DIGITAL WATERMARKING OF IMAGES AND WAVELETS

Alexandru ISAR

Electronics and Telecommunications Faculty, "Politehnica" University, Timișoara
2 Bd. V. Pârvan, 1900 Timișoara, 40 56 190608, isar@hermes.ee.utt.ro

Abstract. The aim of this paper is a new digital watermarking method. This is a very simple and very fast method. At its basis stays the D.W.T. This transform has a great advantage, its details separation capacity. From this characteristic is inspired the title of the paper. First is established the place of the digital watermarking between the information security methods. Then are presented the new watermark embedding and extraction methods and some simulation results are reported. The digital watermarking method, presented in this paper, can be slightly modified, to embed in the watermark a text containing different information about the watermarking process, named private key. So, a new encryption method of this private key, based on the transmission of images, was obtained. The robustness of the new digital watermarking method against some attacks, like the JPEG compression, was studied. Because the proposed method is fragile against attacks based on translations, in the last paragraph is suggested the substitution of the D.W.T. with a discrete translations invariant wavelet transform.

Keywords: information security, multimedia, watermarking, discrete wavelet transform.

I. Data Security Issues

One of the most important characteristic of a good software or telecommunications product is its security. This is the reason why the research in the field of security becomes more and more important today. The first objectives of the security are:

- the transmitted information confidentiality,
- the transmitted information integrity,
- the transmitted information authenticity,
- the transmitted information non-repudiation,
- the disposability of the required information and of the required services,

One of the most important objective is the preservation of the transmitted information authenticity.

At the basis of any security algorithm (required for the realisation of one of the objectives already mentioned) stay an encryption method. There are two kinds of encryption methods: the symmetric encryption and the asymmetric encryption.

The most important disadvantage of the symmetric encryption algorithms is the necessity to transmit the encryption key, using an unsecured channel.

This is the reason why for the symmetric encryption keys management, asymmetric encryption algorithms are used.

The first asymmetric encryption algorithm was proposed by Professor Martin Hellman, from Stanford University and by he's ex-student Whitfield Diffie, in 1976, [2]. This algorithm was named the Diffie - Hellman algorithm. It permits to the receiver to verify the authenticity of the emitter, too. The authenticity can be verified by another person or system connected in the same network. This kind of authenticity check is very important and was intensively developed in the last years. The author of the message sends a transformed form of another message, related with the first one, to a third entity. Processing this transformed form of the messages the third entity can establish the author. Today, digital signatures or digital envelopes (the transformed forms of a message) are used by specialised systems or organisations to check the authenticity of a message [3].

II. Data Security and Multimedia

The wide-spread communication of multimedia data has created a growing need to protect digital information against illegal duplication and manipulation. Advances that facilitate electronic publishing and commerce also heighten threats of intellectual property theft and unlawful tampering. One approach to address this problem involves embedding an invisible structure into a host signal to mark its ownership. These structures are called digital watermarks and the associated embedding process digital watermarking. One major driving force for research in this area is the need for effective copyright protection scenarios for digital imagery, sound and video. In such an application a serial number is embedded into the signal to protect, to identify the copyright holder. So the objective is an authenticity
check. It is expected that an attacker will attempt to remove the watermark by intentionally modifying the watermarked signal.

At present, digital watermarking research primarily involves the identification of effective signal processing strategies to discreetly, robustly, and unambiguously hide the watermarked information into multimedia signals. The general process involves the use of a key which must be used to successfully embed and extract the hidden information. The embedding mechanism entails imposing imperceptible changes to the host signal to generate a watermarked signal containing the watermark information, while the extraction routine attempts to reliably recover the hidden watermark from a possible tampered watermarked signal.

### III. Digital watermarking of still images

One of the most used multimedia signals category is that of images. For example 80% of the data transmitted using the INTERNET are images. This is the reason why is very important to study the digital watermarking methods of images.

In this paper, is considered the problem of digital watermarking to ensure the credibility of multimedia. We specifically address the problem of digital watermarking for the tamper-proofing of still images. Applications of our problem include authentication for courtroom evidence, insurance claims and journalistic photography. A novel watermarking approach which embeds a watermark in the discrete wavelet domain of the image is presented. Tamper detection is possible in localised spatial and frequency regions. Unlike previously proposed techniques, this novel approach provides information on specific frequencies of the image that have been modified. This allows the user to make application-dependent decisions concerning whether an image, which is JPEG compressed for instance, still has credibility. Analysis is provided to evaluate the performance of the technique to varying system parameters. In addition, we compare the performance of the proposed method to existing watermarking techniques to demonstrate the success and potential of the method for practical multimedia tamper-proofing and authentication.

