Proceedings of the Federated Conference on Computer Science and Information Systems pp. 681–688
DOI: 10.15439/2017F177
ISSN 2300-5963 ACSIS, Vol. 11

Selective Image Authentication Using Shearlet Coefficients Tolerant to JPEG Compression

Aleksei Zhuvikin
Department of Secured Communication Systems,
The Bonch-Bruevich Saint Petersburg State University of Telecommunications
Saint-Petersburg, Russia
Email: zhuvikin@ya.ru

***Abstract*—A novel selective image authentication system based on the robust digital watermarking is proposed. The discrete shearlet transform is performed in order to extract the feature vector from the image. The cone-adapted version of the transform is used to calculate the shearlet coefficients more precisely and to avoid the biased treatment. The proposed approach allows to use conventional cryptographic digital signature for the image feature vector verification and makes the authentication scheme more secure. In order to embed watermark (WM) into the image the areas HL3 and LH3 of the Haar wavelet transform coefficients are used. Experimental results show that the proposed selective image authentication system is effective in terms of tolerance to JPEG compression, malicious image tampering detection and visual image quality just after embedding.**

***Index Terms*—Digital images; selective image authentication; cone-adapted shearlet transform; JPEG; 3-bit hash quantization; Haar-wavelet transform.**

I. Introduction

AN authentication of digital objects is widely applicable and is commonly used nowadays. The primary aim of this procedure is a saving of data integrity and a confirmation of the truth. Regarding to the digital images and other multimedia kinds of content, there are no problems to perform a content verification in a case of strict authentication type. This definition of the problem assumes that the data integrity is broken even if only one data bit had been changed. Several methods are well known for authentication within cryptography, e. g. digital signature (DS) [1]. The only limitation is that DS is appended to the object itself and can be corrupted or even lost in case of incautious use. As an alternative approach a *digital watermarking* [2] for image content authentication can be applied. There are practical applications implying to keep image exactly as it is. For example, if medical image would contain compression artefacts this could lead to wrong diagnostics. This issue is usually solved with conventional cryptography by *strict image authentication* [3], [4]. However, strict image authentication methods are not applicable in the fields where a certain set of the content manipulations is assumed to be acceptable. So called *selective image authentication* manages to solve this task [2].

A selective image authentication is a well known problem and is a point of interest of many works [5]–[10]. Usually an image compression is classified as a legal image manipulation since it doesn't change image content, and thus should not break in an authentication. In the proposed method we primarily focus on the tolerance to JPEG compression algorithm [11] for its wide application in legal image processing.

Image features extraction techniques of the most advanced proposed methods for selective image authentication use the following types of the image preprocessing. Method based on the key-points features extraction is presented in [5]. The several algorithms use the image moments calculation [6], [7], content describing by using of wavelet coefficients [8], central-finite differences [9], ridgelet and radon transforms [10], etc. In this paper we present a novel selective image authentication method which uses *shearlet transform coefficients* [12] as an image content descriptor. Recent investigations [13] show that shearlet coefficient properties are well suited for this purpose as a face and pattern recognition. Due to the fact that shearlets are able to describe considered signal in details and sparsely [12] it is reasonable to involve these properties to the problem of selective image authentication. We show that some of the shearlet coefficients are tolerant to JPEG compression and, on the other hand, are sensitive to the image content modifications. Due to the usage of 3-bit quantization technique the extracted image features can be signed and embedded in the image as a digital watermark (WM). Any algorithm robust to JPEG compression can be chosen as a watermark embedding method. We use 3-level *Haar wavelet transform* [14] for watermarking embedding that provides acceptable visual quality just after embedding.

Section II of the paper presents the main properties of discrete shearlet transform and explains the feature vector calculation technique. 3-bit quantization method is covered in Section III. The usage of the embedding and extraction algorithms is considered in Section IV. The simulation results are presented in Section V followed by conclusions in Section VI.

II. Cone-Adapted Discrete Shearlet Transform and Image Features Extraction

The shearlet transform was introduced in 2006 [12] for the mathematical analysis of anisotropic features of the multivariate signals. Being a generalisation of wavelets, shearlets provide sparse representations for the large class of multidimensional data by given dilation, shear and translation parameters. We propose shearlet transform to be used for image features

$$\mathcal{SH}_{j,k,m}(I)=\begin{cases}\mathcal{F}^{-1}\left(\phi(\omega_1,\omega_2)\,I(\omega_1,\omega_2)\right) & |\omega_2|<1,|\omega_2|<1,\\ \mathcal{F}^{-1}\left(\psi\left(4^{-j}\omega_1,4^{-j}k\omega_1+2^{-j}\omega_2\right)I(\omega_1,\omega_2)\right) & |\omega_1|\geq 1/2,|\omega_2|<|\omega_1|,|k|\leq 2^j-1,\\ \mathcal{F}^{-1}\left(\psi\left(4^{-j}\omega_2,4^{-j}k\omega_2+2^{-j}\omega_1\right)I(\omega_1,\omega_2)\right) & |\omega_1|\geq 1/2,|\omega_2|>|\omega_1|,|k|\leq 2^j-1\\ \mathcal{F}^{-1}\left(\psi^{h\times v}\left(4^{-j}\omega_1,4^{-j}k\omega_1+2^{-j}\omega_2\right)I(\omega_1,\omega_2)\right) & |\omega_1|\geq 1/2,|\omega_2|\geq 1/2,|\omega_1|=|\omega_2|,|k|=2^j.\end{cases}\tag{3}$$

