Journal of Computational and Applied Mathematics 227 (2009) 213–220

Contents lists available at ScienceDirect

Journal of Computational and Applied Mathematics

journal homepage: www.elsevier.com/locate/cam

Applying robust multibit watermarks to digital images

Dimitrios Tsolis [a,*], Spiridon Nikolopoulos [b], Lambros Drossos [c], Spyros Sioutas [d], Theodore Papatheodorou [a]

[a] Department of Computer Engineering and Informatics, University of Patras, Greece
[b] Informatics and Telematics Institute, Centre of For Research and Technology, Greece
[c] Department of Applied Informatics in Administration and Economics, Technological Institute of Messolongi, Greece
[d] Department of Informatics, Ionian University, Greece

ARTICLE INFO

Article history:
Received 1 December 2007
Received in revised form 19 May 2008

Keywords:
Multibit watermarking
Spread spectrum analysis
Wavelet domain
Subband-DCT
Copyright protection
Digital information management on the web

ABSTRACT

The current work is focusing on the implementation of a robust multibit watermarking algorithm for digital images, which is based on an innovative spread spectrum technique analysis. The paper presents the watermark embedding and detection algorithms, which use both wavelets and the Discrete Cosine Transform and analyzes the arising issues.
© 2008 Elsevier B.V. All rights reserved.

1. Introduction

Wide access and delivery of valuable content raise several critical issues, pertaining to management, protection and exploitation of digitized content. These include the critical problem of IPR (Intellectual Property Rights), protection and the unauthorized use and exploitation of digital data (electronic theft) [6]. Besides economical and other implications, such problems create considerable skepticism to organizations and individual content owners. As a result content of great educational and economical value is often held secret and private [4]. Technological means is one of the key components, attracting plenty of scientific research, within the generalized Digital Rights Management framework. Watermarking is probably the most promising technological approach against Intellectual Property Rights violations [8]. The majority of watermarking systems achieving high robustness are only capable of embedding one bit of information placing specific limitations on the potentials of the encrypted information. Most of the real word applications raise the requirement of a multi-bit robust watermarking scheme where the detectors output can be interpreted into meaningful and valuable information.

2. Multibit watermark technique

2.1. Spread spectrum watermarking in the wavelet domain

Generally, a watermark is a narrow band signal, which is embedded to the wide band signal of a digital image [9]. Spread Spectrum techniques are methods by which energy generated at one or more discrete frequencies is deliberately spread or

* Corresponding author. Tel.: +30 2610996900; fax: +30 2610969001.
E-mail address: dkt@hpclab.ceid.upatras.gr (D. Tsolis).

0377-0427/$ – see front matter © 2008 Elsevier B.V. All rights reserved.
doi:10.1016/j.cam.2008.07.035

distributed in time or frequency domains. In particular, these techniques employ pseudo-random number sequences (noise signals) to determine and control the spreading pattern of the signal across the allotted bandwidth. The noise signal can be used to exactly reconstruct the original data at the receiving end, by multiplying it by the same pseudo-random sequence: this process, known as "de-spreading", mathematically constitutes a correlation of the transmitted pseudo-random number sequence with the receiver's assumed sequence. Thus, if the signal is distorted by some process that damages only a fraction of the frequencies, such as a band-pass filter or addition of band limited noise, the encrypted information will still be identifiable. Furthermore, high frequencies are appropriate for rendering the watermarked message invisible but are inefficient in terms of robustness, whereas low frequencies are appropriate with regards to robustness but are useless because of the unacceptable visual impact.

An example of an additive spread spectrum watermarking scheme has been developed in [10] for DVD protection. An important example of a multiplicative and detectable spread spectrum watermarking system is the work in [3], which has strongly influenced subsequent watermarking research. Another example of a multiplicative spread spectrum watermarking algorithm has been presented in [1], who proposed an optimal and blind decoding and detection of multiplicative watermarks.

Prior to presenting the proposed method, it is important to mention some of the basic features carried by the spread spectrum technique.

