Fourth International Conference
Modelling and Development of Intelligent Systems
October 28 - November 1, 2015
"Lucian Blaga" University
Sibiu - Romania

# Ownership tracking with dynamic identification of watermark patterns

**Dana Simian, Ralf Fabian**

**Abstract**

The demand of adaptation in marking digital content for later author identification has become of huge interest given that nowadays it has become easier than ever to acquire and copy multimedia content. The paper focuses on visual content based owner or author identification applicable to digital images. It builds on a survey of techniques designed for minimal image quality loss. The techniques employed are chosen to reduce tempering visual delight of an image and making inserted information hardly detectable or removable. We propose an architecture for a system intended to provide digital watermarking services with automatic ownership tracking. The main issue in this endeavour is to overcome pattern degradation if the host image has been altered. To address this problem we apply a neural network based classifier. The more classifier design implies generating an initial training data set upon known transformations. Robustness of the implemented watermarking method was tested against common image processing operations.

# 1 Introduction

Digital recorded information has one main advantage and drawback at the same time: it can be copied without any kind of degradation in quality. If it is copyright protected material the content owner is forced to seek out for new technologies to protect his rights. Digital Watermarking technology protects the content even after or during transferring by placing information in the visual content itself that is never removed under normal conditions. Visually perceivable markings in form of text or other graphical elements are easily identified and can be modified with image editing applications. By design, unlike the printed visible watermark, a digital watermark usually remains invisible to viewers. As tool, it is adequate to identify the source and authorized consumer of an image or document. Three attributes distinguish watermarking form other techniques that deal with information hiding and protection like Cryptography or Steganography: *imperceptible* for an observer, *inseparable* from the content and *experience the same transformations* as their container.

Digital images are commonly stored and processed in the spatial domain and frequency domain. The spatial domain refers to the pixel amount composing an image and the processing involves here only those pixels directly, whereas in the frequency domain, high-frequency components correspond to edges and low-frequency components to interior regions of an object. Hence, visual content based operations might benefit from transforming an image from spatial to frequency domain.

Digital watermarking techniques are considered promising techniques for multimedia authentication. Among these, semi-fragile watermarking allows acceptable content preserving against manipulations such as common image processing like: blurring, low-pass filtering, median filtering, salt and peppers noise and lossy compression [3].

The paper focuses on visual content based owner or author identification applicable to digital images, using watermarking techniques. Digital watermarking is in essence digital code embedded into host data. Based on this scheme, various methods are developed for working in the spatial or frequency domain [3], 5, 7]. In the spatial domain, embedding techniques make use of changing the gray levels of pixels to insert supplementary data into a host image. These techniques, e.g. LSB method, are easy to implement but don't resist well on processing operations and might significantly degrade image quality. On the other hand, in the frequency domain, information is embedded in coefficients of the transformed image. Nevertheless, visual quality could suffer too, on high amount of inserted data. Common transforms include: discrete cosine transform (DCT), discrete Fourier transform (DFT) and discrete wavelet transform (DWT) [3][6], 7, 8]. A system based on Watson's perceptual model is proposed in **Error! Reference source not found.**.

The watermark system chosen for the application and described here is based on the frequency domain to achieve embedding in the visual content itself by exploiting peculiarities of human vision. To avoid the distortion of the chrominance quality, the focus is on the luminance component to perform embedding on. Sensitivity for luminance difference is high in middle rage frequency and decreases in low and high frequency range. Low frequency components are more robust and visually sensitive than the high frequency once. If a low frequency component is modulated, it will cause the more seriously distortions, but it has higher ability to resist tempering than the high frequency component. Hence, the technique applied here will embed watermark information in frequency domain whereas all components of the watermark will not equally perceptible.

In Section 2 we present the formulas for finding the DCT. Mathematical preliminaries used in this section are adapted and inspired from [2][1]. The details of our watermarking technique are presented in the Section 3. In Section 4 we propose architecture for a system intended to provide digital watermarking services with automatic ownership tracking. The main issue in this endeavour is to overcome pattern degradation if the host image has been altered. Experimental results that validate our proposed watermarking approach are presented in Section 5. They have been obtained using the system described in Section 4.