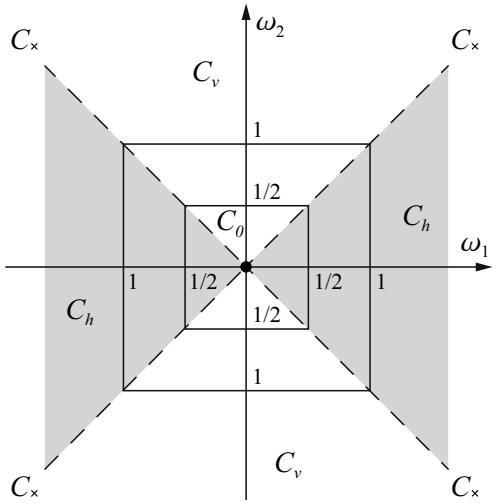

Fig. 1. Used notations of the calculation cone-areas C_v, C_h, seams $C_\times$ and the middle cap C_0 in the frequency domain defined by the discrete cone-adapted shearlet transform.

calculation procedure. As it will be shown in Section V some of the shearlet transform coefficients are robust to introduce small image noise, wherein allow to describe image content quite enough. Let describe briefly the main features of the shearlet transform and it's algorithmic efficient digital version that was introduced in [15].

For $\psi\in L^2\left(\mathbb{R}^2\right)$ the continuous shearlet system generated by ψ is defined as $\{\psi_{a,s,t}=a^{-\frac{3}{4}}\psi\left(A_a^{-1}S_s^{-1}(x-t)\right)|a>0,s\in\mathbb{R},t\in\mathbb{R}^2\}$. Functions $\psi_{a,s,t}$ are called shearlets where dilation a and shear s parameters determine dilation A_a and shear S_s matrices respectively as[15]

$$A_a=\begin{pmatrix}a & 0\\ 0 & \sqrt{a}\end{pmatrix},\quad a\in\mathbb{R}^+$$
$$\text{and}\quad S_s=\begin{pmatrix}1 & s\\ 0 & 1\end{pmatrix},\quad s\in\mathbb{R}.$$

Then, corresponding continuous shearlet transform is given by mapping

$$f\to\mathcal{SH}_\psi f(a,s,x)=\langle f,\psi_{a,s,x}\rangle,$$
$$f\in L^2\left(\mathbb{R}^2\right),(a,s,t)\in\mathbb{R}_{>0}\times\mathbb{R}\times\mathbb{R}^2.\tag{1}$$

So, the values of shearlet coefficients can be found as a convolution of f with shearlet functions $\psi_{a,s,t}$ [12]

$$\mathcal{SH}_\psi f(a,s,x)=\int_{\mathbb{R}^2}f(t)\psi_{a,s,t}(x-t)\,\mathrm{d}t=f*\psi_{a,s,t}(x).$$

For we need to use discrete version of the shearlet transform (1), we consider only digital images $\mathbb{R}^{M\times N}$ as functions sampled on the grid $\{\left(\frac{m_1}{M},\frac{m_2}{N}\right):(m_1,m_2)\in\mathcal{G}\}$ with $\mathcal{G}=\{(m_1,m_2):m_1=0,...,M-1,m_2=0,...,N-1\}$ and periodic continuation over the boundary is assumed. However, due to the known problem of biased treatment of directions cone-adapted version of the discrete shearlet transform is commonly used [15]. In this calculation technique, frequency domain is divided into the cones that are shown in the Figure 1 where $C_\times$ is the cone seam line, C_v and C_h represent vertical and horizontal cones of the frequency bands and C_0 is the low-frequency component. The main part of the signal energy is contained in the low-frequency region whereas the bands around represents high-frequency parts.

We define auxiliary functions $\chi_\kappa,\kappa\in\{\times,v,h\}$ equal to 1 for coordinates (ω_1,ω_2) which are in the areas C_κ, i.e. $(\omega_1,\omega_2)\in C_\kappa$ and equal to 0 for $(\omega_1,\omega_2)\notin C_\kappa$. In this notation the cone-adapted version of discrete shearlet transform is the mapping

$$I\to\mathcal{SH}_\psi I(j,k,m)=\langle I,\psi_{j,k,m}\rangle,$$
$$(j,k,m)\in\mathbb{R}_{>0}\times\mathbb{R}\times\mathbb{R}^2\tag{2}$$

where $j\in\mathbb{Z},0\leq j<\lfloor\frac{1}{2}\log_2\max\{M,N\}\rfloor$ and $k\in\mathbb{Z},-2^j\leq k\leq 2^j$ are the discrete versions of the dilation and shear parameters, $I(m)=I(m_1,m_2)\in L^2\left(\mathbb{R}^2\right)$ is the function of the $\{M,N\}$-dimensioned discrete image with translation parameter $m=(m_1,m_2):m_1=0,...,M-1,m_2=0,...,N-1\}$. By means of the cone-adapted scheme the coefficients $\mathcal{SH}_{j,k,m}(I)$ of the shearlet transform can be obtained similarly to (3) [15] , where (ω_1,ω_2) are the coordinates (m_1,m_2) mapped to the frequency domain, $\mathcal{F}^{-1}(g(\omega_1,\omega_2))$ is the inverse two-dimensional discrete Fourier transform [16] of function $g(\omega_1,\omega_2)$ and

$$\psi^{h\times v}(\omega_1,\omega_2)=\psi_1(\omega_1,\omega_2)\,\chi_\times+$$
$$\psi_1(\omega_1)\,\psi_2\left(\frac{\omega_2}{\omega_1}\right)\chi_h+\psi_1(\omega_2)\,\psi_2\left(\frac{\omega_1}{\omega_2}\right)\chi_v,\tag{4}$$
$$\psi(\omega_1,\omega_2)=\psi_1(\omega_1)\,\psi_2\left(\frac{\omega_2}{\omega_1}\right),\tag{5}$$

where ψ_1, ψ_2 and ϕ are the predefined scaling functions. In the proposed method we use Meyer's wavelet-based functions for (3)-(5) that can be chosen as in [15].

