially remarkable property that a marked image can be unmarked and yet still rendered pixel for pixel in exactly the same way as the marked image by a standard browser.

The attack was motivated by a fielded automatic system for copyright piracy detection, consisting of a watermarking scheme plus a web crawler that downloads pictures from the net and checks whether they contain a watermark.

It consists of chopping an image up into a number of smaller subimages, which are embedded in a suitable sequence in a web page. Common web browsers render juxtaposed subimages stuck together, so they appear identical to the original image, which is shown in Fig. 3. This attack appears to be quite general; all marking schemes require the marked image to have some minimal size (one cannot hide a meaningful mark in just one pixel). Thus by splitting an image into sufficiently small pieces, the mark detector will be confused. The best that one can hope for is that the minimal size could be quite small and the method might therefore not be very practical.

Cryptographic attacks aim at cracking the security methods in watermarking schemes and thus finding a way to remove the embedded watermark information or to embed misleading watermarks. One such technique is *brute-force* search for the embedded secret information. Practically, application of these attacks is restricted due to their high computational complexity. They cover, for example, direct attacks to find the secret key or attacks called collusion attacks. Cryptographic attacks are very similar to the attacks used in cryptography. There are the brute force attacks, which aim at finding secret information through an exhaustive search. Since many watermarking schemes use a secret key, it is very important to use keys with a secure length. Another attack in this category is so-called *Oracle attack* which can be used to create a non-watermarked image when a watermark detector device is available.

Protocol attacks neither aim at destroying the embedded information nor at disabling the detection of the embedded information (deactivation of the watermark). Rather, they take advantage of semantic deficits of the watermark's implementation. The protocol attacks aim at attracting the concept of the watermarking application. The first protocol attack was proposed by Craver et al. [6]. They introduced the framework of invertible watermark and showed that for copyright protection applications watermarks need to be non-invertible. The idea of inversion consists of the fact that an attacker who has a copy of the stego-data can claim that the data contains also the attacker's watermark by subtracting his own watermark. This can create a situation of ambiguity with respect to the real ownership of the data. The requirement of non-invertability on the watermarking technology implies that it should not be possible to extract a watermark from non-watermarked image. As a solution to this problem, the authors proposed to make watermarks signal-dependent by using a one-way function.

Consequently, a watermark must not be invertible or to be copied. A *copy attack*, for example, would aim at copying a watermark from one image into another without knowledge of the secret key. It also belongs to the group of the protocol attacks. In this case, the goal is not to destroy the watermark or impair its detection, but to estimate a watermark from watermarked data and copy it to some other data, called target data.

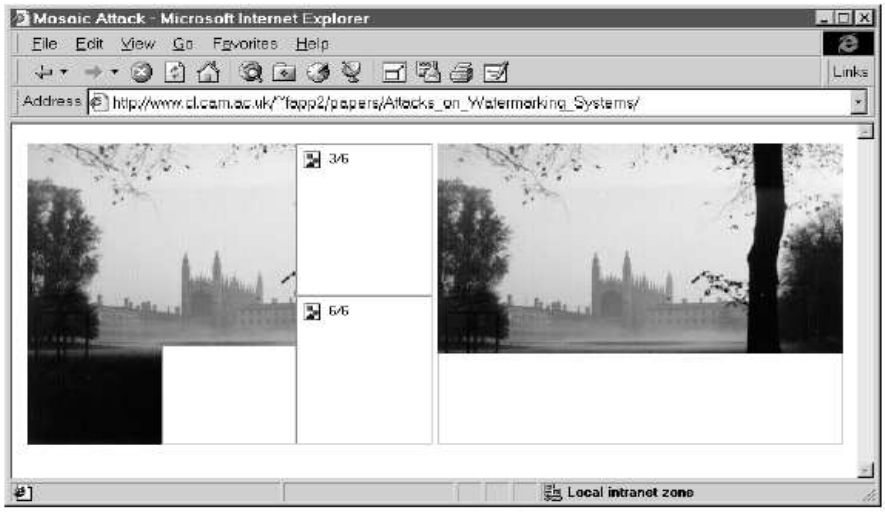

Fig. 3. Screen-shot of a web browser while downloading an image after the mosaic attack

If the watermarking system or protocol makes not only the watermarked image, but at the same time additional devices publicly available, the presence of such devices can be exploited [7]. When exploiting the presence of a watermark detector, a test-image should be created near the detection boundary and then successively change single pixels until the detector response indicates that a particular pixel value has significant influence on the watermark. This way, a set of influential pixels can be determined which has the largest influence on the detector while introducing low disturbance into the image when manipulated. This process has linear complexity. With the presence of a watermark inserter, the difference image between the watermarked and the original image can be easily computed and analyzed. A public watermark inserter is provided by the *Digital Versatile Disc*(DVD) system for copy generation management.