# .2. Mathematical preliminaries. Discrete Cosine Transform (DCT)

The discrete cosine transform (DCT) allows the representation of an image as a sum of sinusoids of varying magnitudes and frequencies. DCT is a special case of Fourier transform, because instead of complex values, it uses only the real part of the transform. One specific property of DCT is exploited for images, namely, that most of the visually significant information is concentrated in just a few DCT coefficients, while the others are negligible small. This permits addressing image composition with respect to visual quality. That is why DCT is the heart of lossy image compression techniques, like the JPEG standard.

Like the Fourier Transform, the DCT provides a one-to-one mapping from spatial to frequency domain. Thus, to get back the original image, one simply has to take the inverse transform (IDCT) of the transformed image.

## 2.1 Bidimensional dimensional DCT (2D DCT)

An image of size $M$x$N$ in the spatial domain can be represented in bidimensional manner, as a function $f(x,y)$, $0 \le x \le M$, $0 \le y \le N$ in the spatial domain. The corresponding image $C(u,v)$, in the frequency domain is given by the bidimensional discrete cosine transform (2D DCT):

$$C(u,v)=\alpha(u)\alpha(v)\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}f(x,y)\cos\left(\frac{(2x+1)u\pi}{2M}\right)\cos\left(\frac{(2y+1)v\pi}{2N}\right),\ 0\le u\le M-1, 0\le v\le N-1,$$

$$\alpha(k)=\begin{cases}\sqrt{1/K}, if\ k=0\\ \sqrt{2/K}, if\ 1\le k\le K\end{cases}$$ and $K=M$ if $k=u$ and $K=N$ if $k=u$.

The values $C(u,v)$ are called DCT coefficients. We can observe that all samples of $f$ contribute to the coefficient.

The bidimensional discrete cosine transform (2D DCT) is a direct extension of the 1D DCT. Since the DCT is an invertible transform, its inverse, 2D IDCT, is given by:

$$f(x,y)=\sum_{u=0}^{M-1}\sum_{v=0}^{N-1}\alpha(u)\alpha(v)C(u,v)\cos\left(\frac{(2x+1)u\pi}{2M}\right)\cos\left(\frac{(2y+1)v\pi}{2N}\right),\ 0\le x\le M-1, 0\le y\le N-1.$$

## 2.2 DCT transformation matrix

The image $f(x,y)$ can be seen as a matrix A of size $M$x$N$ and the inverse equation can be interpreted as meaning that any matrix A can be written as sum of $M$*$N$ functions, called basic functions, of the form:

$$\alpha(u)\alpha(v)\cos\left(\frac{(2x+1)u\pi}{2M}\right)\cos\left(\frac{(2y+1)v\pi}{2N}\right),\ 0\le u\le M-1, 0\le v\le N-1$$

Without restricting the generality, in the following we will work only in the case $M=N$.

From a computational perspective, in order to reduce the amount of cosine functions, a more efficient attempt to compute a 2D DCT is using a $M$x$M$ transformation matrix $T$ of the form:

$$T_{i,j}=\begin{cases}\sqrt{\frac{1}{M}}, if\ i=0\\ \sqrt{\frac{1}{M}}\cos\left(\frac{(2i+1)j\pi}{2M}\right), if\ i>0\end{cases}$$

The matrix $T$ is named the DCT transformation matrix and it is an orthogonal matrix. If $A$ is an initial pixel matrix $M$x$M$, then $T$*$A$ produces a $M$x$M$ matrix whose columns contain the one-dimensional DCT of the columns from $A$. Hence, the 2D DCT is defined by the matrix product $C=T*A*T'$ and the 2D IDCT by $A=T'*C*A$.

The DCT coefficients typically represent the same information in a more compact form that can be stored in fewer bits. Moreover, purposely losing precision in the DCT domain is much less noticeable than losing the same amount of information in the spatial domain. Modern lossy image compression techniques use this as primary basis of operation. The JPEG standard relies on the block DCT domain and applies quantization according to step sizes.

