Robust Digital Watermarking Based on the Log-Polar Mapping

Radovan RIDZOŇ, Dušan LEVICKÝ

Dept. of Electronics and Multimedia Communications, Technical Univ. of Košice, Park Komenského 13, Košice, Slovakia

Radovan.Ridzon@tuke.sk, Dusan.Levicky@tuke.sk

Abstract. *The geometrical attacks are still an open problem for many digital watermarking algorithms used in present time. Most of geometrical attacks can be described by using affine transforms. This article deals with digital watermarking in images robust against the affine transformations. The new approach to improve robustness against geometrical attacks is presented. The discrete Fourier transform and log-polar mapping is used for watermark embedding and for watermark detection. Some attacks against the embedded watermarks are performed and the results are given.*

Keywords

Digital watermarking, geometrical attacks, discrete Fourier transform, log-polar mapping, hash function.

1. Introduction

Progress in digital data processing has brought many advantages into the data transmission, storage, copying and so on. But some advantages in one way can be disadvantages in other way. The easy processing of the digital multimedia has caused that the illegal digital copy can be made in exactly the same quality as the original, may be created at low cost and can be transmitted very easily through the networks. These reasons have established the question of the ownership rights protection in multimedia data.

There are two approaches to the multimedia data protection: Multimedia protection during the transmission and multimedia protection after the transmission.

The multimedia protection during the transmission is based on the usage of cryptographic algorithms. Cryptographic algorithms can be divided into the two main groups: symmetric or secret-key algorithms, and asymmetric or public-key algorithms. But these cryptographic algorithms protect the multimedia only during the transmission. After the decryption in the receiver multimedia terminal multimedia are not protected any more and data may be copied easily and without quality degradation.

The protection after the transmission and decryption can be achieved by adding some information into the multimedia data in which the information about the multimedia source, about the author or about the permission for further multimedia processing can be included. The art of hiding information into multimedia data in a robust and invisible manner is known as a ***digital watermarking***. Embedded information should be undetectable by human visual system but has to be detectable by a detector, which is used in the watermark extraction or detection process.

Cryptographic methods and digital watermarking are basic techniques in the field that is called Digital Right Management (DRM). Digital right management is a collection of techniques and technologies that enable technically enforced licensing of digital information, secure transmission, authors and ownership rights for all types of multimedia.

In digital watermarking as tools for the protection of ownership rights and copy prohibition, there are lots of processes performed by unauthorized persons which aim to corrupt the embedded information. These processes are called ***attacks***. There are various categorizations of attacks on watermarks. One from the categorization, presented in [4], is categorization into four main groups:

- removal attacks,
- geometrical attacks,
- cryptographic attacks,
- protocol attacks.

Removal attacks achieve complete removal of the watermark information from the watermarked data without cracking the security of the watermarking algorithm. This category includes denoising, lossy compression, quantization, remodulation, collusion, and averaging attacks.

Geometrical attacks do not remove the embedded watermark itself, but intend to distort the watermark detector synchronization with the embedded information. Cropping, flip, rotation, shift, scaling, translation and so on belong to the category of the geometrical attacks.

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. These 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.

Protocol attacks aim at attacking the entire concept of the watermarking application. This category includes the copy attack and the attacks made by invertible watermarks.

The geometrical attacks on the digital watermarks are still an open problem for many watermark algorithms used in present time. A few approaches to improve the robustness against geometrical attacks are presented in papers [1], [2], [3], [5].

The methods capable to estimate and recover the undergone global affine transformations can be divided into three main groups:

Invariant watermarks. The transform invariant domain approach mostly consists in the application of the Discrete Fourier Transform (DFT) followed by the log-polar (LPM) or a log-log coordinate mapping. And the watermark is embedded into the image by the modification of the DFT magnitude. This DFT followed by the LPM is the same as the Fourier-Mellin transform. The watermarks, which use the Fourier-Mellin transform, are designed to be robust mainly against the rotation, scales and translations.

Template based schemes. In this case, the watermark consists of two parts: template and the self watermark. The template contains no information but is merely a tool used to recover possible transformations in the image. The recovery of the watermark is a two stage process. First, the transformation undergone by the image is determined, and then inversion or compensation for the transformation when decoding the watermark is done. The points of the template may be distributed for example in the DFT domain.

