INFORMATICA, 2012, Vol. 23, No. 4, 507–520

Pixel-Wise Tamper Detection Under Generic Blur/Sharpen Attacks

Romualdas BAUŠYS, Artūras KRIUKOVAS
Vilnius Gediminas Technical University, Graphical System Department
Saulėtekio al. 11, LT-10223, Vilnius, Lithuania
e-mail: romas@fm.vgtu.lt

Received: June 2011; accepted: June 2012

Abstract. In this paper robust image authentication integrated with semi-fragile pixel-wise tamper localization is analyzed. A new pixel-wise transformation robust to blurring/sharpening while fragile to all other image processing operations is proposed. A new method featuring binary and percentage measures with novel ability to integrate human opinion for image authenticity evaluation is presented. Protection for all bits in the pixel is advantage as well as small size of the signature – less than 10% of initial image.

Keywords: image digital signature, semi-fragile, blur, sharpen resistant, pixel-wise tamper localization.

1. Introduction

Image authentication and tamper localization nowadays are becoming more and more important as influence of digital media increases in our life. One of serious challenges in image protection and tamper localization is detection and evaluation of blur or sharpen operations. In standard, casual, every day image processing, use of these operations does not change the essence of the image. Even more, they are used in order to increase attractiveness of the image by blurring it a bit or by highlighting the smallest details by sharpening it. But these two global processing operations present so big challenges in image tamper localization because of their effect on digital image matrices. Simple blurring operation, based on mathematical averaging of pixel values in scrolling window region, affects the whole image, it leaves no pixel untouched. In such situation only some block-based methods, based on global (average) characteristics of the block are robust enough to survive. Pixel-based methods face serious challenges, as every pixel is modified and usually changes are quite extreme, over 50%. For example, pixel in standard Lena image with initial value 39, became 67 after one iteration of blurring – a change almost 75% from initial value. A pixel with initial value 121 after one iteration of sharpening became equal to 255. All pixels face similar, enormous changes, limited only by the limits of integer digits (0–255) – although for human vision the image does not appear significantly modified. Naturally, pixel-based tamper localization algorithms detect changes of such

scale as malicious – though they are not. That's why pixel-based tamper localization algorithms fail to detect attacks after blurring or sharpening – the whole picture appears to be tampered with, after only a single innocent image quality enhancement operation (Lu *et al.*, 2009; Wang and Lu, 2009). Even block-based algorithms do not propose a complete solution.

Semi-fragile algorithms based on quantization have been proposed in the literature in order to conquer the problem. Eggers and Girod (2001) used a scaling factor and a pseudo-random number for their quantization based watermark. This randomizes the embedding residue, which was also used in Zhu quantization based robust and fragile watermarking schemes (Swanson *et al.*, 1997; Zhu, 1998). Wu and Kuo (2002) applied the Kundur watermark (Kundur and Hatzinakos, 1999) to log values of the magnitude of the low frequency DFT coefficients for speech authentication, with the non-adaptive quantization step at each coefficient determined according to the SNR of a speech codec at that frequency. Salient points, where the audio signal energy is fast climbing to a peak and a synchronization mark by robust audio watermarking are used for synchronization. Tefas and Pitas (2000), Bartolini *et al.* (2001) applied chaotic mixing procedures to generate a watermark from a small logo and then embedded it for image and video authentication. The algorithms present limited robustness against minor blur/sharpen operations. Furthermore, another objective is not solved – no pixel-wise tamper localization is available. The best tamper localization resolution available is limited to the size of one block.

Edges of an image can also be used as features for image/video content based authentication (Queluz, 1998, 1999; Dittmann *et al.*, 1999), as well as zero-crossings (Li *et al.*, 2000), which can be considered as a special case of edges. But in such cases, as well as with all feature based authentication methods, we lose tamper localization. Binary images show better characteristics because of their definition, however the information they contain is very limited (Ganesan and Guptha, 2010; Valantinas and Zumbakis, 2007). PKI helps to identify authentication, at the cost of lost tamper localization (Kazakeviciute and Januskevicius, 2005).