# 3. The proposed watermark's embedding–extraction method

The aim of this section is to present a watermarking technique to add binary pattern to digital images. The method operates in the frequency domain, embedding a pseudo-random sequence of numbers in a selected set of DCT coefficients.

A digital image is divided into $M$x$M$ square sized disjoint pixel blocks, i.e. 8x8, 16x16 etc. Each of these blocks is then transformed into the DCT domain and contains $M$x$M$ DCT coefficients organized by frequency range, like in Figure 1. This transform tends to concentrates the image energy in the low-frequency coefficients of each block.

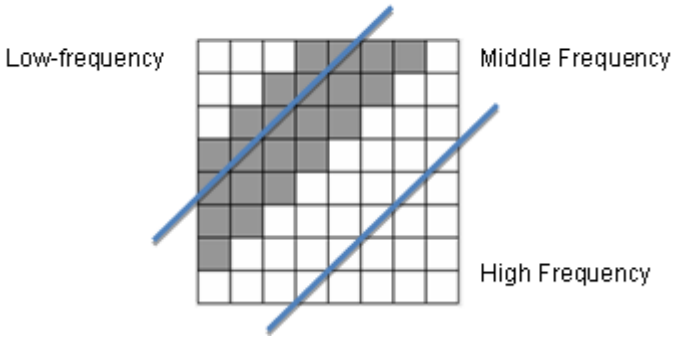


*Figure 1. Frequencies organized in a DCT block.*

To ensure watermark invisibility by exploiting the masking characteristics of the Human Visual System, data is stored in the more important frequency components. That is, from every DCT coefficient block, only a number of *K* middle frequency coefficients are selected for watermark embedding. The selected coefficients are shown marked grey in Figure 1.

By inserting the watermark in the low frequency coefficients, overall visual quality of the original image would be significantly affected. On the other hand, if inserted in high frequency coefficient, the visual quality of the image will not be as much affected, but the watermark is not that robust to processing, e.g. lossy compression.

We consider only small square matrixes *M*x*M* of small sizes, 4X4, 8X8, 16X16. A graphical view of 64 basic functions corresponding to an 8x8 block of an image is illustrated in Figure 2c). It can be easily seen that frequencies increase from left to right and form top to bottom.

*(a)* *(b)* *(c)*

*Figure 2. (a) Lena test image. (b) Visual inspection of image (a) in the 2D DCT transform domain. (c) Basic functions of an 8x8 block.*

After the entire watermark has been embedded, the IDCT is computed to obtain the watermarked version of the initial image in the spatial domain.

The proposed method uses Quantization index modulations (QIM) and performs a blind watermarking. For recovering only embedding settings are necessary, a reference image is not needed. The strategy is to associate watermark bit information with parity bits of DCT coefficients. Quantization step serves for hiding information by quantizing image data in the spatial or DCT domain.

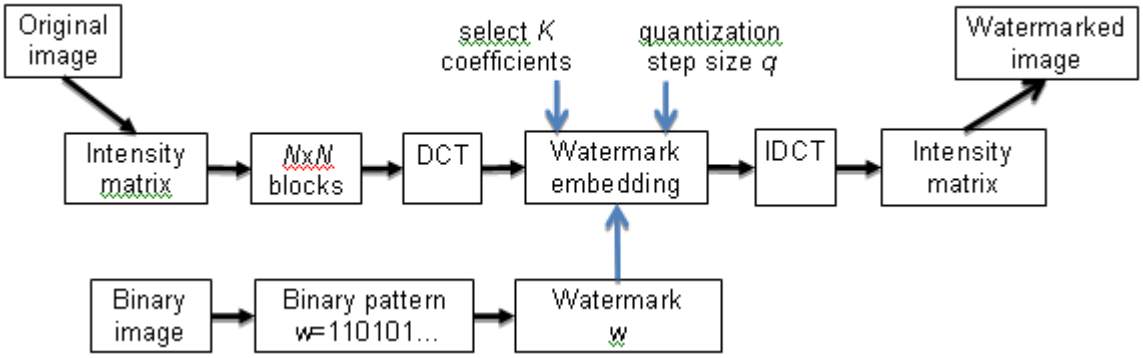


*Figure 3. Block diagram of quantization based embedding procedure*

## 3.1 Embedding

The watermarking embedding process complies with the following steps:

1. Partition the original image into square blocks of *NxN* pixels.
2. Apply 2D-DCT transform to all blocks from step 1, resulting in *NxN* size DCT coefficient blocks.
3. Transform the binary watermark $w$ image of size $A \times B$ into a binary row vector $w$ of size $P = A \times B$.
4. Select a DCT block and scan in zig-zag order (see Section 3.3).
5. Select a number of *K* coefficients from the current DCT block for embedding.
6. Embed a watermark bit $w(i)$ into each selected DCT coefficient by rounding its value to an even or odd quantization level *q*. Rounding to an even quantization level embeds a "0" bit, while rounding to an odd quantization level embeds a "1" bit. The new value of the DCT coefficient is calculated according to the following equation:

$$C_{u,v}^{w} = \left\lfloor \frac{C_{u,v}}{q} \right\rfloor q + \frac{q}{2} w(i) \operatorname{sgn}\left( C_{u,v} - \left\lfloor \frac{C_{u,v}}{q} \right\rfloor q \right)$$

   Where $C_{u,v}$ is the original DCT coefficient before embedding, $u, v$ are the raw and column index, *q* is the quantisation step and $\operatorname{sgn}(x)$ is the signum function of *x*.
7. Repeat steps 4-6 for the next blocks until all bits of $w$ are embedded.
8. If redundant embedding is requested, repeat L times the embedding of $w$ through multiple steps 4-7.
9. Computed the 2D Inverse Discrete Cosine Transform (2D-IDCT) for each block to obtain the watermarked image in the spatial domain.

Redundant embedding watermarking is applied in order to increase the robustness of the watermarking systems [3]. In a case of an image distortion not all coefficients are affected equally. Therefore the watermark is redundantly embedded across several coefficients.

## 3.2 Extraction

To extract the watermarked information out of an image, a reverse process to the one used to embed is applied. Recovering or detecting the embedded watermark can be performed in blind or non-blind manner, depending on the embedding strategy employed. If blind, then no reference image must be present at extraction, else, both reference and embedded image are necessary to search for differences, where data is probably embedded. In our embedding-extraction method we chose a blind recovering method.

The block diagram of the watermark extractor is shown in Figure 4. With this method the embedded sequence is extracted without comparing to the original image.

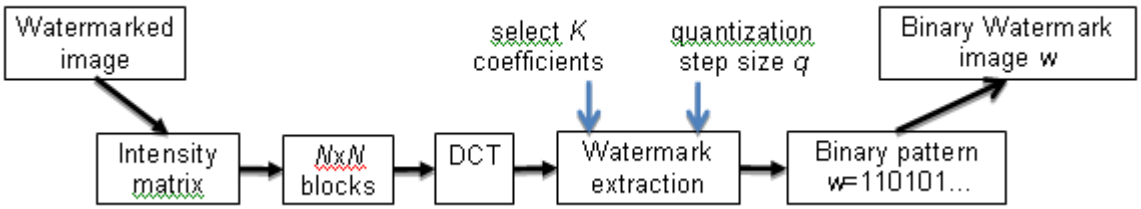


*Figure 4. Block diagram of extraction procedure*

The steps of the extraction process are:

1. Partition the watermarked image into square blocks of *NxN* pixels.
2. Apply 2D-DCT transform to all blocks from Step 1, resulting in *NxN* size DCT coefficient blocks.
3. Select a DCT block and scan in zig-zag order (see Section 3.3).
4. Select the same number of *K* coefficients from every DCT block used in the embedding process.
5. Extract one watermark bit from each coefficient selected in Step 4 by applying the equation:

   $w'(i) = \mathrm{mod}\,2\left( round\left( \frac{C^{w}_{u,v}}{q/2} \right) \right)$, where $C^{w}_{u,v}$ is DCT coefficient with embedded watermark data, *u,v* are the raw and column index, *q* is the quantisation step and $w'(i)$ is the extracted watermark bit.

6. Repeat steps 3-6 for the next blocks until all bits of $w'$ are extracted.
7. Transform the resulting vector back to a binary image of size $A \times B$.