Autocorrelation techniques. The third method for the recovery of geometrical transformations is the use of the auto-correlation function. These methods are based on the adding of the repeated watermarks in the overlapping fashion. At the detection, the estimation of the watermark is performed and the autocorrelation function is calculated. The peaks in the auto-correlation function are obtained due to the repetitive insertion of the watermark. Since the auto-correlation of the inserted watermark is known, this is compared with the auto-correlation function of the recovered watermark. A transformation matrix is calculated based on the two sets of peaks. This transformation is then inverted and the watermark is decoded.

2. Affine Transformations

Most of geometrical attacks can be uniquely described using the paradigm of general affine transforms, that can be represented by the 4 coefficients t_{11}, t_{12}, t_{21}, t_{22} forming a matrix $\boldsymbol{T}$ for the linear component, plus the two coefficients τ_h, τ_v, for the translation part of the transform. The affine transform maps each point of cartesian coordinates from (x,y) to (x',y'). This transform can be depicted in the following form

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \boldsymbol{T} \times \begin{pmatrix} x \\ y \end{pmatrix} + \boldsymbol{\tau} = \begin{pmatrix} t_{11} & t_{21} \\ t_{21} & t_{22} \end{pmatrix} \times \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} \tau_h \\ \tau_v \end{pmatrix} \tag{1}$$

where "×" represents the matrix product. The $\boldsymbol{\tau}$ component corresponds to the cropping and the translation.

The different values of the t_{ij} components in the matrix $\boldsymbol{T}$ represent the different types of the affine transforms.

The parameters of the transformation for a ***rotation*** $R(\theta)$ of a certain angle θ are

$$\boldsymbol{T}(\theta) = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}; \quad \begin{pmatrix} \tau_h \\ \tau_v \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}. \tag{2}$$

For ***scaling*** $S(\rho)$ factors ρ_x and ρ_y applied, respectively, to the horizontal and vertical axes, the transformation parameters are

$$\boldsymbol{T}(\rho_x, \rho_y) = \begin{pmatrix} \rho_x & 0 \\ 0 & \rho_y \end{pmatrix}; \quad \begin{pmatrix} \tau_h \\ \tau_v \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}. \tag{3}$$

The parameters for ***translation*** $T(h,v)$ in a x and y directs of a h and v pixels are

$$\boldsymbol{T}(h,v) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}; \quad \begin{pmatrix} \tau_h \\ \tau_v \end{pmatrix} = \begin{pmatrix} h \\ v \end{pmatrix}. \tag{4}$$

3. Log-Polar Mapping

As it was mentioned before, the exploitation of the features of some transformations which are invariant against the affine transformations can be used to improve robustness of watermarks against the geometrical attacks. Discrete Fourier transform (DFT) fulfill these requests and is often being used in the digital watermarking algorithms.

If the picture is defined as two dimensional function $x(i,j)$ in the Cartesian coordinate system with limitations $0 \le i < N_1$ and $0 \le j < N_2$, the DFT and inverse DFT is defined as follows

$$F(u,v) = \sum_{i=0}^{N_1-1} \sum_{j=0}^{N_2-1} x(i,j) \cdot e^{-j(2\pi/N_1)ui} \cdot e^{-j(2\pi/N_2)vj}, \tag{5}$$

$$x(i,j) = \frac{1}{N_1 N_2} \sum_{p=0}^{N_1-1} \sum_{q=0}^{N_2-1} F(u,v) \cdot e^{j(2\pi/N_1)ui} \cdot e^{j(2\pi/N_2)vj}. \tag{6}$$

Affine transforms performed with images in the spatial domain caused the specific changes in the DFT domain.

The ***picture shift*** in the spatial domain causes a linear shift in the phase component of the DFT

$$F(k_1,k_2)e^{-j(\gamma_x k_1+\gamma_y k_2)} \leftrightarrow f(x+\gamma_x, y+\gamma_y). \quad (7)$$

The symbol $\leftrightarrow$ represents the transform relationship between DFT domain and the image spatial domain. Note that both $F(k_1,k_2)$ and $f(x,y)$ are periodic functions so the translations cause the image to be "wrapped around" and this feature is called *circular translation.*

Scaling the axes in the spatial domain causes an inverse scaling in the frequency domain

$$\frac{1}{\rho}F\left(\frac{k_1}{\rho},\frac{k_2}{\rho}\right) \leftrightarrow f(\rho x,\rho y). \quad (8)$$

The ***image rotation*** through an angle θ in the spatial domain causes the DFT representation to be rotated through the same angle

$$F(k_1\cos\theta - k_2\sin\theta, k_1\sin\theta + k_2\cos\theta) \leftrightarrow \\ \leftrightarrow f(x\cos\theta - y\sin\theta, x\sin\theta + y\cos\theta) \quad (9)$$

From equation (7) it is clear that spatial shifts affect only the phase representation of the image. Also equations (8) and (9) can be rewritten by using the specific substitution. The changes in the image caused by scaling and image rotation in the spatial domain can be described by invariant shift after this substitution. This can be performed by the substitution which is called ***log-polar mapping (LPM)***.