2.2. General description of the additive algorithm

In additive watermarking algorithms, the signature data is a sequence of numbers w_i of length N that is embedded in a suitably selected subset of the host signal data coefficients, f. The basic and commonly used embedding formula is

$$f'(m, n) = f(m, n)(1 + aw_i) \tag{1}$$

where a is a weighting factor and f' is the resulting modified host data coefficients carrying the watermark information. Alternative embedding formulas have been proposed in [2], such as

$$f'(m, n) = f(m, n) + aw_i \tag{2}$$

or using the logarithm of the original coefficients,

$$f'(m, n) = f(m, n)\mathrm{e}^{aw_i}. \tag{3}$$

An important property of the above formula is that an inverse embedding function,

$$w_i' = \frac{f''(m, n) - f(m, n)}{a \times f(m, n)} \tag{4}$$

can be easily derived to compute w' from f'' given the original host coefficients as reference. By f' we denote the received, possibly altered, image that might contain the watermark w. At the next step, the extracted watermark sequence w' is compared to the original embedded watermark w using the normalized correlation of the sequences as a similarity measure

$$\delta = \frac{w' \times w}{\|w'\| \times \|w\|}. \tag{5}$$

The similarity δ varies in the interval $[-1, 1]$, a value well above 0 close to 1 indicates the extracted sequence w' matching the embedded sequence w and therefore concluding that the image has been watermarked with w. A detection threshold τ can be established to make the detection decision,

$$\delta > \tau. \tag{6}$$

The detection threshold was derived experimentally by observing the correlation of random sequences. For example, a threshold

$$\tau = \frac{\alpha}{S \times N} \sum^{N} |f'| \tag{7}$$

can be used, where S, the standard deviation, is 2 or 3.

Of course, the choice of the threshold influences the false-positive and false-negative probability. Hence, a lot of effort has been focused on devising reliable methods to compute predictable correlation thresholds and efficient watermark detection systems.

The weighting factor a does not necessarily have to be constant over the entire watermark sequence, but can be chosen adaptively to capture and exploit local properties of the host signal.

Before the watermark embedding, the host image F is usually subjected to a two dimensional transform T such as the Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT) or Discrete Wavelet Transformation (DWT, non-redundant) to derive a frequency representation f of the data, $f = TxF$. Following the watermarking modifications in the frequency domain, the spatial image representation is regained by applying the inverse transform

$$T^{-1}, F = T^{-1} \times f. \tag{8}$$

Generally, watermarks embedded in the frequency domain have been proved to be more robust to many forms of attacks compared to spatial domain watermarks [7]. In order to achieve robustness, the watermark has to be embedded in the low- and mid-frequency coefficients of the host signal [1]. The frequency representation of the host image easily allows selecting the low- and mid-frequency coefficients which carry most of the signals energy [5]. The selection of suitable transform domain coefficients is one of the most important design issues, as it greatly affects robustness, imperceptibility and security of the resulting watermarking scheme.

2.3. Subband-DCT

The novelty of the proposed implementation is based on a method in which both wavelets and the well known DCT are involved [1]. Highpass and lowpass filters are used to subsample and filter the original image. The combination of the two filters for each direction (horizontal and vertical) of filtering produces four subbands for each level of decomposition. The band that corresponds to lowpass filtering in both directions (LL band) can be further subsampled and filtered, thus providing another level of decomposition. Finally, each of the bands is transformed applying the DCT transform. In the proposed scheme a one level decomposition with four bands was selected, utilizing the most trivial wavelets, originally introduced by Haar and specifically the non-redundant Discrete Wavelet Transformation (DWT) is used. The next stage is transforming the produced bands using the DCT. The watermark casting is performed according to the following additive rule:

$$t_i' = t_i + \alpha t_i x_i \tag{9}$$

where t_i are the transformed coefficients, are the watermarked coefficients and x_i is a random sequence of Gaussian distribution, used as a watermark. The a-parameter specifies the casting strength. The watermark casting method is being presented in Fig. 1. The detection process is accomplished using the correlation detector. Besides the correlation function, a detection threshold is necessary for the detector to decide upon the presence of a watermark. The selection of a threshold value was based on an extensive experimental procedure which included ad-hoc threshold definition, watermarking key detection and statistical processing of the results. The result was an optimal threshold value for the proposed detection process. The driving force for deciding on this method was the increased robustness achieved as a consequence of the DCT utilization, in combination with wavelets, capable of maximizing the watermarks visual masking effects.