A bit another approach was taken by Eggers (Eggers and Girod, 2001) – the user is allowed to decide whether the content has suffered from a malicious or non-malicious manipulation. The verifier calculates the likelihood of a modification event. It is expected that this score is null if the content is authentic, small if some light modification (non-malicious) has been performed and high if the opponent has modified this piece of content (forgery). It is up to the user to set the threshold between the semi-fragile authentication and forgery. Some statistical considerations can help him. For instance, in Kundur and Hatzinakos (1999), the verifier calculates the bit-error rate. This measure equals zero in case of successful authentication and $\frac{1}{2}$ in case of unsigned content. In the same way Zhu *et al.* (2004) estimate the mean square error between the observed coefficients and their expected values (knowing the bits they should carry). Filtering in Fourier domain is proposed to increase robustness of fingerprint identification (Popovic *et al.*, 2011).

As we see in order to enable pixel-wise tamper localization after general image processing operations, such as blurring or sharpening, we need a new solution.

2. Invariance to Blur/Sharpen Procedures

With the introduction of the new and more effective JPEG-2000 image compression method and a decision to use wavelets instead of DCT as a basis for the JPEG-2000, wavelet transform domain become more attractive to the watermarking research community. The advantages of using the wavelet transform domain are an inherent robustness of the scheme to the JPEG-2000 lossy compression, and possibility of minimizing computation time by embedding watermarks inside of a JPEG-2000 encoder. Additionally, the wavelet transform has some properties that could be exploited by digital image security solutions. For example, wavelet transform provides multi-resolution representation of images, and this could be exploited to build more efficient watermark detection schemes, where watermark detection starts from the low-resolution sub-bands first, and only if detection fails in those sub-bands, it explores the higher resolution subbands and additional coefficients it provides. The following advantages of the wavelet transform domain are defined in Meerwald and Uhl (2001) – space-frequency localization, multi-resolution representation, superior HVS modeling, liner complexity and adaptivity. However the new wavelet transform fails to provide any robustness against blurring or sharpening. This is why we took a decision to return back to more classical Fourier transform.

2.1. *Discrete Fourier Transform and Phase of the Transform*

Fourier transformation is one of the basic analysis tools. Many different fields use Fourier analysis – electronics, radio, medicine, astrology – image processing as well. Our image is a continuous function $f(x, y)$ with M uniformly-spaced samples in the x direction and N samples in the y direction and that the inter-sample distances are Δx and Δy respectively. The discrete Fourier transform of $f(x, y)$ is then defined as:

$$F(p,q) = \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x,y) \mathrm{e}^{-i2\pi(\frac{px}{M}+\frac{qy}{N})}, \tag{1}$$

where $p = 0, 1, 2, \ldots, M-1,\ q = 0, 1, 2, \ldots, N-1$.

Each value of a Fourier transformed image $F(p, q)$ is a complex number. As it is more convenient to think about complex numbers as vectors, having a magnitude and a phase angle, $F(p, q)$ may be expressed in terms of its magnitude and phase:

$$F(p,q) = |F(p,q)| \mathrm{e}^{i\varphi(p,q)}, \tag{2}$$

where

$$\big|F(p,q)\big| = \sqrt{\mathrm{Re}(p,q)^2 + \mathrm{Im}(p,q)^2}, \tag{3}$$

$$\varphi(p,q) = \tan^{-1} \frac{\mathrm{Im}(p,q)}{\mathrm{Re}(p,q)}. \tag{4}$$

$|F(p,q)|$ is the real-valued Fourier amplitude spectrum and $\varphi(p,q)$ is the real-valued phase spectrum. This exponential form which, on the face of it looks more complicated is very useful as it allows us to think of each Fourier component, i.e., each complex Fourier value at a given spatial frequency (p,q) as a vector having magnitude $|F(p,q)|$ and phase $\varphi(p,q)$. Thus we can think about the Fourier transform of an image in two ways:

(a) as a 2-D distribution of complex numbers;

(b) as a 2-D distribution of vectors.