In case of redundant embedding, step 6 is preceded by one step that includes a decision function to identify the extracted bit:

From every block *i*, of DCT coefficients extract a sequence $w_i(j)$ of *L* bits, one bit from every DCT coefficient, and use the following decision function to determine the watermark bit extracted:

$$w(j) = \begin{cases} 0, if \sum_{i=0}^{L} w_i(j) \le \frac{L}{2}, \; j = 0,1,...,P-1. \\ 1, otherwise \end{cases}$$

*P* is the length of the watermark pattern; *L* is the number of pixels where the same watermark bit was inserted.

## 3.3 Zig-Zag scanning order

By traversing a DCT block in zig-zag order, low frequency coefficients are placed in top of a vector. In Figure 5 is shown how a *NxN* sized square matrix gets transformed into one dimensional array of length *NxN*.

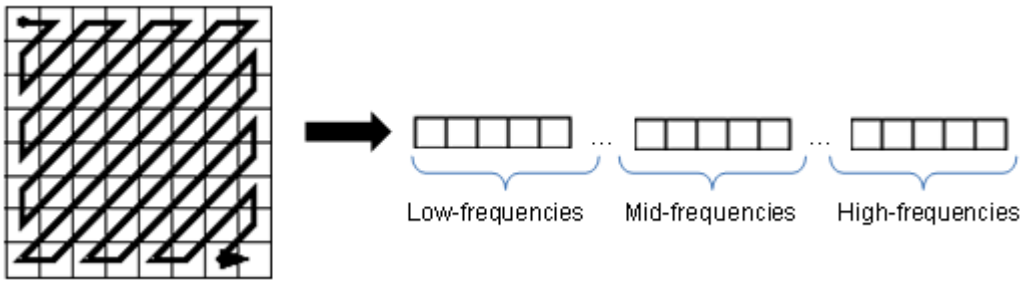


*Figure 5. Zig-zag transformation of a DCT block*

# 4. Experimental results

For benchmarking purpose, the results presented here are related to two test images that reached large popularity not only in image processing and computer vision fields. They are depicted in Figure 6, known as Lena and Cameraman. Experiments were conducted on different color and monochrome images. Results presented here are strictly related to the samples form Figure 6. Both images have a size of 512x512 pixels. One gray image is considered because the watermarking methods work with luminance information form pixels and therefore visual quality is influenced in very similar manner.

*Figure 6. Test images known as (a) Lena, (b) Cameraman*

Watermark bit embedding is done into blocks of 16x16 DCT coefficients. Hence, for 1 bit per block, the watermark payload has to be 512x512/256 =1024 bits. For demonstration propose, the binary image chosen as watermark information, presented in Figure 7, has a size of 64x64 (4096 bits), meaning a total payload of 4 bits per block.


*Figure 7. Binary watermark test pattern.*

In order to increase reliability of watermark preservation in the host image data, redundant embedding was tested. This strategy simply increases the number of bits inserted in a DCT block by duplicating the watermark bits.

To be useful in an image processing application a watermark embedding technique has to embed watermarks that survive normal processing including lossy compression, digital-analogue conversions, printing and scanning, format conversions etc.

The robustness of the implemented watermarking method was tested against common image processing operations, called attacks:

a) No processing applied;
b) Blurring using blocks of 3x3 pixels;
c) Exponential contrast modification;
d) Brightness increased by an amount of 50;
e) Brightness decreased by an amount of -50;
f) Gamma contrast modification with 1.6;
g) Gamma contrast modification with 0.6;
h) Linear contrast with 0.5;
i) Linear contrast with 1.2;
j) Adding “salt and pepper” noise with density d=0,5%;
k) Resize;
l) Rotate.

The extracted watermark images are listed in Table 1. Row letters correspond to each operation from the list above. Columns represent different redundancy factors.