Consider a point $(x,y)\in R^2$ and define $x=e^{\mu}\cos\theta$, $y=e^{\mu}\sin\theta$, where $\mu\in R$ and $0\le\theta<2\pi$. The result of this substitution is that for every point (x,y) there is a point (μ,θ) that uniquely corresponds to it. The new coordinate system (μ,θ) converts the scaling and rotation into the simple translation in the direction of the axis.

Scaling is converted to a translation

$$(\rho x,\rho y) \leftrightarrow (\mu+\log\rho,\theta). \quad (10)$$

Rotation is converted also to a translation

$$(x\cos(\theta+\delta)-y\sin(\theta+\delta), x\sin(\theta+\delta)+y\cos(\theta+\delta)) \leftrightarrow \\ \leftrightarrow (\mu,\theta+\delta) \quad (11)$$

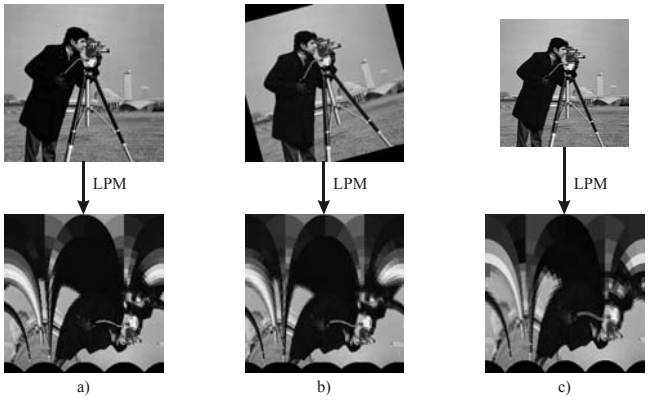

Fig. 1. Image and corresponding LPM a) original image, b) rotated image, c) scaled image

4. Proposed Watermarking Method

The proposed algorithm is based on the combination of the DFT and LPM features. Watermark is in the form of spare matrix which is created depending on the sequence of the alphanumeric values. The watermark is inserted into the original picture in the DFT domain. During the embedding process the hash function RIPEMD-160 is used for the algorithm security improvement.

On the receiver side, the watermark is not extracted but only detected. That means there is a binary decision process about the presence or the absence of the watermark in the image.

4.1 Watermark Embedding

The entries of the watermark embedding process are the original gray scale image I and the key K, which is in the alphanumeric form and after the processing by hash function is used as the initialization vector for the pseudorandom generator.

The process of the watermark embedding is shown in Fig. 2 and can be described in five steps:

- DFT of the original image I,
- watermark generation based on the secret key K,
- transformation of the key by using inverse LPM,
- watermark embedding into the chosen coefficients of the magnitude spectrum of the DFT,
- inverse DFT.

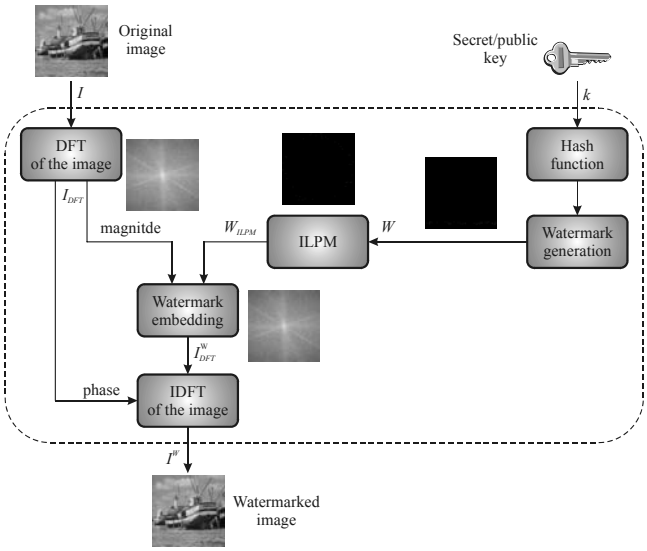

Fig.2. Watermark embedding algorithm

The calculation of the DFT of the original image is the first step in the watermark embedding process. The secret key K is used as the input for the RIPEMD-160 hash function. The output of the hash function is used as the initialization vector for the pseudorandom generator. Generated pseudo-

random sequence has normal dispersion and zero mean value and based on the chosen decision level is mapped into the two values (0,1) (Fig. 3). The size of the sequence is selected based on the desired quality of the watermarked image and on the desired robustness of the embedded watermark against the attacks.