### IV. Image processing using wavelets

The discrete wavelet transform of an image transforms that image into two parts: an approximation part and a detail part. So, using this transformation the details of an image can be extracted. This is a great advantage and it permits to implement efficiently some image processing methods. For example the small details can be rejected, obtaining an images compression method. This method stay at the basis of the last images compression standard, JPEG 2000, [4].

Another application of the wavelets theory in the field of image processing is the de-noising of images. The control of the details of an image permits to identify the invisible ones. Transforming these details, a new image, very similar with the original one, can be obtained. This new image can be regarded like the watermarked image associated to the original one. Their difference can be considered the watermark embedded in the original image. So the discrete wavelet transform can be used to embed a watermark into an image. This is the connection between the wavelets theory and the digital watermarking of images representing the title of this paper.

There are a lot of papers dealing with the use of wavelets theory to images watermarking. For example, the standard JPEG 2000 can be used for the digital watermarking of images, [5]. The Professors Deepa Kundur and Dimitrios Hatzinakos, from the University of Toronto, have written some papers on the subject of the use of wavelets theory for the digital watermarking of images, [6], [7]. An international research team, where Romania is represented by Professors Borda and Naforntita, studies the connection between the theorie of wavelets and the digital watermarking, [8].

### V. Digital watermarking and wavelets

A very modern transformation is the Discrete Wavelet Transform (D.W.T), [9]. The most important advantage of this transformation is its separation capacity. The DWT of an image has two parts: an approximation part (this is an image with smaller dimensions) and a detail part (this is a set of images with smaller dimensions containing the details of the original image). Hence the DWT gives the access to the details of the original image. This is very important because changing only the less important details of an image is easy to insert a watermark in this image, keeping the insertion procedure invisible. This can be a very simple and fast procedure.

### VI. Amplitude modulation of DWT coefficients

The values of the DWT coefficients corresponding to the less important details can be changed using an amplitude modulation technique. One of the simpler watermark insertion techniques is described in the following.

### VII. The watermark insertion system

This system is presented in figure 1. This is an adaptive insertion system. The watermark $w_a$ depends of the details of the original image (O.I.) and of the value of the constant $K$. The watermark can be generated very easy making the difference between the original image and the watermarked image (W.I.). The transformed image (T.I.), obtained at the output of the system that computes the D.W.T. of the input image, is composed of an approximation sub-image $A$ and a sequence of detail sub-images $D_k, k = 1...6$.
The less important details are contained in the detail images, $D_4$, $D_5$, and $D_6$. The block called DETAILS SEPARATOR, in figure 1, extracts these sub-images. The block called APPROXIMATION SEPARATOR, in figure 1, makes the extraction of the image formed with the sub-images $A$, $D_1$, $D_2$, and $D_3$, (A.I.). The pixels of the images D.I. (representing the details less important of the original image) are multiplied with the constant $K$. Their amplification is not visible in the watermarked image if the value of the constant $K$ is well chosen (not too big). There is a domain of values of this constant, large enough, which keep the watermark insertion procedure invisible. The role of this constant is similar with the role of a key for an information security system. After this “modulation” of details the new detail images $D_4$, $D_5$, and $D_6$ are obtained. These represent the new detail images N.D.I. Using the sub-images A.I. and $D_4$, $D_5$, and $D_6$, with the aid of the block called ASSEMBLER, in figure 1, the new transformed image, N.T.I. is generated.

The watermarked image is obtained computing the Inverse Discrete Wavelet Transform (I.D.W.T) of the image N.T.I. This is the image to be offered to different users (the image to be transmitted in the INTERNET network, for example).

The watermark can be generated, using this image, very easy, making the difference between the images O.I. and W.I.

$$w_a = O.I. - W.I.$$

This “modulation technique”, used for the insertion of the watermark in the D.W.T. domain is fast and very simple. This is an adaptive insertion technique because the position and the values of the most important coefficients in the N.D.I. depend of the image O.I. It is easy to find values for the constant $K$ such that this insertion procedure to be invisible. So, the necessity to use any perceptual domain technique is avoided. Such techniques must be used if the energetic content of the watermark must be increased.

**VIII. The watermark extraction system**

When the authenticity of a certain watermarked image must be verified the watermark contained in this image must be extracted. The watermark extraction system is presented in figure 2.