2.4. Spread spectrum multibit watermarking technique

The embedding of a robust multibit watermark is accomplished through casting several zero-bit watermarks onto specified coefficients. The image watermark, a random sequence of Gaussian distribution in our case, is casted multiple times onto the selected coefficients preserving the same sequence length but shifting the start point of casting by one place. Actually the final watermark that will be embedded into the image is not a single sequence but many different sequences generated with different seeds. These sequences will be casted, one after the other, on the mid coefficients of the image, using the additive rule mentioned above and begging from successive starting points. If all sequences where to be casted, beginning from the same starting point, then, besides the severe robustness reduction resulting from the weak correlation, the possibility of false positive detector response would dramatically increase, since every number that has participated as a seed during the sequence generation procedure, will be estimated by the detector as a valid watermark key. Shifting the starting point by one degree for every sequence casting ensures that the false positive rate will remain in very small level due to the artificial desynchronisation introduced. Every single random sequence of Gaussian distribution is generated using a different number as the seed for the Gaussian sequence generator. It is important to differentiate the sequences in order not to mislead the detection mechanism, since it is based on the correlation between the extracted sequence and the sequence produced with the watermark key.

The watermark key is responsible both for the generation of the first sequence and the construction of a vector, containing the rest of the numbers that will serve as the corresponding seeds. The placement of several Gaussian sequences into the image content can model, under specific conventions, a multibit watermark (Figs. 2 and 3). The detection of a zero-bit watermark is interpreted as if the bit value of the specified bit is set to one. On the contrary, failure of the detector to detect the zero-bit watermark leads to the conclusion of a zero bit value. Thus, in order for a message to be casted into the image content, it is initially encoded using the binary system and applied afterwards in the sense of zero-bit watermarks using the embedding mechanism and according to the derived bit sequence. Fig. 4 presents a sample pseudo-code of the multibit watermarking scheme.

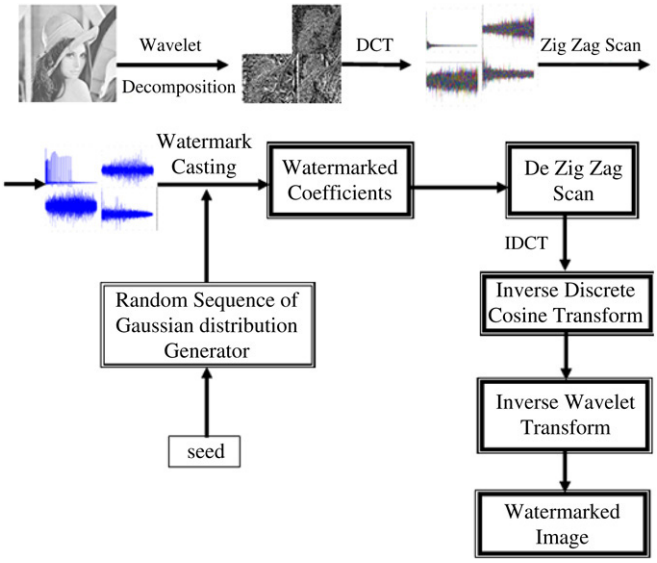

Fig. 1. Watermark casting.

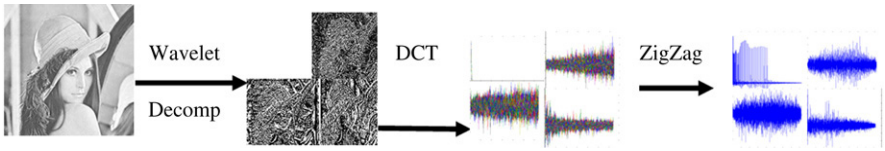

Fig. 2. Zig–zag coefficients of the LL band.