Conceiving the Fourier transform as a 2-D distribution of vectors is particularly appealing because it allows us to visualize a 2-D Fourier transform quite easily and it facilitates a very intuitive understanding of the Fourier transform and its properties.

2.2. *Blur/Sharpen Effect on the Phase of the Fourier Transform*

We assume that blur in the image is spatially invariant. This assumption corresponds quite accurately to a real situation where the blur is a result of an out of focus lens or linear motion of the camera. In the discrete model for spatially invariant blurring/sharpening of an original image $f(x)$ resulting in an observed image $g(x)$ can be expressed by a convolution:

$$g(x) = (h * f)(x), \tag{5}$$

where $h(x)$ is the point spread function (PSF) of the blur, $*$ denotes 2-D convolution and x is a vector of coordinates $[x,y]$. In Fourier domain this corresponds to:

$$G(u) = H(u)\cdot F(u), \tag{6}$$

where $G(u)$, $F(u)$ and $H(u)$ are the discrete Fourier transformations (DFT) of the blurred/sharpened image $g(x)$, the original image $f(x)$ and the PSF $h(x)$ respectively and u is a vector of coordinates $[u,v]$. We may separate the magnitude and phase parts of (6), resulting in:

$$\big|G(u)\big| = \big|H(u)\big|\cdot\big|F(u)\big| \tag{7}$$

$$\varphi\big(G(u)\big) = \varphi\big(H(u)\big) + \varphi\big(F(u)\big), \tag{8}$$

where (7) and (8) represent magnitude and phase of the blurred/sharpened image $g(x)$.

If blur/sharpen PSF $h(x)$ is centrally symmetric, then $h(x) = h(-x)$ its Fourier transform is always real-valued and as a consequence its phase is only a two-valued function given by:

$$\varphi\big(H(u)\big) = \begin{cases} 0, & \text{if } H(u) \geqslant 0, \\ \pi, & \text{if } H(u) < 0. \end{cases} \tag{9}$$

This means that $\varphi(G(u)) = \varphi(F(u))$ for all $H(u) \geqslant 0$ and proves that phase of Fourier transform is essentially unaffected by image blurring/sharpening operations. This

property became one of building blocks of the new MPOF transformation, invariant to image sharpening or blurring and rotating.

We have shown property of Fourier phase – robustness to blur/sharpen operations. This property becomes one of key elements in the proposed method – but it makes only one step closer to final method. It should be noticed that Fourier domain generally and Fourier phase as well, maintain no spatial relation with the pixels in spatial domain. Pixel in spatial domain is transformed into a property of sine wave in Fourier domain. If we want to have pixel-wise tamper localization, we have to introduce and enforce relation of pixel in spatial domain with pixel in Fourier domain.

3. Proposed Method

MPOF transformation (modified phase only filter transformation) is called a process of transforming spatial domain into specially processed phase of Fourier transform. The full transformation is described here, in practical implementation the transformation is separated in two parts. The first part of the process is used in digital signature generation; the second part of transformation process is used in establishing tampered pixels.

3.1. *Architecture of the Modified Phase Only Filter Transformation*

The MPOF transformation is designed in a special way, to be semi-invariant to blur/sharpen image processing operations and to hold spatial localization feature. It transforms the given image from spatial domain to transformation domain that essentially has spatial characteristics with added invariance to image blurring/sharpening.

Previously we have proved that phase of Fourier transformation is unaffected by image blurring/sharpening operations. However phase domain fails to sustain spatial relation with spatial domain, i.e., pixel in spatial domain is expanded over the all phase domain. If we have tampered pixel we cannot locate it in Fourier phase and otherwise – detection of change in Fourier phase is of no help for us when trying to determine exact pixel that is the cause of the change. Therefore we need to enforce spatial relation between spatial domain and the domain of Fourier phase.