Experimental results show that the watermark is robust to several processing techniques and distortions.

| | 1 | 2 | 3 | 4 | 6 | 8 | 10 |
|---|---|---|---|---|---|---|---|
| a) |  |  |  |  |  |  |  |
| b) |  |  |  |  |  |  |  |
| c) |  |  |  |  |  |  |  |
| d) |  |  |  |  |  |  |  |
| e) |  |  |  |  |  |  |  |

| | 1 | 2 | 3 | 4 | 6 | 8 | 10 |
|---|---|---|---|---|---|---|---|
| f) |  |  |  |  |  |  |  |
| g) |  |  |  |  |  |  |  |
| h) |  |  |  |  |  |  |  |
| i) |  |  |  |  |  |  |  |
| j) |  |  |  |  |  |  |  |
| k) |  |  |  |  |  |  |  |
| l) |  |  |  |  |  |  |  |

*Table 1. Extracted watermark patterns for different attacks and different redundancy factors.*

From an information security perspective it is highly important to detect an existing watermark or any kind of operation meant for altering or eliminating him. It is not impossible for watermarks or modified signals to remain undetected (false negative) or to be detected when they do not exist (false positive).

# 5. Ownership tracking system

In order to perform automate identification of watermark patterns we design an ownership tracking system. An image of the watermark identification using this system is presented in Figure 8. The dynamic authentication is based on a neural classifier with back propagation neural network. From an architectural view the system incorporates four processing steps:

a) Image pre-processing
b) Training/testing set construction
c) Classifier training
d) Performance evaluation

The image pre-processing is realized using a specially designed tool, allowing to apply common processing operation (blurring, brightness, different contrasts, salt and pepper effect, rotate, resize). For supervised learning the training/testing sets are obtained as results of generated attacks (as those presented in Section 4, Table 1). The more challenging classifier design implies building an initial training data set upon known transformations.

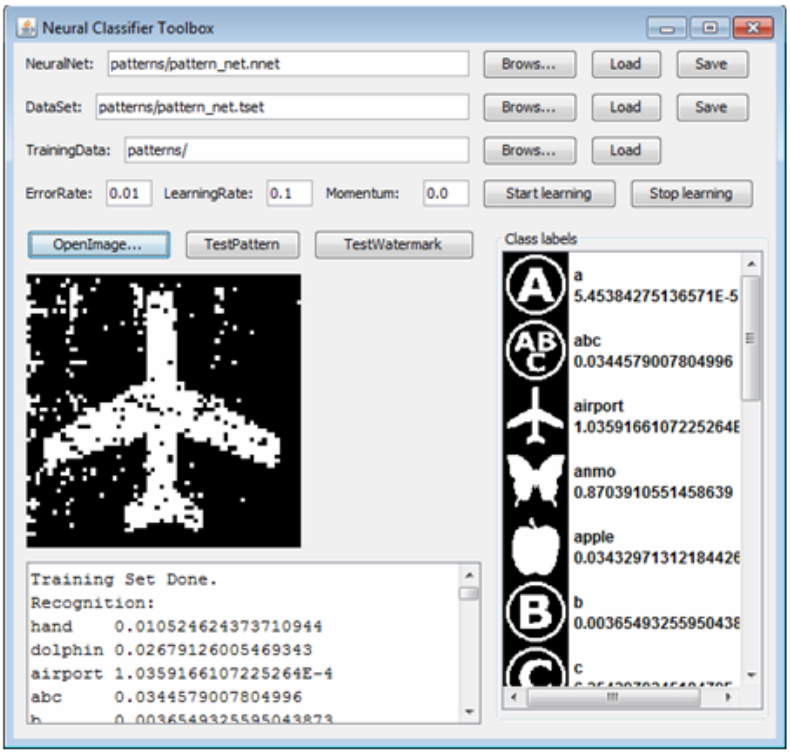


*Figure 8. Screen capture from the Ownership tracking system.*

Automatic identification also provides an identification rate and correlation between the identified watermark and the original one. (see Figure 9).