Fig. 3. Pseudorandom sequence and sequence mapped on the values (0,1).

The size of the watermark has to be the same as the size of the original image. Generated and mapped sequence is situated in the lower part of the watermark (Fig. 4). The quality of the watermarked image is influenced by the location of the sequence in the watermark, the size of the sequence and by the density of the ones in the sequence.

Fig. 4. Embedded watermark.

The next step in the embedding process is the transformation of the watermark by using inverse log-polar mapping (ILPM). The location of the pseudorandom sequence in the watermark is selected by following DFT and LPM properties. Watermark and its ILPM are shown in Fig. 5.

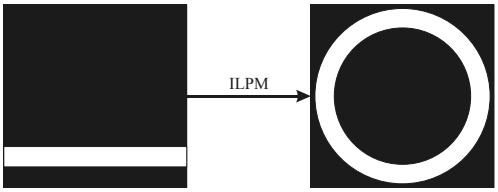

Fig. 5. Watermark and its inverse log-polar mapping.

As can be seen in Fig. 5, the ILPM transforms the pseudorandom sequence in the watermark into the concentric ring. In the DFT spectrum the medium frequencies are situated in this region. These frequencies are chosen for the watermark embedding for two reasons:

- modification of medium frequencies causes less degradation of the watermarked image as the modification of the lower frequencies would caused,
- if the higher frequencies are modified during the watermark embedding process, the watermark robustness would be low against the attack, mainly against loss compressions.

The location of the concentric ring in the ILPM domain can be modified by the vertical shifting of the pseudorandom sequence in the watermark (Fig. 6).

The watermark is embedded into the magnitude coefficients of the DFT in the form of local peaks. The process of the embedding is adaptive, that means the watermark is not embedded into the whole picture with the same power. The process of the watermark embedding can be described as

$$I_{DFT}^{W}(i,j)=\begin{cases}\dfrac{\alpha}{9}\displaystyle\sum_{i-1}^{i+1}\sum_{i-1}^{i+1}I_{DFT}(i,j) & if \quad W_{ILPM}(i,j)=1\\ I_{DFT}(i,j) & if \quad W_{ILPM}(i,j)=0\end{cases} \tag{12}$$

where α (alfa) is the power of the embedded watermark.

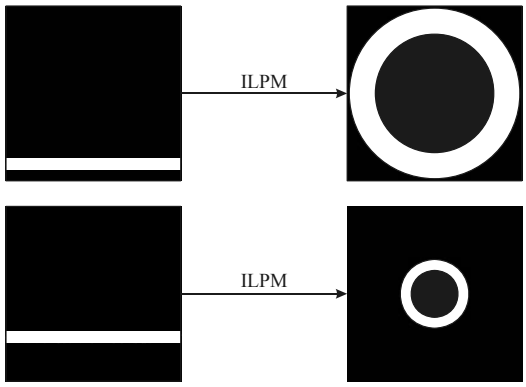

Fig. 6. Vertical shifting of the pseudorandom sequence.

The inverse DFT is the final step in the watermark embedding process and the watermarked images are obtained (Fig. 7).

Fig. 7. Watermarked images.

4.2 Watermark Detection

The detection algorithm does not require the original image and is based on the correlation test between the original and extracted watermark. The algorithm entries are tested image and secret key K for the watermark generation.

The process of the watermark detection is shown in Fig. 8 and can be described in five steps:

- DFT transformation of the tested image,
- position finding of the local maxima,
- LPM transformation of the local maxima,
- watermark generation by using secret key K,
- correlation test,
- decision about the presence or absence of the watermark in the tested image.