At the input of the watermark extraction system is connected the image to be tested (the owner of this image must be established). Let us call this watermarked image received, $W_I_r$. If this image was not attacked it can be said that there are not transmission errors. These errors
can appear due to the compression of the image for example. If this hypothesis is satisfied, then:

\[
W_{I_r} = WI
\]  

(1)

In the following, to explain the watermark extraction system, we will suppose that this relation is true. After the computation of the D.W.T. the image \( T_{W_I} \), with:

\[
TW_{I_r} = \text{DWT}\{WI\} = TWI
\]

is obtained. At the output of the DETAILS SEPARATOR block, the detail images \( D\{TWI\} \) are obtained. If the relation (1) is satisfied then these sub-images are \( D_4, D_5 \) and \( D_6 \). At the output of the APPROXIMATION SEPARATOR block is obtained the image \( A\{TWI\} \). If the relation (1) is true then this image is composed by the sub-images \( A_1, A_2 \) and \( A_3 \).

The detail sub-images \( D_4, D_5 \) and \( D_6 \) are multiplied with the constant \( K \), obtaining the old detail images \( O\{D\{TWI\}\} \). In fact the images \( D_4, D_5 \) and \( D_6 \) are obtained. These are the details contained in the DWT of the image \( O.I \). At the output of the ASSEMBLER block is obtained the image \( T\{OI\} \). If the relation (1) is true then this image represents the DWT of the original image. Computing the IDWT of this image the image \( O.I \) is obtained. This is just the original image, if the relation (1) is satisfied. Making the difference of the images \( O.I_r \) and \( W_{I_r} \) is computed the image \( w_{ar} \). This represents the result of the extraction of the watermark. If relation (1) is satisfied then:

\[
w_{ar} = w_a
\]  

(2)

If there are transmission errors then the functions \( w_{ar} \) and \( w_a \) are different. Their difference must be small if the watermark insertion procedure is robust. To measure the similarity of these two functions their correlation factor is computed:

\[
f_c = \frac{\sum \sum w_a[m,n] \cdot w_{ar}[m,n]}{\sqrt{\sum \sum w_a^2[m,n] \cdot \sum \sum w_{ar}^2[m,n]}}
\]

This factor brings its highest value, 1, when the two watermarks are identical (when the relation (2) is true). The condition (2) is satisfied in the absence of any attack against the image \( WI \).

**IX. An example**

In this paragraph are presented some results obtained using the method already described. These results, presented in figure 3, correspond to a single selection of the secret constant \( K \). Similar results can be

*Figure 3. The results obtained in this example.*
values are selected from an invisibility domain (see the next paragraph). The value of the constant $K$ used in this experiment is 1.1. The wavelet mother used is Dau 4, and the number of iterations of the wavelet transforms used is 3. The watermarked image was applied to the input of the watermark extraction system. The correlation factor of the images $w_a$ and $w_{ar}$ obtained is equal with 1.

**X. The analysis of the robustness of the proposed watermarking method**

It is very important to know if a watermarking method is resistant to attacks. Some experiments realised with the goal to respond to the question if the proposed watermarking method is robust or not are presented in the following.

**XI. How to choose the constant $K$?**

This constant must be chosen such that the watermark insertion to be invisible. An experiment with the goal to determine the domain of values for $K$ for which the insertion procedure is invisible was realised. The mean square error between the images O.I. and W.I. was computed for different values of $K$. If the error's value was inferior to 0.1% of the energy of the original image then the value of $K$ was retained. This threshold value is used in transparent images compression methods, too. For the image O.I. presented in figure 3, the invisibility domain found for $K$ is:

$$K \in \left[1.0 \times 10^{-14}, 1.6686\right]$$

Another interesting question is if the same image can be watermarked with different watermarks using the proposed watermarking method. With other words, there are different values of $K$ to produce different watermarks for the same image? If so then the same image can be watermarked with different watermarks for different users. So, a certain watermark could be associated with a certain couple (owner, user) with the aid of the value of the constant $K$. To establish the step between two different values of the constant $K$, $K_1$ and $K_{i+1}$, associated with two different watermarks (of the same image), the following experiment was realised. The two watermarks corresponding to the two consecutive values of the constant $K$, $K_1$ and $K_{i+1}$ are generated using the method already presented. These two values must be in the invisibility domain already determined. The energies of the two watermarks are computed and then the absolute value of the difference of the two energies is determined. If this difference is inferior to 10% of the energy of the first watermark (generated using the constant $K_1$) then the distance between the two values $K_i$ and $K_{i+1}$ is too small and the value $K_{i+1}$ must be increased. For the original image in figure 3 the step value, obtained using the method already presented is of 0.00488.

**XII. The robustness against compression**

In the following are described two experiments. The goal of the first experiment is to make a comparison between two compression methods. The first is based on the use, in the compression system, of the Discrete Cosine Transform (D.C.T.) and the second is based on the use of the Discrete Wavelet Transform (D.W.T.). The coefficients obtained in the two cases (first the DCT coefficients and second the DWT coefficients) are compared with a threshold and all the coefficients inferior to the threshold are rejected (set to zero).