The frequency tiling that represent different directions and scales of the shearlets up to $j=1$ and low-pass band with corespondent values of parameters (j,k) are shown in the Figure 2.

In the proposed method, we use only $(1,1)$, $(1,3)$, $(1,5)$ and $(1,7)$ frequency bands (that are highlighted in the Figure 2)

for the image feature vector calculation due to the following reasons. These bands have tolerance to the introduced small image noise as well as to JPEG compression. On the other hand, it was found that chosen bands are sensitive to image content modifications and malicious image tampering. It is worth to note, that the more scale parameter is selected, the more sensitivity to image modifications is achieved and, at the same time, the less tolerance to the JPEG compression is observed. Our experiments showed that scale parameter $j = 1$ is a good candidate for the trade-off between noise sensitivity and malicious tampering detection. Secondly, we choose bands with dilation indices $k \in \{1, 3, 5, 7\}$ just to insure to proposed image feature vector be more sparse and occupy less memory space.

Due to the considerations above, let us define four vectors $d_{\mathcal{SH}_k}$ of used shearlet coefficient amplitudes

$$d_{\mathcal{SH}_k} = \left(\|\mathcal{SH}_{j,k,m}(I)\|\right)_{j=1,m\in\mathcal{G}}, \quad k \in \{1, 3, 5, 7\}. \quad (6)$$

Elements $d_{\mathcal{SH}_k}$ can be calculated according to (3) for given image I. In order to compress image features up to available size we propose to use *average downsampling* technique [17] with integer parameter h, divisor of $M \times N$: $\forall(i) \in \left\{1, \ldots, \frac{M\times N}{h}\right\}$ as follows

$$d_k(i_k) = \frac{1}{h}\sum\{d_{\mathcal{SH}_k}(m)|\ h(i_k - 1) < m \le hi_k\}$$

Finally, we define *image feature vector* $d \in \mathbb{R}^L$ as

$$d = (d(i))_{i=1}^{L} = \left(\bigcup_{k\in\{1,3,5,7\}} d_k(i)\right)_{i=1}^{\frac{M\times N}{h}}, \quad L = \frac{4(M\times N)}{h} \quad (7)$$

Calculated by (7) image feature vector d gives the compact representation of the image features. However, coordinates of the image feature vector d are the real numbers and they should be digitised before signing and embedding into the image as WM.

III. Recovering of Image Feature Vector After JPEG Compression by 3-Bit Quantization Technique

Digital watermarking techniques expect that data to be embedded have the binary form and of a finite length. Also, as we mentioned in the Section II, in order to apply digital signature to the image feature vector (7) it should be pre-digitized.

Let quantize the values of d with step $\Delta \in \mathbb{R}$ called *image features quantization parameter* as

$$d_\Delta(i) = \left\lfloor \frac{d(i)}{\Delta} \right\rfloor + 1 \quad (8)$$

where $\lfloor\cdot\rfloor$ is the floor map.

Now, it would be possible to authenticate the tested image $\left(\tilde{I}(m)\right)_{m\in\mathcal{G}}$, given the embedded vector d_Δ and the corresponding vector $\tilde{d_\Delta}$ calculated for the image $\left(\tilde{I}(m)\right)_{m\in\mathcal{G}}$.

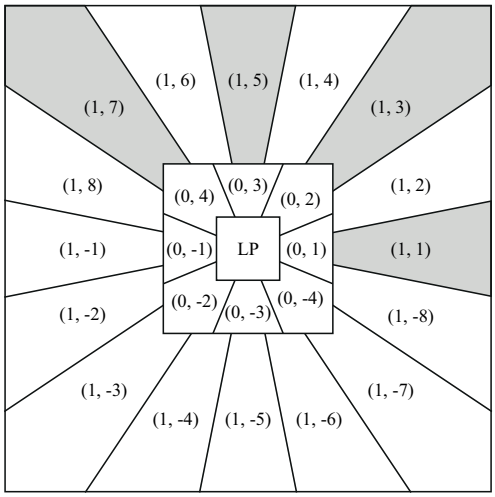

Fig. 2. Frequency tiling and respective notations with parameters (j, k) and the low-pass band (LP). Bands used for the feature vector calculation in the proposed method are highlighted.

Then, the following condition should be taken for the authentication rule

$$\left(\tilde{I}(m)\right)_{m\in\mathcal{G}} \text{ is authentic } \iff \max_i |\tilde{d_\Delta}(i) - d_\Delta(i)| \le 1. \quad (9)$$

However, the use of the authentication rule (9) is inconvenient for two reasons. First, the size of the authenticator d_Δ is large enough to be embedded into the image without significant corruption. Second, any adversary might be able to forge the authentication process because no cryptographic technique was used. In order to overcome the difficulties mentioned above, we propose to hash the feature vector d_Δ and to obtain its digital signature. On the other hand, hashing the vector d_Δ after its corruption by JPEG compression leads to error expansion. In order to recover d_Δ, after jumps of their coordinates in at most one quantization level, it is possible to use so called *3-bit quantization* technique [18] briefly considered below.

Let introduce an *auxiliary perturbation vector* p of dimension L where its *i*-th coordinate contains three bits p_{1i}, p_{2i}, p_{3i} computed as follows [18]

$$(p_{1i}, p_{2i}) = [d_\Delta(i) \bmod 4]_2 \quad (10)$$

$$p_{3i} = \begin{cases} 1 & \text{if } d(i) \in [a_i, b_i) \\ 0 & \text{if } d(i) \in [b_i, a_{i+1}) \end{cases} \quad (11)$$

with $a_i = \Delta\, d_\Delta(i)$, $b_i = \Delta\left(d_\Delta(i) + \frac{1}{2}\right)$, and $[\cdot]_2$ the binary representation of the integer argument. An example mapping of the value $d(i)$ into the bits p_{1i}, p_{2i}, p_{3i} and $d_\Delta(i)$ is illustrated in the Figure 3.