3 WAVELET TRANSFORM

The wavelet transform (WT) has been extensively studied in last decade. Many applications of the wavelet transform, such as compression, signal analysis and signal processing have been found. There are many good tutorial books and papers on this topic. Here, we just introduce the necessary concepts of the Discrete Wavelet Transform (DWT) for the purpose of this paper.

The basic idea of the DWT for a one-dimensional signal is the following. A signal is split into two parts, usually high and low frequencies. The edge components of the signal are largely confined in the high frequency part. The low frequency part is split again into two parts of high and low frequency. This process is continued until the signal has been entirely decomposed or stopped before by the application at hand. For compression and watermarking application, generally no more than five decomposition steps are computed. Furthermore, from the DWT coefficients, the original signal can be reconstructed.

The wavelet transform decomposes an image into three spatial directions, *ie* the horizontal **HL**, the vertical **LH** and the diagonal **HH**. At each level of decomposition, the magnitude of the DWT coefficients is larger in the lowest subbands ("approximation" **LL** subband), and smaller for other subbands ("detail" subbands: **HL**, **LH** and **HH**). The most significant coefficients in a subband are those with large magnitudes. The high resolution subbands help in locating the edge and texture patterns for an arbitrary image.

Watermarking in the DWT domain has a number of advantages over other transforms, particularly the Discrete Cosine Transform (DCT) [8]:

- Wavelet coded image is a multi-resolution description of an image. Hence, an image can be shown at different level of resolution and can be sequentially processed from low to high resolution.
- DWT is closer to the properties of the human visual system than the DCT, since it splits the signal into individual bands, which can be processed independently.
- The distortions introduced by wavelet domain coding with high compression ratio are less annoying than those introduced at the same bit rate by the DCT. In the JPEG case, block-shaped distortions are clearly visible, since image coding based on the DCT usually operates on independent 8×8 blocks.
- Watermarking schemes put more watermark energy into the large DWT coefficients, thus affecting mostly regions like lines and texture on which the human visual system is not sensitive, too.
- DWT has spatial frequency locality, which means if the watermark is embedded into the DWT coefficients, it will affect the image locally. Hence, the wavelet transform provides both frequency and spatial description for an image.

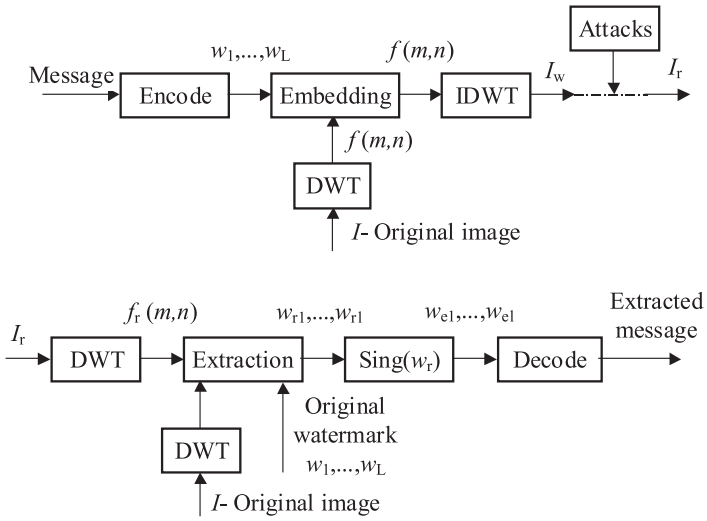

Fig. 4. Block-diagram of the embedding method

4 ADDITIVE WATERMARKING WAVELET ALGORITHM

The watermarking procedure is split into two procedures:

- Watermarking embedding
- Watermarking extraction

At the beginning of embedding procedure a bipolar sequence of bits is transformed into a new sequence $w(1), \ldots, w(L)$ by replacing 0 by -1, where L is the length of the sequence and $w(k) \in \{-1, 1\}$ $(k = 1, \ldots, L)$. The new sequence is used as the watermark. The original image $\mathbf{I}$ is decomposed into two levels of the DWT decomposition [9]. The decomposition is performed using the Haar wavelet filters. The watermark is added to L largest coefficients in all of the detailed subbands ($\mathbf{HL}_i$, $\mathbf{LH}_i$, $\mathbf{HH}_i$, $i = 1, 2$) of the DWT decomposition. $\mathbf{HL}_1$, $\mathbf{LH}_1$, and $\mathbf{HH}_1$ represent the high frequency ranges, while $\mathbf{HL}_2$, $\mathbf{LH}_2$, and $\mathbf{HH}_2$ represent the middle frequency ranges of the image processed. Let $f(m, n)$ denote the set of L largest DWT coefficients at the position (m, n) in any of subband matrices ($\mathbf{HL}_i$, $\mathbf{LH}_i$, $\mathbf{HH}_i$, $i = 1, 2$). The embedding procedure is performed according to the following formula:

$$f'(m, n) = f(m, n) + alfa \cdot f(m, n)w(k)\,,\ k = 1, \ldots, L$$

where *alfa* is the strength of the watermark controlling the level of the watermark $f'(m, n)$ is modified coefficient at the position (m, n) in any of subband matrices. The watermarked image $\mathbf{I}_w$ is obtained by applying the inverse DWT (IDWT). The position vectors of modified coefficients in all subbands are kept secretly and used in extraction procedure as a secret key. The upper part of Fig. 4 shows the block-diagram of the embedding procedure. The lower part of the Fig. 4 represents the detection procedure.

In the watermark extraction procedure (see lower part of the Fig. 4) both the received image $\mathbf{I}_r$ and the original image $\mathbf{I}$ are decomposed into levels of the DWT decomposition. By this the received image $\mathbf{I}_r$ is possibly modified by attacks. It is assumed that the original image $\mathbf{I}$ is available in the extraction procedure, *ie* that is used as an input to this procedure.

When images are decomposed using the DWT the positions of the modified coefficients in the subbands of the original and received images are calculated according to the secret key generated in the embedding procedure [10]. This set of selected DWT coefficients will be denoted with $f(m, n)$ and $f_r(m, n)$, respectively. The position (m, n) represents the particular position in the subband. The extraction procedure is described by the following formula:

$$w_r(k) = \big(f_r(m, n) - f(m, n)\big) / \big(alfa \cdot f(m, n)\big)$$

where w_r is the extracted watermark. The extracted watermark is further transformed as follows:

$$w_e(k) = \mathrm{sign}\big(w_r(k)\big)$$

After extraction of the watermark w_e the bit stream is reconstructed by similar replacing as at the beginning (-1 is replaced by 0).

5 SIMULATION RESULTS

For the purpose of robustness testing the following set of ten standard test- images with the size of 512×512 pixels are used: *Barbara, Boat, Cameraman, Couple, Einstein, Elaine, F16, Goldhill, Hous* and *Lena*. The watermark is firstly converted into ASCII code and than encoded with the error correction code (ECC) in order to