Let $f(x, y),\ 0 \leqslant x,\ y \leqslant N-1$ be an image in non-negative $\boldsymbol{Z}^2$ domain. MPOF transformation of the image $f(x, y)$ is defined as following:

(1) 2-D discrete Fourier transformation of $f(x, y)$ is calculated:

$$F_I(l, m) = \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} f(x, y) \exp\left[-i\frac{2\pi}{N}(xl + ym)\right]. \tag{10}$$

(2) Let us define A^1 as a matrix:

$$A^1(x, y) = 1, \quad 0 \leqslant x,\ y \leqslant N-1. \tag{11}$$

(3) Integer b is maximized with the respect to the following inequality:

$$\mathcal{F}^{-1}\{bA^1(l,m)\mathrm{e}^{i\varphi_{f(l,m)}}\}<256, \tag{12}$$

where $\varphi_{f(l,m)}$ is phase of the signal calculated by (4).

(4) Transformation matrix A is generated:

$$A(p,q)=\begin{cases} bA^1+1, & \text{where } q \text{ is even,}\\ bA^1-1, & \text{where } q \text{ is odd.}\end{cases} \tag{13}$$

(5) Inverse discrete Fourier transformation is calculated:

$$f^d(x,y)=\mathcal{F}^{-1}\{A(l,m)\mathrm{e}^{i\varphi_{f(l,m)}}\}(x,y). \tag{14}$$

Resulting image $f^d(x,y)$ is almost invariant to blur/sharpen operations on the original image $f(x,y)$. In case of extreme blurring or sharpening, some Gaussian noise appears in transform domain – but in case of extreme blurring/sharpening it is more a question of how much original image has been left.

3.2. *Algorithm of the Proposed Method*

The algorithm of the digital signature method, based on the MPOF, is proposed in this section. Authentication establishment and tamper localization procedures are also described here.

3.2.1. *Generation of the Digital Signature*

The algorithm of digital signature generation is constructed as follows:

(1) Nth level down-sampling of the image $f(x,y)$ is

$$B_1=LL_N\big(f(x,y)\big) \tag{15}$$

Level N is chosen in such a way, that size of final decomposed image should be no less than 32×32 pixels and no more than 64×64 pixels, i.e., $(32,32)\leqslant \text{size}(f(p,q))<(64,64)$. Resulting image B_1 is used in image authentication establishment procedures.

(2) Original image is partially transformed into MPOF space. 2-D discrete Fourier transform of $f(x,y)$ is calculated and phase $\varphi_{f(l,m)}$ is extracted (4, 10).

(3) Resulting phase is quantized and compressed in order to achieve efficient size of the signature. We recommend using JPEG compression method – this allows achieving signature size less than 8% of initial image size. However other compressions methods, such as ZIP or JPEG-2000, are available [5].

$$f_{\text{compressed}}(x,y)=\text{JPEG}\big(f_{\text{MPOF}}(x,y)\big) \tag{16}$$

(4) Resulting compressed image $f_{\text{compressed}}(x, y)$ is permutated according to a secret key K in order to enable private key based image authentication:

$$f_K(x, y) = K\big(f_{\text{compressed}}(x, y)\big). \tag{17}$$

If public usage is required then K is initialized to a known in advance value. Resulting image is used in image tamper localization procedures.

(5) Finally, parts of would-be digital signature are combined together into a final digital signature of the image $f(x, y)$:

$$\text{DS}\big(f(x, y)\big) = B_1 \cup f_K(x, y). \tag{18}$$

Some comments on the algorithm above.

First of all, separation of image authentication and tamper localization parts is enforced in order to prevent oracle attack. Oracle attack makes extensive usage of image authentication engine changing the image pixels one-by-one until the modified image passes image authenticator as authentic one. This attack is the most effective when image authentication is based only on tamper localization function. The proposed algorithm completely disables oracle attack by separating image authentication and tamper localization processes. Now it is more complicated to adopt the attacked image to pass both authentication and tamper localization engines, especially as they have no common mathematical basis in between.