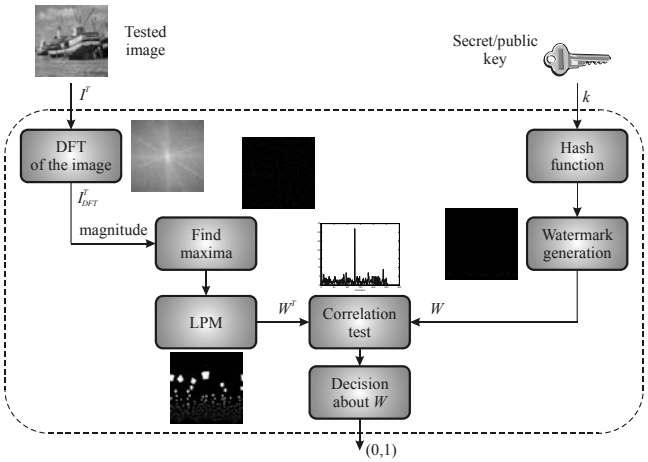

Fig. 8. Watermark detection algorithm.

The DFT is the first step in the watermark extraction process. The local maxima are searched in the small non-overlapping windows. In the experiments the window with 10x14 pixels was used. The positions of all founded local maxima are saved into the empty matrix. This matrix represents the extracted watermark.

In the next step, the local maxima are transformed by using LPM (Fig. 9) and the correlation test between the original and tested watermark is calculated. The decision about the watermark presence or absence is based on the chosen level of the correlation function.

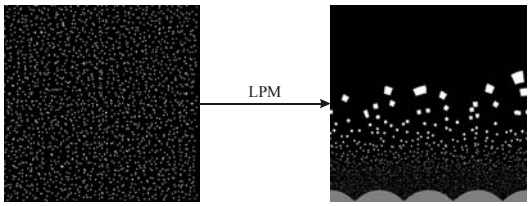

Fig. 9. LPM of the founded maxima.

5. Experimental Results

In the experiments, five different images were used and five different watermarks were added into each image. Examples of one watermarked image with embedded watermarks are shown in Fig. 7. Three different powers of the α parameter during the watermark embedding process were used. The robustness of the embedded watermarks was tested against some attacks.

Rotated images are shown in Fig. 10. As it can be seen, in the second and third image there is one local peak in the correlation function and the watermark was detected. The detection of the watermark in the first image is disputable, because there are two ambiguous local peaks.

The attack by image scaling is shown in Fig.11. The image was reduced in dimensions to the half and thereafter enlarged to the original dimensions. As it can be seen, the watermark was detected in two cases. The watermark was destroyed in the first case and the watermark detection was unsuccessful.

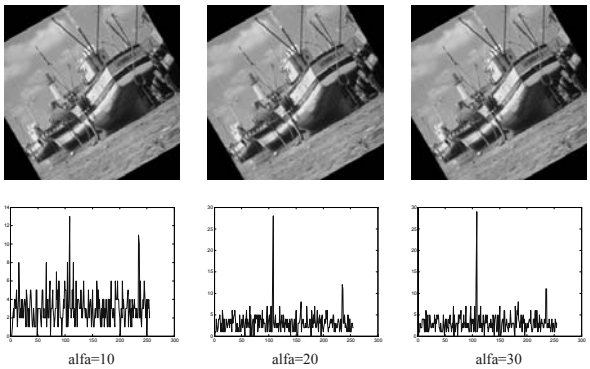

Fig. 10. Rotated images (30 degrees).

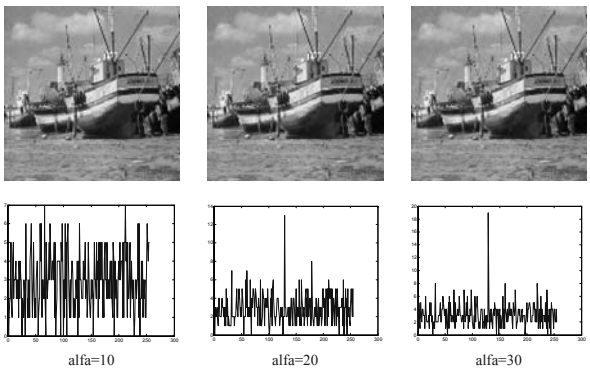

Fig. 11. Image scaling.

The results of the average correlation test (KT) for all attacks and for all watermarked images with different settings of parameter α (10,20,30) are shown in Fig. 12.