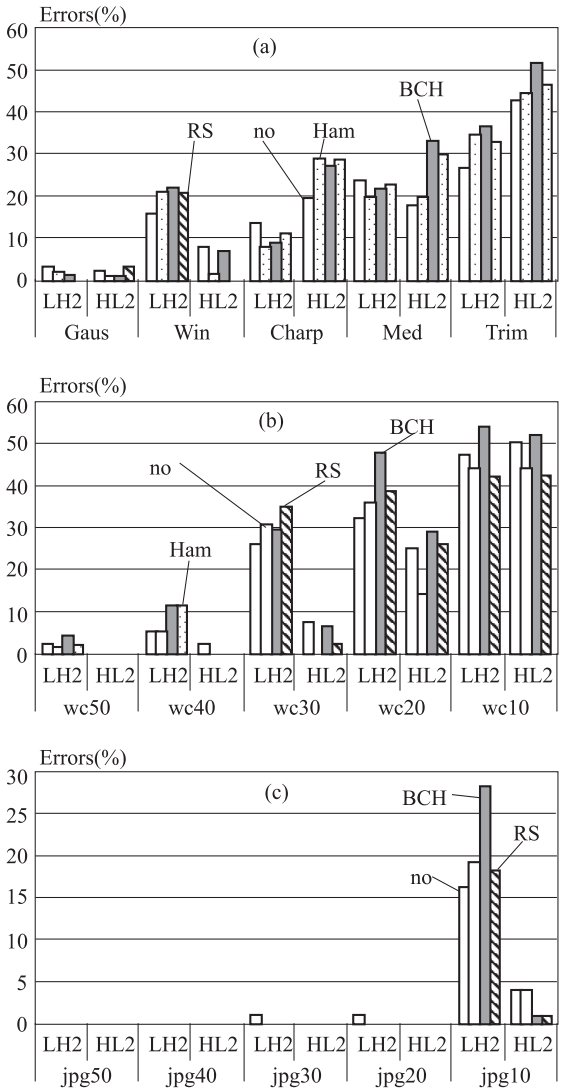

Fig. 5. (Simulation results for: (a) different filtering attacks, (b) JPEG 2000, (c) JPEG compression attacks

improve the robustness. Here, the robustness of the algorithm will be tested for the watermark sequence encoded with three different ECCs and for the watermark sequence that is directly embedded without using ECC. The following ECCs are used in order to determine which ECC performs the best from the robustness point of view:

(15,7) Bose-Chaudhuri-Hocquenghem (BCH) code

(7,4) Hamming code and

(15,7) Reed-Solomon (RS) code

The same watermark is embedded in all detail subbands of the two-level DWT according to the embedding procedure. In order to fit our sequence to the codeword of the ECC for Hamming code, the 8-bit representation of the particular character will be used. For other ECC as well as for the directly embedded watermark sequence, the 7-bit representation will be used. The characteristic of the embedded watermark will be given in the Table 1.

Table 1. Characteristic of the embedded watermark

	MESSAGE LENGTH (bits)	ENCODED MESSAGE LENGTH (bits)	ADDITIONAL INFORMATION (bits per character)
NO ECC	147	147	7
BCH	147	315	7
HAMMING	168	294	8
RS	147	360	7

The Table shows that with the Reed-Solomon coding more then twice of bits have to be embedded into the DWT subband compared to the approach without ECC. This fact must be taken into account when designing the watermark scheme due to the possible problem with the capacity of the cover image.

In the testing, several non-geometrical processing operations are applied watermarked test-images: median filtering with 3×3 window size (med), Gaussian filtering with 5×5 window (gaus), Wiener filtering with 5×5 window (wien), trimmed mean filtering with 7×7 window (trim), sharpening with 3×3 high-pass filter (sh), JPEG compression with different quality factors from 50 to 10 (jpg50, jpg40, jpg30, jpg25, jpg15, jpg10), as well as JPEG compression with different bit rates from 0.5 to 0.1 bits per pixel (bpp) (wc50, wc40, wc30, wc20 and wc10).

The watermark is extracted separately from every subband in order to compare the robustness of the watermark embedded in that subband. The results for the *Lena* image are given in Fig. 5. The similar results are obtained for other test-images. All graphs in Fig. 5 present different attacks on the x-axes. The results are calculated as the total number of not correctly extracted watermark bits (errors) divided by the total number of watermark bits, expressed in percentage and presented on the y-axes of all three graphs. The best results are obtained for the watermark embedded in the subbands $\mathbf{HL}_2$ and $\mathbf{LH}_2$ and only results for these subbands are presented. The results for other tested subbands were not good and they were not being further considered. This was expected due to the fact that the common signal processing operations like filtering and compression will be most effective in the high frequencies (level 1 of the DWT decomposition).

From Fig. 5 it can be concluded that for the most attacks Reed-Solomon code gives less errors than other ECCs. It can also be concluded that the results strongly depend on the subband in which the watermark sequence was embedded. In some cases like trimmed mean filtering better results are obtained without using ECC.

6 CONCLUSION

The majority of copyright marking schemes are vulnerable to attacks involving the introduction of subperceptual levels of distortion. In particular, many of the marking schemes in the market place provide only a limited measure of protection against attacks. New ways to

represent the characteristics of the watermarking attacks are under development. One DWT based watermarking algorithm is proposed and tested against different signal processing attacks, like filtering and compression. The best results are obtained if the watermark is embedded in higher subbands. Also, it is shown that the Read-Solomon error correcting code delivers the best results from the watermark robustness point of view. We can conclude that the better understanding of possible attacks will lead to the development of more efficient and robust watermarking techniques.