Then the digest of vector d_Δ by means of any convenient hash function can be calculated. The obtained hash is signed with the use of cryptographic DS [1] and then this DS is embedded jointly with the auxiliary perturbation vector p into the image I. Verification of DS is performed by conventional cryptographic methods, where it is necessary to recover the

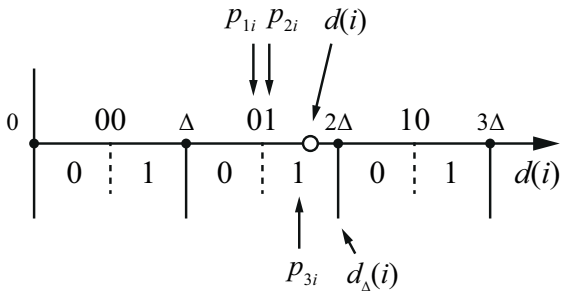

Fig. 3. An example mapping of the value $d(i)$ into the bits p_{1i}, p_{2i}, p_{3i} and $d_\Delta\,(i)$ by means of 3-bit quantization technique.

feature vector $\tilde{d_\Delta}$ only, which corrupted possibly by JPEG compression of the original feature vector d'_Δ. This can be performed as follows [18]

$$d'_\Delta(i) = \left\lfloor \frac{d'(i)}{\Delta} \right\rfloor \tag{12}$$

where

$$d'(i) = \begin{cases} \tilde{d}(i) + \Delta & \text{if } \alpha_i = 0 \ \&\ \tilde{p}_{3i} = 0 \\ \tilde{d}(i) + \Delta & \text{if } \alpha_i = 0 \ \&\ \tilde{p}_{3i} = 1 \ \&\ p'_{3i} = 1 \\ \tilde{d}(i) - \Delta & \text{if } \alpha_i = 1 \ \&\ \tilde{p}_{3i} = 1 \\ \tilde{d}(i) - \Delta & \text{if } \alpha_i = 1 \ \&\ \tilde{p}_{3i} = 0 \ \&\ p'_{3i} = 0 \\ \tilde{d}(i) & \text{otherwise} \end{cases}$$

and

$$\alpha_i = \begin{cases} 0 & \text{if } [p'_{1i}p'_{2i}]_{10} = ([\tilde{p}_{1i}\tilde{p}_{2i}]_{10} - 1) \bmod 4 \\ 1 & \text{if } [p'_{1i}p'_{2i}]_{10} = ([\tilde{p}_{1i}\tilde{p}_{2i}]_{10} + 1) \bmod 4 \\ 2 & \text{otherwise} \end{cases} . \tag{13}$$

Here $[\cdot]_{10}$ is the decimal representation of the binary integer; $(\tilde{p}_{1i}, \tilde{p}_{2i}, \tilde{p}_{3i})$ are the three bits of each entry $\tilde{p}_i$ of the perturbation vector $\tilde{p}$ extracted as a WM, and $(p'_{1i}, p'_{2i}, p'_{3i})$ are obtained from the perturbation vector p' calculated by (10), (11) given by the corrupted image $\left(\tilde{I}(m)\right)_{m\in\mathcal{G}}$; $\tilde{d}(i)$ is the *i*-th element of the feature vector given by (8) and the image $(I(m))_{m\in\mathcal{G}}$ is the original one before recovering.

It has been proved in [18] that the feature vector $\tilde{d_\Delta}$ can be recovered exactly by (12)–(13) if the extracted auxiliary perturbation vector $\tilde{p}$ is correct and rule (9) is achieved. This rule will be fulfilled if a corruption of the quantized feature vector coordinates $\tilde{d_\Delta}(i)$ have transitions to at most one neighbour quantization level. In this case the proposed authentication method will be tolerant to JPEG compression if the quantization step was chosen in such a way that the last requirement holds with the high probability. Clearly, the method of embedding and extraction is also assumed to be robust to JPEG compression.

IV. Watermarking method based on 3-level HWT coefficients quantization

In this section we consider a digital watermarking method providing acceptable error probability of both feature vector signature and auxiliary perturbation vector. An authentication

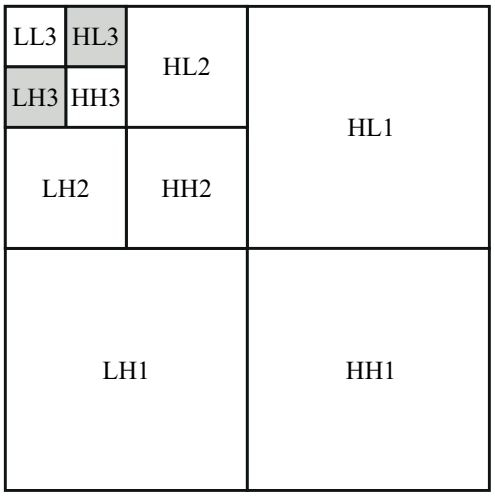

Fig. 4. Notations of 3-level Haar wavelet transform coefficients submatrices. The used HWT areas LH3 and HL3 are highlighted.

data, that is usually briefly called *authenticator* [2], is embedded into the image with one of the existing watermarking techniques. Authenticator of the proposed method consists of both feature vector d signature and the auxiliary perturbation vector p have been explained in the Section III. There are several necessary properties for the embedding algorithm for the proposed selective image authentication system namely

- tolerance to JPEG compression;
- capacity that is enough for both d and p;
- lower computational complexity; and
- high visual quality of the watermarked image right after embedding.