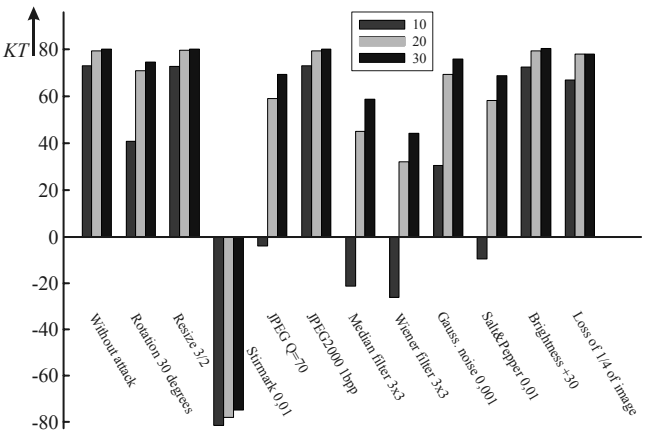

Fig. 12. Correlation test.

As it can be seen, when the parameter α is increasing, the value of the KT is increasing, too and this caused the better detection of the watermark in the attacked images.

The results of the detection of the watermarks in the attacked images are shown in Tab. 1.

Correlation test				
Attacks	**Power**	**10**	**20**	**30**
Without attack		**Y**	**Y**	**Y**
Rotation	30°	**Y**	**Y**	**Y**
Resize	**1x–>1/2**	**Y**	**Y**	**Y**
Stirmark	**0,01**	**N**	**N**	**N**
JPEG	**Q=70**	**N**	**Y**	**Y**
JPEG2000	**1 bpp**	**Y**	**Y**	**Y**
Median filter	**3x3**	**N**	**N**	**Y**
Wiener filter	**3x3**	**N**	**Y**	**Y**
Gauss noise	**0,001**	**Y**	**Y**	**Y**
Salt&pepper	**0,01**	**N**	**Y**	**Y**
Brightness	**+30**	**Y**	**Y**	**Y**
Loss of image	**1/4**	**Y**	**Y**	**Y**

Tab. 1. Effect of the parameter α on the watermark detection (Y – watermark is detected, N – watermark is not detected).

The smallest noise, added into the image, is in the case, when $\alpha = 10$. But in this case, there is the smallest robustness against some types of the attacks.

6. Conclusion

In this paper one approach how to improve robustness of the digital watermarks in gray scale images based on the DFT and LPM was shown. As it was demonstrated by providing some types of attacks, the proposed watermarking method is highly robust against the geometrical attacks. The further work will be oriented on the improving of the robustness against the removal attacks, mainly the loss compressions and the exploitation of the human visual system in the watermark embedding process for the better hiding the watermark into the original image.

Acknowledgements

The work presented in this paper was supported by the Grant of the Ministry of Education and the Academy of Science of the Slovak Republic VEGA under Grant No. 1/4054/07.

References

[1] DEGUILLAUME, F., VOLOSHYNOVSKIY, S., PUN, T. A method for the estimation and recovering from general affine transforms in digital watermarking applications. In *Proc. SPIE Vol. 4675, Security and Watermarking of Multimedia Contents IV*, p. 313–322, 04/ 2002.

[2] LIU, Y., ZHAO, J. Rotation, scaling, translation invariant image watermarking based on radon transform. In *First Canadian Conference on Computer and Robot Vision*. Ottawa (Canada), May 17–19, 2004, p. 225-232.

[3] RUANAIDH, J. J. K., PUN, T. Rotation, scale and translation invariant digital image watermarking. In *Proc. IEEE Int. Conf. Image Processing 1997 (ICIP 97)*. Santa Barbara (CA), Oct. 1997, vol. 1, p. 536–539.

[4] VOLOSHYNOVSKIY, S. et al. Attack modeling: Towards a second generation watermarking benchmark. *Sig. Processing, Special Issue on Information Theoretic Issues in Digital Watermarking*. 2001, vol. 81, no. 6, p. 1177-1214.

[5] ZHENG, D., ZHAO, J., El SADDIK, A. RST Invariant digital image watermarking based on log-polar mapping and phase correlation. *IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Authentication, Copyright Protection and Information Hiding*, August 2003, vol. 13, issue 8, p. 753-765.

About Authors...

Radovan RIDZOŇ was born in Banská Bystrica (Slovak Republic) in 1979. He graduated from the Technical University in Košice, Faculty of Electrical Engineering and Informatics. From 2003 till 2007 he was PhD. student at the Department of Electronics and Multimedia Communications and now he is assistant professor at the same department. His research is focusing on digital watermarking, information and network security, and digital image processing.

Dušan LEVICKÝ was born in Slanec (Slovak Republic) in 1948. He received the M.Sc. and PhD. degrees at the Technical University (TU) in Košice and now he is professor at the Department of Electronics and Multimedia Communications, TU in Košice. His research interests include digital image processing, image transmission and cryptography.