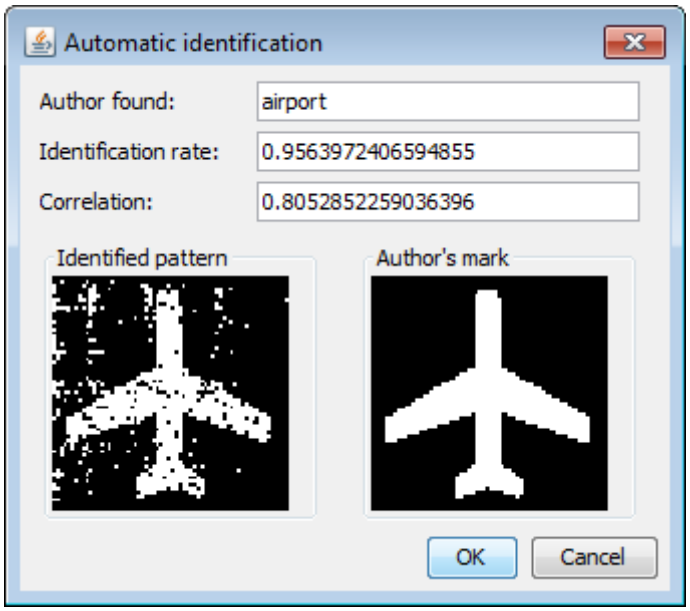


*Figure 9. Automatic identification with the proposed Ownership tracking system.*

A detailed presentation of the developed Ownership tracking system is outside the scope of this paper and will be subject of a future scientific presentation.

# 6. Conclusions and further directions of study

The watermarking method presented in this paper was tested against a series of attacks meant to determine the robustness for ownership tracking and verifications. All practical results are obtained by embedded in DCT coefficients of middle frequency. Low frequency coefficients make the watermark more resistant but lower the image quality, on the other hand, high frequency coefficients do not lower image quality but make the technique more vulnerable to attacks.

Quantisation step size and redundancy level are another two parameters that affect image quality and consequently watermark robustness. Since an acceptable balance has to be established at least between these three values, we are looking forward to developing an approach that allows dynamically finding best settings for any image based only on the visual particularities.

The results presented in this paper are part of an on-going research aimed at identifying best practice for providing secure and reliable tools of multimedia ownership tracking or identification. A strong emphasis is on the side of providing highly visual content adaptive methods that can be easily automatized with and integrated in classical pattern recognition.

**Acknowledgement**: Dana Simian was supported by the research grants LBUS-IRG-2015-01, project financed from "Lucian Blaga" University of Sibiu.

# References

[1] John C. Russ, *The Image Processing Handbook*, Fifth Edition, CRC Press, 2007.

[2] R.C. Gonzalez, R.E. Woods, *Digital Image Processing*, Second Edition, Addison-Wesley Publishing, 2001.

[3] Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Jessica Fridrich, Ton Kalker, *Digital Watermarking and Steganography*, Second Edition, Morgan Kaufmann Publishers, 2008.

[4] Q Li, I. J. Cox, Using perceptual models to improve fidelity and provide resistance to valumetric scaling for quantization index modulation watermarking, *IEEE Transactions On Information Forensics and Security*, vol. 2, no. 2, 127–139, June 2007.

[5] H. Y. Huang, C. H. Fan, W. H. Hsu, An effective watermark embedding algorithm for high jpeg compression, *Proceedings of Machine Vision Applications*, 256-259, May. 2007.

[6] Frank Y. Shih, *Image Processing and Pattern Recognition: Fundamentals and Techniques*, Wiley-IEEE Press, 2010.

[7] N. M. Charkari, M. A. Z. Chahooki, A robust high capacity watermarking based on DCT and spread spectrum, *Proceedings of IEEE International Symposium on Signal Processing and Information Technology*, 194–197, 2007.

[8] Xiaojun Qi, Xing Xin, A quantization-based semi-fragile watermarking scheme for image content authentication, *Journal of Visual Communication and Image Representation*, vol. 22, 187-200, 2011.

DANA SIMIAN
Univ. Lucian Blaga of Sibiu
Faculty of Science
Research center ITI
5-7, Dr. I. Ratiu str.
ROMANIA
E-mail: dana.simian@ulbsibiu.ro

RALF FABIAN
Univ. Lucian Blaga of Sibiu
Faculty of Science
5-7, Dr. I. Ratiu str.
ROMANIA
E-mail: ralfi_mail@yahoo.com