Image down-sampling was chosen as an engine for generating a small size data set for image authentication. This mechanism is numerically effective, allows for easy digital authentication establishment with SSIM index, allows for initial rough tamper localization and allows backup human opinion integration in authenticity establishment process – a feature, which can be rarely found in other algorithms.

Permutation according to a secret key K is optional step (permutation with $K = 1$ effectively means no permutation) in order to allow for private/public usage. If K is used, then even obtained digital signature has no commercial value for the would-be attacker.

3.2.2. *Determining Image Authentication*

Establishment of authenticity of image in question is fast and not expensive operation that requires no special transformations. If we have image in question $f'(x, y)$ then:

(1) Nth level down-sampling of the image in question $f'(x, y)$ is calculated:

$$B'_1 := LL_N\big(f'(x, y)\big). \tag{19}$$

(2) B_1 from the digital signature is extracted.

(3) Structural similarity index is calculated between these two images:

$$\text{rez\_sim} = \text{SSIM}\big(B_1, B'_1\big). \tag{20}$$

(4) Binarization function with a threshold value equal to 0.40 may be executed in order to get binary result of authenticity detection. The value of 0.40 was chosen during the numerical experiments as it enables to achieve best results with least false positives:

$$\mathrm{rez}_{\mathrm{auth}} = \mathrm{threshold}(\mathrm{rez}_{\mathrm{sim}}, 0.40). \tag{21}$$

As it was already mentioned, in case of any uncertainty human opinion can be easily integrated as both B_1' and B_1 represent human-understandable images.

3.2.3. *Determining Tamper Localization*

Image tamper localization is a separate process based on different kind of mathematical engine than image authentication. This enables tamper localization to be executed independently of image authentication. Immunity against oracle attack is ensured via such architecture.

Authentication establishment procedure determines authenticity of the image in question. But even if the image in question has been determined as non-authentic, some parts of the image still may be trusted therefore it is important to determine what parts of the image have been tampered with. For this purpose tamper localization is applied.

Tamper localization process has been designed to detect tampered regions with resolution of up to one pixel – at the same time allowing some general image processing operations, such as blurring or rotation. If we have image in question $f'(x, y)$ then:

(1) At first, tamper localization map $f_K(x, y)$ and column vector C_1 are extracted from digital signature. K is initialized to a known value, if private key function was used, localization map is inverse permutated.
(2) Image in question $f'(x, y)$ is converted into lossless log-polar coordinates.
(3) The image $f'(x, y)$ is then transformed into MPOF domain $f'_{\mathrm{MPOF}}(x, y)$, then converted back to Cartesian coordinates in order to make tamper localization map understandable for human.
(4) Tamper localization signature f_K is extracted from global signature of the image.
(5) Extracted signature is permutated according to a secret key, if protection was used:

$$f_{\mathrm{sign}}(x, y) = K^{-1}\big(f_K(x, y)\big). \tag{22}$$

(6) Let A^1 be a matrix as defined in (11).
(7) Integer b is maximized with the respect to the inequality (12).
(8) Transformation matrix A is generated as in (13).
(9) Inverse discrete Fourier transformation is calculated and transfer into MPOF domain is finalized:

$$f_{\mathrm{MPOF}}(x, y) = \mathcal{F}^{-1}\big\{A(p, q)\mathrm{e}^{i\varphi_{f_{\mathrm{sign}}(p,q)}}\big\}(x, y). \tag{23}$$

(10) Resulting image $f_{\mathrm{MPOF}}(x, y)$ is converted back to Cartesian coordinates in order to make tamper localization map understandable for human vision.

(11) Difference map between $f_{\mathrm{MPOF}}(x, y)$ and $f'_{\mathrm{MPOF}}(x, y)$ is generated. This difference map represents tampered regions in the image in question.

The numerical experiments on image authentication are presented in following section.