Some important remarks regarding the novelty of the proposed schema are addressed below.

Data payload: The reason that most of the proposed robust watermarking systems are zero-bit, is highly related to the data payload. Data payload is the amount of information encoded into the image during the watermark procedure. In other words, it is the number of coefficients modified according to the additive rule. The performance of the correlation function adopted by the detector is increased when a strong statistical dependency is present. On the other hand, the statistical dependency requires a significant sequence length in order to fulfill the requirements of the correlation function. In addition, the position and the amount of coefficients modified, affects directly the resulting image quality. This is one of the most important tradeoffs that the designer of a watermarking system has to balance.

Casting multiple sequences will maximize the problem of image distortion. In that sense, the maximum number of bits allowed for encoding the watermark message is crucial. In the proposed scheme a total number of 16 bits were selected. The first bit indicates the existence of a watermark. If the response is positive the detector continues with the following zero-bit watermarks, otherwise the mechanism outputs a negative response. This is a useful shortcut saving the detector of valuable time and processing power. The second bit serves as a flag important for the decoding operation. The role of this bit flag is described in detail in the following paragraph. The next 14 bits are dedicated to the encoding of the watermark message. Under the aforementioned conventions the system is capable of embedding 2^{14} different messages.

Seed Vector Generation: The watermark key is a positive integer value playing a vital role in the overall watermarking procedure. It corresponds to the private information that must be shared between the embedder and the detector of the watermark. One of the basic principles of private watermarking is that the encryption of the information to be embedded is performed according to a private key. Thus, if an image is watermarked using a specified key, it is impossible for the detector to detect the watermark unless provided with the same key. The encryption is accomplished by using the private key as the seed for the pseudo-random sequence of Gaussian distribution generator. In our case, there is the necessity of 15 extra numbers, one for each sequence. Thus, the private key except from its basic operation as a pseudo-random generator seed is also used as the seed for producing a vector containing 15 numbers. It is important for every private key to produce a different vector of numbers, in order to avoid undesirable statistical dependencies between different watermarks. A pseudo-random generator provided by any compiler is capable of applying this one-way relationship between the private key and the produced vector of numbers.

Flag bit operation: Under the convention, that for every one-bit-value we cast a zero-bit watermark and for every zero-bit-value we don't do anything except moving to the next starting point, the number of zero-bit watermarks to be casted is dictated by the bit sequence. It is obvious that a bit sequence containing only a single one-bit-value is preferable from a