Taking into account the requirements presented above, the embedding algorithm based on coefficients quantization of 3-level discrete *Haar Wavelet Transform* (HWT) [14] was selected. Only LH3 and HL3 submatrices for WM embedding were chosen because of their robustness to small noises that can be introduced by JPEG compression. According to the experimental results, the coefficients of LL3 which have more evident influence on visual image quality after embedding whereas second level coefficients are less tolerant to JPEG compression. So, in this method, LH3 and HL3 areas are selected as a compromise. Let assume for simplicity that the DI is square of order $2^l \times 2^l$. Note that if the image I is not represented by a square matrix then it can be padded with zero elements. According to [14], two-dimensional forward and inverse HWT of the square image luminance values $(2^l \times 2^l)$-matrix of the image I can be found as:

$$S_H = H_l I H_l^T, \quad I = H_l^T S H_l, \tag{14}$$

where l is the level of HWT, S_H is the matrix of the HWT coefficients, and the upper index T denotes matrix transposition. The recurrent relations [14]

$$H_0 = [1], \quad H_l = \frac{1}{\sqrt{2}} \begin{bmatrix} H_{l-1} & H_{l-1} \\ H_{l-1} & -H_{l-1}, \end{bmatrix}, \quad l \in \mathbb{Z}^+$$

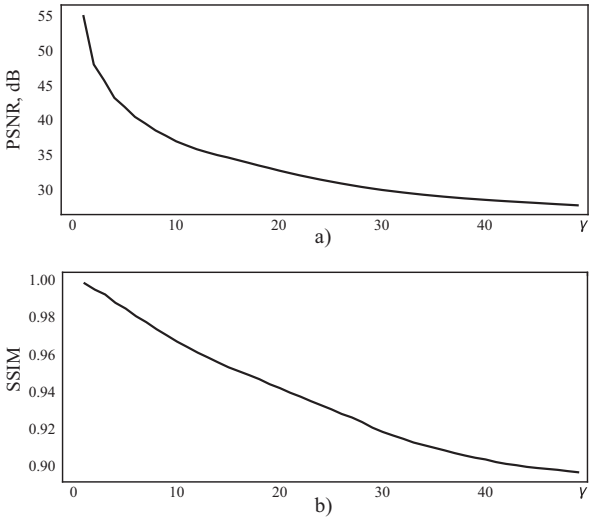

Fig. 5. Dependencies of PSNR and SSIM image quality measures just after WM embedding against HWT coefficients quantization parameter γ.

determine the $(2^l \times 2^l)$-Haar single level matrices H_l. The next level l of HWT can be obtained if, the $(2^{l-1} \times 2^{l-1})$-submatrix of HWT approximation coefficients is used instead of the original image I. Figure 4 shows the 3-level HWT coefficients submatrices with conventional notations and the used HWT areas LH3 and HL3 as highlighted ones.

We chose only LH3 and HL3 coefficients as they represent low-frequency components of the image and have explicit robustness to the distortions introduced by JPEG compression, see Figure 5. The used approach allows to minimize DI corruption after embedding. The general scheme of proposed selective image authentication method including embedding and extraction procedures with correspondent notations is presented at Figure 6.

The quantized feature vector d_Δ is hashed and signed by any standard cryptographic algorithm [1] giving strong digital signatures s. Next, this DS and perturbation vector p is concatenated into one binary string b. In order to increase efficiency of authentication data transferring in the presence of corrupting noise *Low-Density Parity-Check* (LDPC) code [19] was applied. Encoded block b_e represented by digits b_{e_k} is embedded into the coefficients S_k belonging to HWT areas HL3 and LH3 (Figure 4) by the following rule:

$$\tilde{S}_k = \begin{cases} \gamma\left(\left[\frac{S_k}{\gamma}\right] + \frac{1}{4}\right) & \text{if } b_{e_k} = 1 \\ \gamma\left(\left[\frac{S_k}{\gamma}\right] - \frac{1}{4}\right) & \text{if } b_{e_k} = 0 \end{cases} \tag{15}$$

where γ is the quantization interval of HWT coefficients, $[\cdot]$ is the nearest integer of a real number, and $\tilde{S}_k$ is the coefficient after embedding the bit b_{e_k}. In order to complete embedding procedure an inverse HWT is performed by (14) using quantized coefficients from (15).

An obtained watermarked image $\hat{I}$ is then sent through insecure channel and is possibly have been forged by an attacker

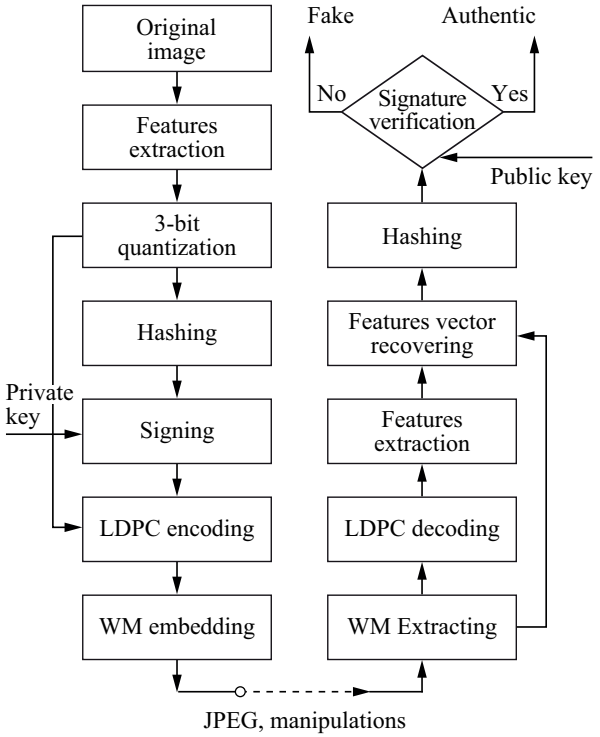

Fig. 6. General scheme of the proposed selective image authentication method.

or have been processed using non-malicious manipulations. In order to verify that DS is authentic, see Figure 6, it is necessary to take a decision $\tilde{b}_{e_k}$ regarding the digits of the binary string b_e using the decision rule

$$\tilde{b}_{e_k} = \begin{cases} 1 & \text{if } \tilde{S}_k - \gamma\left[\frac{\tilde{s}_k}{\gamma}\right] \geq 0, \\ 0 & \text{if } \tilde{S}_k - \gamma\left[\frac{\tilde{s}_k}{\gamma}\right] < 0. \end{cases} \tag{16}$$

Here $\tilde{S}_k$ are the coefficients S_k of areas HL3, LH3 that might be corrupted by some image processing. Decoding of received code word $\tilde{b}_e$ is performed with *iterative belief propagation* technique [20].