The compression factor is proportional with the number of rejected coefficients. For different threshold values, different compressed image (C.I.) are obtained, for the same initial image I.I. Some of them were obtained using the D.C.T. and others using the D.W.T. We consider in the following that the input image was a watermarked image:

$$I.I. \equiv W.I.$$

From every compressed image C.I. (already obtained) the watermark was extracted. The correlation factor between the generated watermark ($w_g$) and the extracted watermark ($w_{ar}$) was computed for any threshold value in the two cases (when the D.C.T. is used and when the D.W.T. is used). The dependence of this correlation factor of the number of rejected coefficients for the compression of the image in figure 3 (the value of $K$ was 1.1) is presented in figure 4, for the compression based on D.C.T. (the continuous line). The same dependence for the case of the use of the D.W.T. is presented in the same figure (the dashed line). Comparing the two lines it can be said that the proposed watermarking method is more robust against the compression based on the D.W.T. This is an important result because the use of D.W.T. in image compression applications becomes a standard procedure. The watermarked image used in the experiment already described was that presented in figure 3. The value of constant $K$ used to generate the watermark was 1.1. The conclusion of this experiment is the superiority of the D.W.T. against the D.C.T. for compression purposes from the point of view of the proposed watermark insertion procedure.

The second experiment, [11], was realised to study the robustness of the proposed watermarking method against the JPEG compression. In this respect the watermarked image W.I. from figure 3 was compressed using the JPEG compression standard implemented in the software ADOBE PHOTO SHOP. Different compression factors were chosen. In every case a watermark image was obtained. An original image W.I. was reconstructed in every case (using the reconstruction procedure offered by the same software).

Because the JPEG is a lossy compression method the reconstructed images are different (for every compression
factor) and differ from the image \( W.I. \). From the images \( W.I. \), the watermarks \( w_{ar} \) are extracted. The correlation factors between the generated watermark \( w_a \) and the extracted watermarks \( w_{ar} \) are computed. The dependence of this correlation factor of the compression factor is presented in figure 5. Comparing this result with the result presented in [6] (in figure 3) the superiority of the watermarking method proposed in this report can be observed. So, the method proposed here is most robust than other watermarking methods based on wavelets. This method is very fast too. It is one of the simpler watermarking method proposed in the literature. In [6] to embed the watermark in the domain of the D.W.T. is used a quantization phase. This idea can be very useful because the quantization operation is used in any compression system. The drawback of any quantization method is its irreversibility. So the equivalent of the uniform quantization process in security terminology is a hash function. This is the reason why the use of a quantization stage must be done with care. In [10] is presented a study of the irreversibility degree of the uniform quantization process.

XIII. Some developments of the proposed method

The information required for the implementation of the proposed method consists of the value of the constant \( K \) and the parameters of the D.W.T: the wavelet

![Figure 4. The robustness against compression.](image)

![Figure 5. The robustness against JPEG compression.](image)
mother and the number of iterations. All this information can be regarded like a public key. The owner of the image can be interested also in the transmission of other characteristics of that image:
- the date of its generation,
- some technical characteristics like the number of pixels or the number of colours,
- some characteristics of the user of the image,
- some characteristics of the owner of the image.
All these characteristics can form a private key. So, is interesting to complete the watermarking insertion procedure, already described, with the facility of supplementary embedding of an informational content.

XIV. The insertion of an informational content into the watermark

All the details of the image obtained using the proposed watermarking method are multiplied with the same constant K (or 1/K). There is the possibility to multiply with this constant only some details. Such a method was described in [12]. These details can be selected with the aid of the informational content. This task can be accomplished doing the following steps:
- The text containing all the characteristics of the image to be watermarked is coded, using for example the Huffman coding technique,
- The code is transformed in binary form,
- The binary form is transformed into a matrix, called support matrix,
- The support matrix is used for the generation of the watermark in the wavelet transform domain. The indices of the elements of this matrix, of value 1, are considered the spatial coordinates of the pixels in one of the details image obtained after the computation of the D.W.T. of the image to be watermarked. The values of those pixels will be added with the biggest detail value and the sum obtained will be multiplied with the constant K. The indices of the elements of the support matrix, obtained at the anterior step, of value 0, are considered the spatial coordinates of the pixels in the same details image and the value of those pixels will be multiplied with the constant K. So is obtained the new sequence of detail images.
- The rest of the watermark embedding method remains unchanged. Using the new sequence of detail images and the image A. I., is assembled a new image. Computing the I.D.W.T. of this image a new watermarked image is obtained. Making the difference between this image and the original one can be obtained the new watermark.