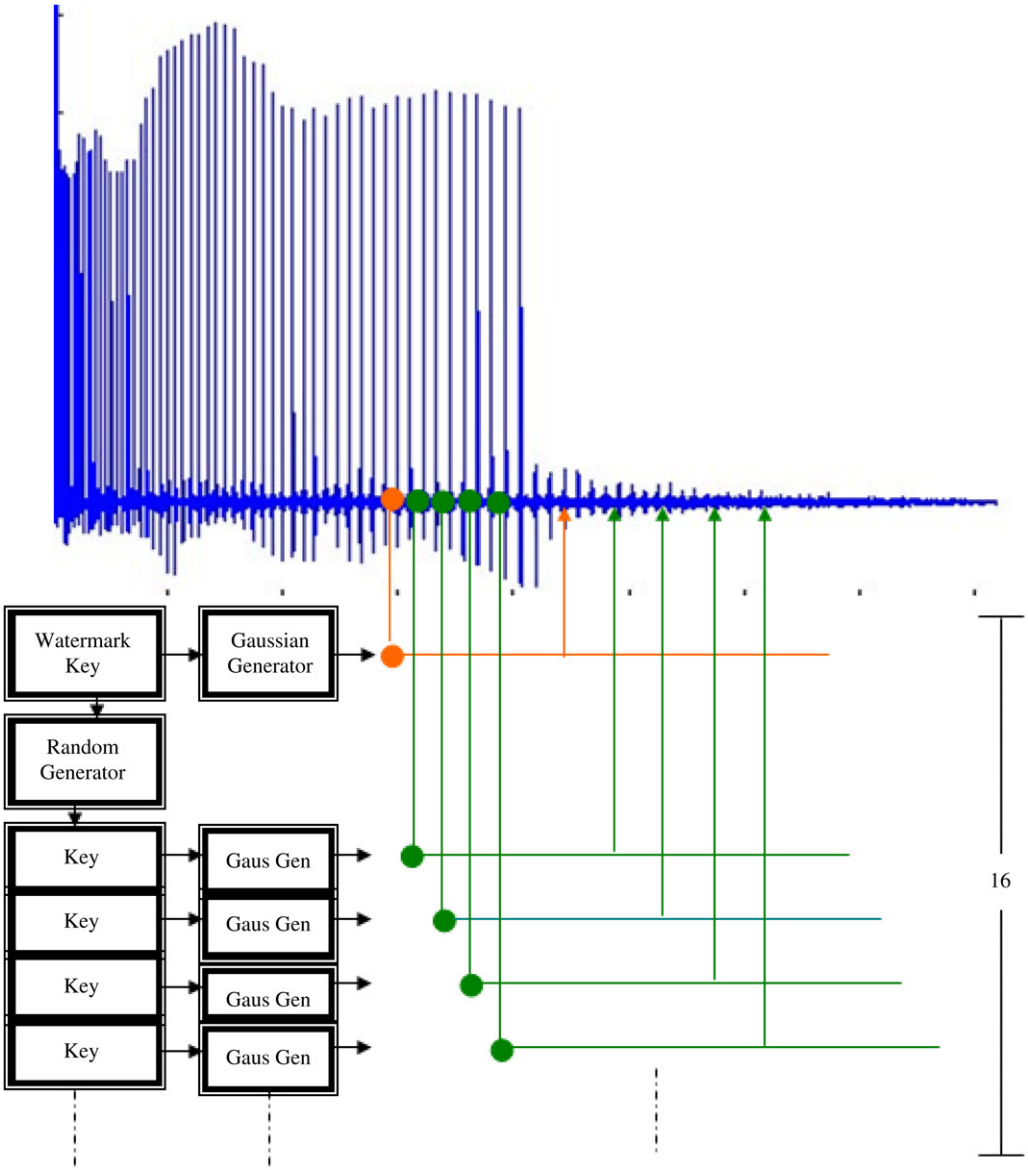

Fig. 3. Multibit watermarking.

sequence consisted of 14 aces. Both for, processing power and watermarks imperceptibility purposes, a bit reversal trick is required for optimizing the embedders performance.

Thus, after acquiring the binary representation of the message, a counter scans the bit sequence counting the zeros and the aces. If the number of aces is grater than the number of zeros a bit reversed sequence is generated. The zero-bit watermarks casting is now performed according to the newly generated sequence. In that case, the flag bit is set to one serving as an indicator to the detector that the extracted sequence is bit-reversed. As a consequence, the decoder, equipped with the appropriate information, can easily decode a message represented by 14 aces binary sequence, even though the embedder had casted only two zero-bit watermarks. The benefit of using the specified trick is that even though a 16-bit watermark is supported, we only need to cast 8 zero-bits watermarks in the worst case.