The elements of the perturbation vector $\tilde{p}$ are extracted from decoded data using (16) and the vector p' calculated directly from the image by (10), (11), and then recover d'_Δ, given the vectors $\tilde{d}_\Delta$, $\tilde{p}$ and p'. Then the recovered vector d'_Δ is hashed to h' and compared with the hash $\tilde{h}$ obtained from the DS $\tilde{s}$ with use of the corresponding public key. If $h' = \tilde{h}$ then DI is recognized as authentic, otherwise it is assumed as a fake one.

V. Evaluation of Effectiveness of Proposed Selective Image Authentication

In this paper we focus ourselves on JPEG compression related to the set of manipulations that not change an image content. Thus, it is necessary to investigate the sensitivity of the authentication system to JPEG compression. The proposed

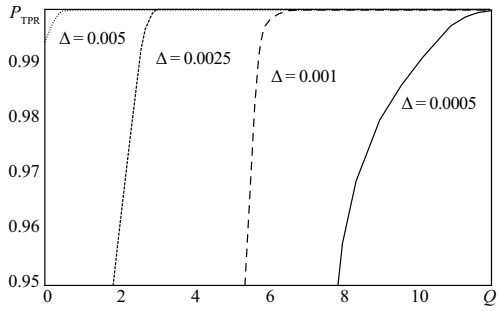

Fig. 7. Dependencies of the P_{TPR} against JPEG compression quality with factor Q depending on the different feature vector quantization parameters Δ.

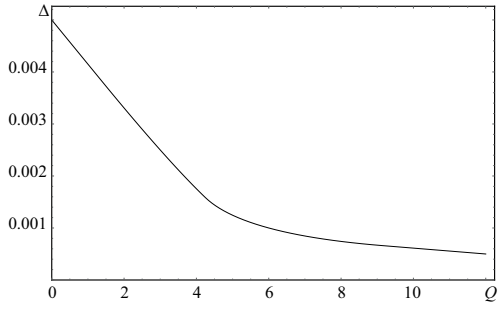

Fig. 8. Dependency of the required value of feature vector quantization parameter Δ against JPEG compression quality factor Q that gives $P_{\text{TPR}} = 100$ over the test image base.

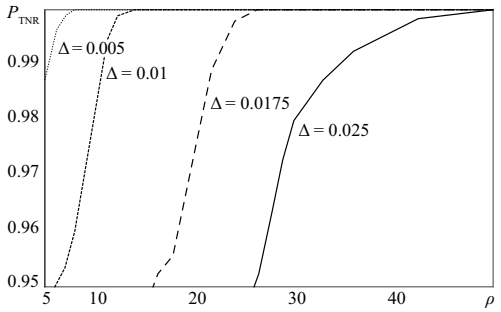

Fig. 9. Dependencies of the P_{TNR} against the size ρ of malicious image tampering areas depending on the different feature vector quantization parameters Δ.

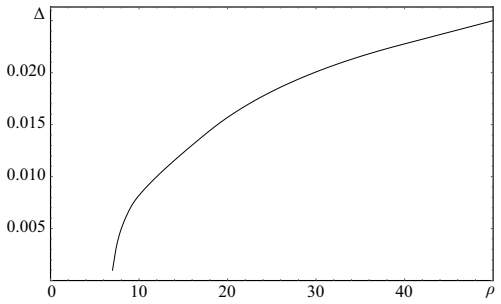

Fig. 10. Dependency of required value of feature vector quantization parameter Δ against the size ρ of malicious image tampering areas that gives $P_{\text{TNR}} = 100$ over the test image base.

method will be tolerant to such compression if the rule (9) is met. We have selected 100 different 512×512 DI having varied content, textures and so forth. Then the HL3 and LH3 areas of HWT contains $2 \times (2^6)^2 = 2^{13} = 8192$ coefficients. According to the rule (15), each HWT coefficient allows to embed one bit.

As we mentioned before, in order to provide some redundancy, the length of the feature vector d was $2^{10} = 1024$ corresponding to the length of $2^8 = 256$ of the matrix b_k. This requires $h = 2^{10} = 1024$ in (6). Thus, the auxiliary perturbation vector p has $3 \times 2^{10} = 3072$ bits length. As a hash function, the standard SHA-2 [1] and the DS algorithm based on RSA cryptosystem [1] with length of modulo 1024 bits were used. The total size of the embedded bits is $3072 + 1024 = 4096$. Given the total number of HWT coefficients in HL3 and HL3 areas it was chosen the $(8192, 4096)$-LDPC code to achieve appropriate error correction.

It is worth to note, that proposed selective image authentication framework allows one to choose any other hash, digital signature and error correcting algorithms which are suitable for the available watermark capacity. After the selection of the main parameters, the investigation of the authentication system efficiency was carried out. Figure 7 shows the dependencies of the *True Positive Rate* P_{TPR} against JPEG compression quality factor $Q = 0, 1, \ldots, 12$ depending on the different feature vector quantization parameters Δ used in the formation of d_Δ by (8).

It can be seen from Figure 8 that the greater is the *Quality factor* Q, the better is image authentication method tolerant to JPEG compression.