3.3. *Advantages of the Proposed Method*

The method presented above has the following advantages. First advantage is usage of digital signature scheme. There are applications where keeping accurate and not modified original data is important, like medical or military images. In such cases digital signature application that ensures integrity of original data and provides required protection is the best solution. Additional feature – robustness to steganalysis attacks. Contrary to watermark, digital signature methods introduce no artificial data in to the original image. This disables steganalysis methods. Ability for the casual human himself/herself to verify image authentication visually, in intuitive way, without going into mathematical formulas and equations is also an advantage, especially as we still have mathematical evaluation available as the basis of the same method. Algorithmic separation of authentication and tamper localization procedures makes image authentication establishment less expensive and more effective than usual algorithms where tamper detection is also used to determine authenticity of the image. Oracle attack is also disabled because of such separation of authentication and tamper localization.

Ability to withstand general image processing – blurring, sharpening – both for authentication and for tamper localization is novelty of the proposed method. General operations used to increase graphical value of the image without malicious changes to the essence of the image are quite common in our digital world. Naturally, methods for image authentication and tamper localization establishment should be able to adapt to the requirements of the real world, should not identify such changes as a suspected ones. Robustness to the authentication establishment and tamper localization methods is of different operational level. Tamper localization is semi-fragile – robust only to limited set of image processing methods – blurring, sharpening. Authentication, on the other hand, is designed to fail only when essence of the image is completely changed. Construction of the method, making it both robust in general authentication and semi-fragile in tamper localization presents extraordinary challenges. The proposed method successfully combines the best characteristics of image authentication and tamper localization algorithms.

4. Numerical Experiments

During localized attacks some small artificial element is added into the picture – the picture in question is modified in some small region. Efficiency of image authentication and precision of tamper localization are evaluated in such case.

Simple added text “VGTU, Lithuania” – imitates artificial copyright sign. This represents real-world problem when graphical information is presented with false credentials.

Size of the letters was chosen to be normal – not too big, not too small. One label is smaller than the other.

Added picture of crow – represents illegal logo modifications. Size of the crow is variable, amount of the crows is different – to demonstrate ability of the method to adapt both to different size of the attack and to different amount of attack zones. As we see, independently of size of the crow or of the number of the crows, the method correctly identifies tampered regions with the resolution of up to one separate pixel. It should be noticed that tamper map is not binary map, but value map, we see not only damaged pixels but also we can evaluate how much damage the pixel has received.

Combined attacks represent the most interesting and challenging class of attacks. They combine malicious attacks with general image processing operations – thus the name – combined attack. At first a real attack is performed and then the image is a bit blurred or sharpened with the objective to deceive image authenticating and tamper localization procedures.

The objective of this section is to show precision and effectiveness of the proposed method, capable to correctly identify tampered regions despite influence of general image processing operations.

Figure 1 shows combined attacks – some localized attack plus general image processing operation – sharpening or blurring. Images used are standard – Boat, Goldhill, Cameraman.

Global attacks represent subsection of general image processing operations – such as blurring, sharpening, rotation, JPEG compression. These attacks can be considered as "good attacks" – they do not change and sometimes even expand essence of the image. Although it remains for open discussion whether these image processing operations have positive or negative effect on quality of the image, it is not difficult to observe that we are discussing about *quality*, not about *content* modification.

In order to compare the proposed method with popular watermarking approaches, we consider the standard Lena image in the proposed method and in watermark based solution implementation (Bausys and Kriukovas, 2009). Figure 2 shows three images – Lena after attack ("LNK" + "Lithuania" + blur) on the left. In the middle we see tamper localization results using watermark based approach. When one knows the damage introduced, it is possible to indentify tampered pixels. But when the tampered pixels have to be identified without initial knowledge, vast amount of false positives, introduced by blur step, make this task almost impossible. The right-most picture shows the results of the proposed method. As we see, there are no false positives from blur operation, only successfully identified tampered locations of "LNK" and "Lithuania". This confirms having tamper localization method able to locate tampered pixels after general blur/sharpen operations.