2.5. Evaluation and robustness

In this section the experimental results concerning the evaluation and robustness of the watermarking algorithm are being presented. Robustness is the most highly desired feature of a watermarking algorithm especially if the application demands copyright protection, and persistent owner identification. In addition the image distortion and false positive parameters are being evaluated.

```
void watermark_main(int iQuadraticFrameSize, long key, long M1, long L1, long
M2, long L2, int Strength)
{
initialization
M1  -> starting coeff, 1st level decomposition, all bands except LL
M2  -> starting coeff, 1st level decomposition, only LL band
L1  -> number of coeffs to change, 1st level decomposition, all bands except LL
L2  -> number of coeffs to change, 1st level decomposition, only LL band
key -> watermarking key
IF the image is grayscale start from the beginning of the image
ELSE use the quadratic frame located on the image center
IF exists handle the remaining pixels
//----------1o decomposition----------
add_hor_add_ver(ll, lh, hl, hh);
//----------Watermark medium frequency bands---
watermark(lh, key, L1, M1, strength);
watermark(hl, key, L1, M1, strength);
watermark(hh, key, L1, M1, strength);
watermark(ll, key, L2, M2, strength);
//----------Synthesis stage----------
band_synthesis(ll, lh, hl, hh);
// Do the other way around if grayscale of RGB
}
void watermark(long key, long int L, long int M, double a)
{
initialization
do {
        temp=row*N+col;
        v[temp]+=a*fabs(v[temp])*gasdev(&seed);
        count++;
    }
}
```

Fig. 4. Pseudo-code.

In our experiments the metric selected for evaluating the image distortion introduced by the multi-bit watermark casting is PSNR (Pick Signal to Noise Ratio). Although PSNR is definitely insufficient for modeling the complexity of the human visual system is by all means an effective metric for measuring image similarity. The experiments proved that in most cases the PSNR value was above 40 dB (Fig. 5), which is satisfactory and the derived results can be consider to meet the image quality requirements.

Casting multiple zero-bit watermarks onto the same coefficient area raises the probability of causing abnormal fluctuation of the detectors false positive probability. In order to confirm that no such case is true, we used 5 different watermarks applied to a sample of 5 images for approximating the false positive probability. The watermarks were generated from 5 different integer numbers, also responsible for the generation of the vector containing the rest integer values required by the embedding mechanism. Every image was watermarked using each of this numbers as a watermark key while afterwards the detector was tested for possible false positive response with every number contained in the produced vector. That is, an image watermarked with the number K1 as a watermark key was examined by the detector 15 more times using as primary keys the numbers of the vector produced by the random generator with K1 as a seed. The reason for examining only this small subset of numbers instead of a large random set is that this numbers hold highest probability of causing a false positive, due to the statistical dependence introduced to the correlation function. Fig. 6 demonstrates the experimental results. The above diagram indicates only one false positive response under the Plate image. Thus, the derived conclusions justify our hypothesis about the false positive probability of the detector which remains in relatively low values, thanks to the statistical independence introduced by the embedding start point shifting. The watermark's robustness has been extensively tested. The average score of the watermarking robustness against various types of attacks is 94% which is a very efficient result for the type of application under consideration. The results are briefly analyzed in Fig. 7. Closing the performance evaluation it is worth mentioning the results derived from the print-scan or digital to analog attack. A small number of images after they have been compressed with a jpeg algorithm, they were printed to plain paper. The images were scanned back to their digital form and delivered to the watermark detector. The detector output is presented in the Fig. 8.

Based on the above analysis and evaluation the advantages of the proposed multi-bit watermarking scheme as compared with the state of the art are the following. At first the proposed multi-bit watermarking scheme is independent of the core

Image Database				
Original Images				
				
Chariot	Horse	Mask	Plate	Scene
Watermarked Images				
				
Water_chariot	water_horse	water_mask	water_plate	water_scene
PSNR	PSNR	PSNR	PSNR	PSNR
66.65	69.52	64.90	68.36	65.99

Fig. 5. PSNR.

Keys					Chariot					Horse					Mask					Plate				
50	100	200	350	700	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
22715	12662	25325	27935	23102	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
22430	23392	25316	28203	2170	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
16275	22561	2367	21228	32468	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
21417	20718	19320	17222	12328	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4906	6314	9131	13355	23212	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
9000	1073	17987	26975	4255	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3863	24449	86	29076	9340	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
26227	32712	12916	32372	12235	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
20017	27912	10934	1851	24347	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
21604	2031	28420	2467	29292	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
28180	11332	10403	25394	5760	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
940	7595	20906	8104	21924	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
13042	20424	2421	24568	10709	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
26566	10606	11456	29111	15696	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
20934	20780	20474	20015	18943	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Fig. 6. Key seed—one false positive.