The strongest requirements should be formulated for the opportunity to detect all image pixel modifications except for JPEG compression, for instance, some random modifications or malicious attacks intended to compromise the original image, for the thing, changing of car plate numbers for DVR systems, or fingerprints and photos of criminals in police offices. It is a trivial problem for exact authentication, provided that the cryptographic components, namely hash function and DS were selected in an appropriate manner. But it is a relevant problem for semi-fragile authentication because in this case some modifications can not be detected. In order to verify such opportunity for the system under consideration we arranged the following experiment. It was selected a truly randomly circle areas with $(\rho/2)$-pixel radius and inside these areas truly random luminance of pixels was chosen. At least 50 such areas were taken for each image and the number of different typical images was 100. The results of testing are presented in Figure 9, where a dependence of *True Negative Rate* P_{TNR} is showed as a function of areas size ρ depending on quantization step Δ of the feature vector coordinates.

From Figure 9 it can be seen that, in accordance with our expectations, the less is a quantization step Δ, the more probably to detect small image modifications.

In Figure 10 a curve showing a dependence of the requested values of quantization steps Δ against the size of modification

a) b)

Fig. 11. Examples of the original test image «Lena» and the watermarked version just after embedding with PSNR = 41.3 dB with $\gamma = 9$.

area ρ given a by $P_{\text{TNR}} = 1$ is presented for the whole test image base.

Summarizing the experimental results, we can conclude that the proposed authentication method is tolerant to JPEG compression with parameter $Q \geq 1$ providing simultaneously $P_{\text{TNR}} \geq 1$ for modification area size $\rho \geq 8$.

Image quality of DI just after WM embedding is also very important criterion of authentication system efficiency. We evaluate both *Peak Signal-to-Noise Ratio* (PSNR) [21] and *Structural Similarity Index Measure* (SSIM) [22] as commonly used measures and for 8-bit digital images can be calculated as

$$\text{PSNR} = 10 \log_{10} \left[\frac{255^2 MN}{\sum_{m \in \mathcal{G}} \left(I(m) - \hat{I}(m) \right)^2} \right], \qquad (17)$$

$$\text{SSIM} = \frac{\left(2\mu_I \mu_{\hat{I}} + c_1\right)\left(2\sigma_{I\hat{I}} + c_2\right)}{\left(\mu_I^2 + \mu_{\hat{I}}{}^2 + c_1\right)\left(\sigma_I{}^2 + \sigma_{\hat{I}}{}^2 + c_2\right)}, \qquad (18)$$

where μ_I, $\mu_{\hat{I}}$ are mean values, σ_I, $\sigma_{\hat{I}}$ are variances and $\sigma_{I\hat{I}}$ is covariance calculated for I and $\hat{I}$ respectively, $c_1 = 255^2 \cdot 10^{-4}$, $c_2 = 255^2 \cdot 3 \cdot 10^{-4}$ are the constants.

In Figure 5 the curves of image quality assessments PSNR and SSIM given by (17), (18) depending on the quantization step Δ are presented. We can see that the greater is Δ, the worse is the visual comprehension of the images. On the other hand the proposed system requires to keep Δ be not very small in order to WM be tolerant to JPEG compression.

In Figure 11 the visual effect of WM embedding for some chosen WM system parameters is displayed. There is no opportunity to find any differences between images (a) and (b). However, it is worth to note that reliable detection of the image modification has a greater importance than false detection after JPEG compression, because in the last case an error can easily be recognized, whereas the authenticated image content corruption may lead to fatal consequences.

It is obvious that for valid authentication system operation, the *bit error rate* BER after LDPC decoding of code block b_e should be equal to zero even after image compression. Figure 12 (a) specify this problem. This figure shows a dependencies of *bit error rates* (BER) against quantization step γ for HWT coefficients depending on different values of JPEG compression factor Q. It can be seen that there exist

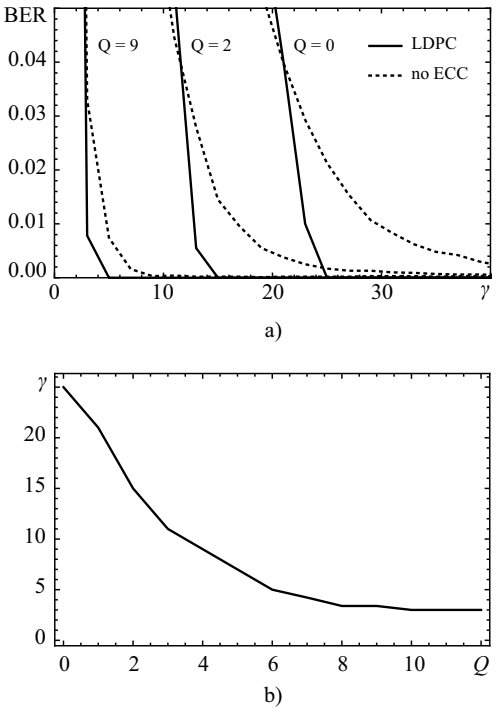

Fig. 12. a) Dependencies of the BER versus HWT coefficients quantization parameter γ given by different JPEG compression quality factor Q with and without LDPC error correction code. b) Dependency of HWT coefficients quantization parameter γ allowing to extract WM without errors against JPEG compression quality factor Q.

values of γ leading to BER$= 0$ in case when LDPC coding is applied, whereas in the case of watermarking without error correction code (ECC) BER is mostly non-zero. Figure 12 (b) presents the dependence of the quantization intervals γ on JPEG compression quality factor Q given the condition BER$= 0$.

Figure 12 shows that the selection of the quantization interval γ equal to 10 provides a resistant authentication method to JPEG compression with quality factor $Q \geq 4$ and quality assessments PSNR ≥ 40, $SSIM > 0.98$ that can be assumed as acceptable values.