As it is shown in Fig. 3, as blur intensity increases (blur0 – no blur, blur1 – one blur operation, blur2 – two sequential blur operations, blur3 – three sequential blur operations), size of detected tampered region increases as well. We see that blurring introduces some minor background noise in tamper localization. In tamper localization map images we can see that this noise does not disturb tamper location identification, i.e., ratio of false positives increases, but ratio of false negatives does not.

Combination of text and image

Tamper localization map

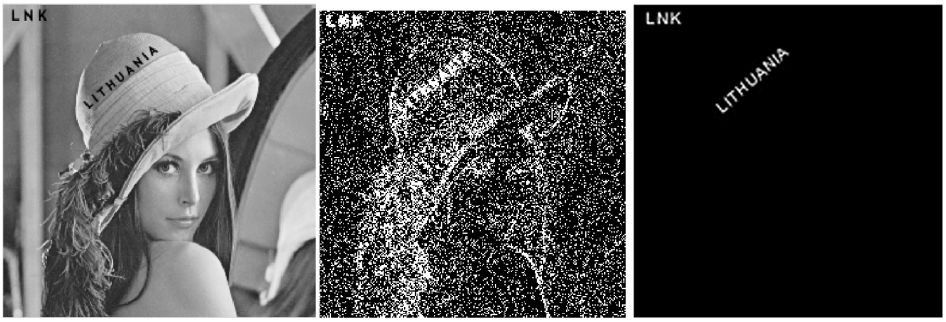
Combination of text and image, blur

Tamper localization map

Combination of text and image, sharpen

Tamper localization map

Fig. 1. Tamper localization, general results.



Attacked image, sharpened | Tamper localization map, watermarking approach | Tamper localization map, proposed method

Fig. 2. Tamper localization, comparison with watermarking based method.

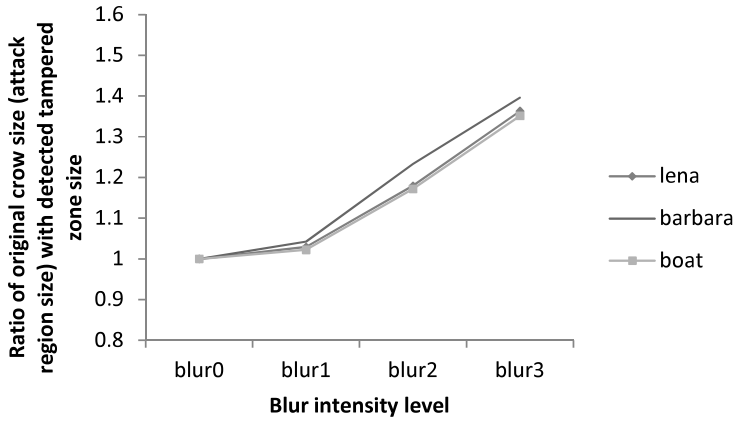


Fig. 3. Size of damaged region detection dependency on blur intensity, average case.

5. Conclusions

In the paper we address the problem of robust image authentication together with semi-fragile pixel-wise tamper localization. A new method for the solution of the problem is proposed. The method is invariant to content-preserving image modifications – blurring, sharpening – and presents pixel-wise sensitivity to content-changing modifications. A new modified phase only filter transformation is proposed. The transformation is loosely based on the phase of Fourier transform and ensures invariance to blur/sharpen image processing operations while retaining spatial reference information. A new method for semi-fragile pixel-wise tamper localization is proposed. The method is based on the new modified phase only filter transformation. This gives the required robustness against general image processing operations – blurring, sharpening – and retains pixel-wise fragility to other processing – like object addition or removal – intact, resulting in semi-fragility against general image processing. A robust image authentication method is developed. The method features both binary and percentage measures for authenticity