Type of Attack	Average Score
Convolution and Median Filters	100%
Jpeg Compression	90%
Scaling	100%
Cropping	95%
Shearing	93%
Rotation – Crop	97,5%
Rotation – Crop – Scale	79%
Linear Transformations	100%
Aspect Ratio	100%
Row and Column Removal	100%
Geometric Distortion	80%

Fig. 7. Watermarking robustness.

watermarking method, as the encrypted information is embedded into the frequency domain, leading to a robust solution. Secondly, the watermarking scheme has the unique, compared with the existing watermarking algorithms, capability of embedding 2^{14} different messages to the digital image without quality degradation, while at the same time the false positive probability of the detector remains in low values. As a result the trade-off between the data payload, the image quality degradation and watermarking robustness for the proposed scheme is optimal. In fact the robustness of the watermarking scheme is comparatively high (94%) ranking amongst the best of the available watermarking algorithms based on the studies conducted in [11]. In accordance with these studies the overall 93% of robustness was the best at that time for the watermarking algorithms and the overall 80% was for the second best algorithm.

Image Format	Image Compression	Print Quality	Result
Tiff	None	Best	Detected
Tiff	None	Normal	Detected
Jpeg	Medium Compression High Quality	Best	Detected
Jpeg	Medium Compression High Quality	Normal	Detected
Jpeg	Medium Compression Medium Quality	Best	Detected
Jpeg	Medium Compression Medium Quality	Normal	Missed

Fig. 8. Print scan or digital analog attack.

3. Concluding remarks

Most of the effort addressed in this work was dedicated on formulating a novel technique to embed robust multibit watermarks into digital images. The result was a technique applicable to every spread spectrum frequency domain watermarking method capable of hiding 2^{14} different keys while maintaining a sufficient level of robustness. Special care was taken on resolving the potential problems derived from the process of casting multiple zero-bit watermarks onto the same coefficient area. Issues like the false positive probability, the image quality degradation and the robustness achieved by the proposed scheme were subject to thorough examination and evaluation.

References

[1] M. Barni, F. Bartolini, A. De Rosa, A. Piva, Optimum decoding and detection of multiplicative watermarks, IEEE Transactions on Signal Processing 51 (4) (2003) 1118–1123.
[2] Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Digital Watermarking, Morgan Kaufmann Publishers, 2002.
[3] Ingemar J. Cox, J. Kilian, T. Leighton, T. Shamoon, Secure spread spectrum watermarking for multimedia, IEEE Transactions on Image Processing 6 (1997) 16731687.
[4] Computer Science and Telecommunications Board, National Research Council, The Digital Dilemma: Intellectual Property in the Information Age, National Academy Press, Washington, 1999, pp. 2–3.
[5] V. Fotopoulos, A.N. Skodras, A subband DCT approach to image watermarking, in: X European Signal Processing Conference, EUSIPCO-2000, 5–8 September, Tampere, Finland, 2000.
[6] House of representatives, Digital Millennium Copyright Act, October 1998.
[7] S. Katzenbeisser, F.A.P. Petitcolas, Information hiding—techniques for steganography and digital watermarking, in: Computer Series, Artech House, 2000, pp. 95–172.
[8] Randall Davis, The digital dilemma, Communications of the ACM 44 (February) (2001) 80.
[9] P. Wayner, Disappearing Cryptography—Information Hiding: Steganography and Watermarking, second, Morgan Kaufmann, 2002, pp. 291–318.
[10] T. Kalker, Considerations on watermarking security, in: IEEE Multimedia Signal Processing, MMSP01 Workshop, Cannes, France, 2001, pp. 201–206.
[11] D. Tsolis, G. Tsolis, P. Papatheodorou, A watermarking environment and a metadata digital image repository for the protection and management of digital images of the Hellenic cultural heritage, in: IEEE International Conference in Image Processing, ICIP 2001, Thessaloniki, Greece, 2001.