VI. Conclusion

The article introduces the new selective image authentication system. The novelty of the method is application of the discrete shearlet transform coefficients for the image features vector calculation procedure. An image authenticator consists of two parts. The first one is the DS of the quantized image feature vector and the second one is the auxiliary perturbation vector generated by 3-bit hash quantization technique. It provides a recovering of hash function even after jumps of the vector coordinates due to JPEG compression.

Quantization of 3-level discrete HWT coefficients as a watermarking technique which allows us to embed authentication data into the digital image was used. Due to the high capacity of this watermarking method an additional redundancy was achieved. This property was used for the error correction code.

We embed WM only into HL3 and LH3 areas of the HWT as it keeps visual image distortion smaller than in case of LL3 area usage. Experimental investigation showed that proposed authentication method provides a good reliability to verify image authenticity even after JPEG compression with Q ≥ 3 and simultaneously an opportunity to recognise even small content image modifications and image quality assessments PSNR ≥ 40 and $SSIM > 0.98$ just after WM embedding.

Proposed selective image authentication allows one to adjust system parameters so that resulting BER, Q, PSNR, SSIM, TNR, and TPR became acceptable with the needs.

ACKNOWLEDGMENT

Author thanks professor V. Korzhik for his everyday kind attention, help in investigations, and fruitful discussions.

REFERENCES

[1] A. A. J. Menezes, P. Van Oorschot, and S. Vanstone, *Handbook of Applied Crytography*, ser. Discrete Mathematics and Its Applications Series. Crc Press, 1997.

[2] A. Haouzia and R. Noumeir, "Methods for image authentication: A survey," *Multimedia Tools Appl.*, vol. 39, no. 1, pp. 1–46, Aug. 2008. [Online]. Available: http://dx.doi.org/10.1007/s11042-007-0154-3

[3] M. H. Lee, V. I. Korzhik, G. Morales-Luna, S. Lusse, and E. Kurbatov, "Image authentication based on modular embedding." *IEICE Transactions*, vol. 89-D, no. 4, pp. 1498–1506, 2006.

[4] M. Goljan, J. J. Fridrich, and R. Du, "Distortion-free data embedding for images," in *Proceedings of the 4th International Workshop on Information Hiding*, ser. IHW '01. London, UK, UK: Springer-Verlag, 2001, pp. 27–41.

[5] X.-y. Wang, L.-m. Hou, and J. Wu, "A feature-based robust digital image watermarking against geometric attacks," *Image Vision Comput.*, vol. 26, no. 7, pp. 980–989, Jul. 2008. [Online]. Available: http://dx.doi.org/10.1016/j.imavis.2007.10.014

[6] M. Alghoniemy and A. H. Tewfik, "Geometric invariance in image watermarking," *IEEE Transactions on Image Processing*, vol. 13, no. 2, pp. 145–153, Feb 2004.

[7] S. Shefali and S. M. Deshpande, "Moment invariants for digital image authentication and authorization," in *2007 International Conference on Control, Automation and Systems*, Oct 2007, pp. 1296–1300.

[8] H. M. Al-Otum, "Color image authentication using a zone-corrected error-monitoring quantization-based watermarking technique," *Optical Engineering*, vol. 55, no. 8, p. 083103, 2016.

[9] A. Zhuvikin, V. Korzhik, and M.-L. Guillermo, "Semi-fragile image authentication based on CFD and 3-bit quantization," *Indian Journal of Science and Technology*, vol. 9, no. 48, 2017.

[10] E. Maiorana, P. Campisi, and A. Neri, "Signature-based authentication system using watermarking in the ridgelet and radon-dct domain," pp. 67 410I–67 410I–12, 2007. [Online]. Available: http://dx.doi.org/10.1117/12.738013

[11] G. K. Wallace, "The jpeg still picture compression standard," *IEEE Trans. on Consum. Electron.*, vol. 38, no. 1, pp. xviii–xxxiv, Feb. 1992. [Online]. Available: http://dx.doi.org/10.1109/30.125072

[12] G. Kutyniok and D. Labate, *Shearlets: Multiscale Analysis for Multivariate Data*. Birkhauser Mathematics, 2012.

[13] Y. Qu, X. Mu, L. Gao, and Z. Liu, *Facial Expression Recognition Based on Shearlet Transform*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 559–565. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-29387-0_86

[14] P. Porwik and A. Lisowska, "The Haar wavelet transform in digital image processing: its status and achievements." *Int. Journal Machine Graphics & Vision.*, vol. 13, no. 1, pp. 79–98, 2004.

[15] S. Hauser, "Fast finite shearlet transform: A tutorial," 2011, university of Kaiserslautern, Preprint.

[16] I. Amidror, *Mastering the Discrete Fourier Transform in One, Two or Several Dimensions: Pitfalls and Artifacts*, 1st ed. Springer Publishing Company, Incorporated, 2015.

[17] N. A. Dodgson, "Image resampling," University of Cambridge, Computer Laboratory, Tech. Rep. UCAM-CL-TR-261, 1992.

[18] F. Ahmed and M. Y. Siyal, *A Robust and Secure Signature Scheme for Video Authentication*. 2007 IEEE, International Conference on Multimedia and Expo, 2007.

[19] R. G. Gallager, "Low-density parity-check codes," 1963.

[20] G. V., "Iterative decoding of low-density parity check codes (a survey)," *eprint arXiv:cs/0610022*, 2006.

[21] Q. Huynh-Thu and M. Ghanbari, "Scope of validity of PSNR in image/video quality assessment," *Electronics letters*, vol. 44, no. 13, pp. 800–801, 2008.

[22] E.-M. A. Mohammadi P. and S. Sh., "Subjective and objective quality assessment of image: A survey," 2014.