So, the private key is embedded in this watermark. Extracting, at the receiver, the watermark, the private key can be reconstructed. The steps of this procedure are the followings:
- The D.W.T. of the received image is computed. The details images are separated. The details of the original images are extracted, using the corresponding inverse operations of the operations described in the watermark generation in the wavelet transform domain step. The support matrix is extracted too. The D.W.T. of the original image is assembled. Computing the I.D.W.T., the original image is obtained. Making the difference between the original image and the received image, the watermark is extracted.
- Using the support matrix, after a Huffman decoding procedure, the text of the informational content of the watermark can be recovered.

XV. A translations invariant discrete watermarking method

The D.W.T. is not a translations invariant transformation. This is the reason why the digital watermarking method proposed in this paper is not translations invariant. Making some small translations on the watermarked image (invisible), the watermark contained in this image can be destroyed. So, the digital watermarking method proposed in this paper is sensitive to attacks based on translations. This is the reason why a translations invariant wavelet transform could stay at the basis of a better digital watermarking method. There are two kinds of translations invariant discrete wavelet transforms: redundant and non-redundant. Two redundant transformations are proposed recently by Kingsbury, [13] and Selesnick, [14]. A non-redundant transformation, based on wavelet packets, was proposed by Israel Cohen [15] and enhanced recently by Quinquis and Ioana, [16]. The use of such a wavelet transform in the system drawn in figure 1 and of its inverse in the system drawn in figure 2 will be a future preoccupation of our research team.

XVI. Conclusion

A new digital watermarking method is reported in this paper. First is established the role of the authentication in the field of information security. Then is highlighted the role of the image processing theory in the field of multimedia applications. An example of fusion of the fields of information security and image processing is represented by the digital watermarking techniques. These techniques have a rapid growing today. There are some sites on INTERNET presenting researches on this topic. For example:
http://dynamo.ecn.purdue.edu/~ace/water2/digwmk.html
This is the reason why the subject of this paper is the digital watermarking. The method proposed in this paper is very simple and very fast. At its basis stays the D.W.T. This transform has a great advantage, its details separation capacity. From this characteristic is inspired
the title of the paper. First are presented the watermark embedding and extraction methods. Second some simulation results are reported. On the basis of these simulations some characteristics of the investigated method are extracted and reported. The robustness of the new digital watermarking method against some attacks, like the JPEG compression, was studied. Maybe this robustness can be improved tacking into account a quantization process at the level of the embedding of the watermark in the discrete wavelet transform domain.

The digital watermarking method, presented in this paper, can be slightly modified, to embed in the watermark a text containing different information about the watermarking process, named informational content. So, a new encryption method of this informational content, based on the transmission of images, was obtained. This is a very interesting research field with great potential for the military secret communications. Due to the watermark embedding technique based on wavelets theory, reported in this paper, an important amount of text can be encrypted using a single image. Because the proposed method is fragile against attacks based on translations, in the last paragraph is suggested the substitution of the D. W. T. with a discrete translations invariant wavelet transform. This substitution is the object of a future paper. A research on this topic was already initiated in the research team where the author of this paper belongs.

Acknowledgement

The author want to thanks Professor Nafornta for all the fruitful discussions on the topics of this article and for the encouragement to work in this very interesting field. A part of this work, connected with the image compression methods, was granted by AUPELF-UREF, under the Grant "Méthodes modernes de traitement du signal pour la compression de données dans les modems haut débit".

References

[6] Deepa Kundur and Dimitrios Hatzinakos, "Digital Watermarking Using Multiresolution Wavelet Decomposition", (mail to deepa@comm.toronto.edu, dimitris@comm.toronto.edu).
[7] Deepa Kundur and Dimitrios Hatzinakos, "Digital Watermarking for Telltale Tamper-Proofing and Authentication", (mail to deepa@comm.toronto.edu, dimitris@comm.toronto.edu).
[8] G. Wade, C. Serdean and A. Ambroze (Department of Communication and Electronic Engineering, University of Plymouth), M. Borda (Communications Department, Technical University of Cluj-Napoca, Romania), I. Nafornta (Communications Department, Politechnica University of Timisoara, Romania), "Watermarking uncompressed video: an overview", Invited Paper, Bulletinul științific al Universității "Politehnica" din Timișoara, Seria ELECTRONICĂ și TELECOMUNICAȚII (TRANSACTIONS on ELECTRONICS and COMMUNICATIONS), Tom 45(59), Fascicola 1, 2000.