References

[1] PETITCOLAS, F.—ANDERSON, R.—KUHN, M.: Attacks on Copyright Marking Systems, in Lecture Notes on Computer Science, pp. 218–238, April 1998.

[2] MACQ, B.—DITTMANN, J.—DELP, E. Benchmarking of Image Watermarking Algorithms for digital Rights Management: Proceedings of the IEEE **92** No. 6 (June 2004), 971–984.

[3] BOJKOVIĆ, Z.—SAMČOVIĆ, A.: XXXVII International Scientific Conference on Information, Communication and Energy Systems and Technologies ICEST 2002, Vol. 1, pp. 131–134, Niš, Yugoslavia, 1–4 October 2002.

[4] BOJKOVIĆ, Z.—TURÁN, J.—SAMČOVIĆ, A.—OVSENIK, L.: Coding, Streaming and Watermarking – some Principles in Multimedia Signal Processing, Acta Electrotechnica et Informatica (Košice) **4** No. 3 (2004), 13–20.

[5] TZOVARAS, D.—KARAGIANNIS, N.—STRINTZIS, M.: Robust Image Watermarking in the Subband or DCT Domain, EUSIPCO'98, Vol.IV, pp. 2285–2288, 8–11 September 1998, Rhodes, Greece.

[6] CRAVER, S.—KATZENBEISSER, S.: Copyright Protection Protocols based on Asymmetric Watermarking: the Ticket Concept, in Communications and Multimedia Security Issues of the New Century, Kluwer Academic Publishers, 2001, pp. 159–170.

[7] SOLACHIDIS, V.—TEFAS, A.—NIKOLAIDIS, N.—TSEKERIDOU, S.—NIKOLAIDIS, A.—PITAS, I.: A Benchmarking Protocol for Watermarking Methods, IEEE Int. Conf. on Image Processing ICIP'01, Thessaloniki, Greece, pp. 1023–1026, 7–10 October 2001.

[8] HSU, C. T.—WU, J. L.: Multiresolution Watermarking for Digital Images, IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing **45** No. 8 (1998), 1097–1101.

[9] PLA, O.—LIN, E.—DELP, E.: A Wavelet Watermarking Algorithm based on a Tree Structure, in Security, Steganography, and Watermarking of Multimedia Contents, pp. 571–580, 2004.

[10] BARNI, M.—BARTOLINI, F.: Improved Wavelet-Based Watermarking Through Pixel-Wise Masking, IEEE Trans. Image Processing **10** No. 5 (May 2001), 783–791.

Received 13 September 2007

Andreja Samčović (Doc, Ing, PhD), was born in 1963 in Belgrade, Serbia. He received the Dipl Ing, Magister and PhD degrees in electrical engineering in 1989, 1995 and 2005, respectively, from the University of Belgrade, Serbia. He joined the Faculty of Traffic and Transport Engineering, University of Belgrade, from 1991, working in the areas of electrical engineering, communications and image coding. He spent 9 months in 1991/1992 at the TU Vienna (Austria), 6 months in 1999/2000 at the Friedrich-Alexander University Erlangen-Nuremberg (Germany), as well as 3 months at the Technical University of Košice (Slovakia) in 2007. In 2003, he served as a lecturer at the UniAdrion summer school in Ammoudia-Preveza, Greece. He participated at the projects with the Virtual University of the Adriatic-Ionian basin, Technical University of Košice (Slovakia), and University of Ljubljana (Slovenia). He has published ten journal papers and over 60 conference presentations, on diffierent aspects of image coding and communications, as well as one monograph.

Ján Turán (Prof, Ing, RNDr, DrSc), was born in Šahy, Slovakia in 1951. He received an Ing degree in physical engineering with honours from the Czech Technical University, Prague, Czech Republic in 1974 and a RNDr. degree in experimental physics with honours from the Charles University, Prague, Czech Republic in 1980. He received a CSc (PhD) and DrSc degree in radioelectronics from the Technical University, Košice, Slovakia, in 1983 and 1992 respectively. From 1974 to 1997, he worked as an electrical engineer at the firm ČKD Polovodiče, Prague. From 1997 to 1997 he was with the Institute of Nuclear Technology and Radioecology, Košice, as a research fellow. Since March 1979 he has been at the Technical University of Košice as a professor of electronics and telecommunications technology. His research interests include multimedia signal processing and fiber optics communication. Prof. Turán is a senior member of the IEEE, member of the Czech and Slovak Radioengineering and Photonics Societies.