establishment as well as novel feature – optional human opinion integration. A complete digital signature based method is developed. The method integrates both robust authentication and semi-fragile pixel-wise tamper localization. Also, the method provides protection for all bits of the pixel, contrary to most pixel-wise watermarking methods. Separate image authentication and tamper localization mechanisms are specifically enforced in order to prevent general algorithmic attacks, such as oracle attack. It is proved that such separation is required to stop an attack were authenticator itself can be used to attack the protected image. Digital signature approach is introduced in order to rupture attacks based on steganalysis as contrary to watermarking approach nothing is embedded into the protected picture. Additional advantage of future upgrades is gained – no image re-watermarking is required. Performance gains were also addressed in the proposed method. Final size of the signature is less than 10% of initial image; tamper localization procedures are not executed if authentication process confirms 100% authenticity; only simple and effective mathematical operations are used.

References

Bartolini, F., Tefas, A., Barni, M., Pitas, I. (2001). Image authentication techniques for surveillance applications. *Proceedings IEEE*, 89(10), 1403–1418.

Baušys, R., Kriukovas, A. (2009). Blur resistant image authentication method with pixel-wise tamper localization. *Journal of Electronics and Electrical Engineering*, 3(91), 35–38.

Dittmann, J., Steinmetz, A., Steinmetz, R. (1999). Content-based digital signature for motion pictures authentication and content-fragile watermarking. In: *IEEE International Conference on Multimedia Computing and Systems*, pp. 209–213.

Eggers, J., Girod, B. (2001). Blind watermarking applied to image authentication. In: *Proceedings of IEEE International Conference on Audio, Speech and Signal Processing*, 3, pp. 1977–1980.

Ganesan, K., Guptha, T.K. (2010). Multiple binary images watermarking in spatial and frequency domains. *An International Journal on Signal and Image Processing*, 1(2).

Kazakeviciute, G., Januskevicius, E., Rosenbaum, R., Schumann, H. (2005). Tamper-proof image watermarking, based on existing public key infrastructure. *Informatica*, 16(1), 75–92.

Kundur, D., Hatzinakos, D. (1999). Digital watermarking for telltale tamper proofing and authentication. In: *IEEE Proceedings in Special Issue on Identification and Protection of Multimedia Information*, pp. 1167–1180.

Li, C.-T., Lou, D.-C., Chen, T.-H. (2000). Image authentication and integrity verification via content-based watermarks and a public key cryptosystem. In: *IEEE International Conference on Image Processing*, pp. 694–697.

Lu, Z.-M., Wang, J.-X., Liu, B.-B. (2009). An improved lossless data hiding scheme based on image VQ-index residual value coding. *Journal of Systems and Software*, 82(6).

Meerwald, P., Uhl, A. (2001). A survey of wavelet-domain watermarking algorithms. In: *Proceedings of SPIE, Electronic Imaging, Security and Watermarking of Multimedia Contents III*, pp. 505–516.

Queluz, M.P. (1998). Towards robust, content based techniques for image authentication. In: *IEEE 2nd Workshop on Multimedia Signal Processing*, pp. 297–302.

Queluz, M.P. (1999). Content-based integrity protection of digital images. In: *SPIE Conference on Security and Watermarking of Multimedia Contents*, pp. 85–93.

Popovic, B.M., Bandjur, M.V., Raicevic, A.M. (2011). Robust fingerprint enhancement by directional filtering in fourier domain. *Journal of Electronics and Electrical Engineering*, 1(107).

Su, K., Kundur, D., Hatzinakos, D. (2001). A content-dependent spatially localized video watermarked for resistance to collusion and interpolation attacks. In: *Proceedings of IEEE International Conference on Image Processing (ICIP)*, 1, pp. 818–821.

Swanson, M.D., Zhu, B., Tewfik, A.H. (1997). Video data hiding for video-in-video and other applications. In: *Proceedings of SPIE Multimedia Storage and Archiving Systems*, 3(229), pp. 32–43.

Tefas, A., Pitas, I. (2000). Image authentication using chaotic mixing systems. *Proceedings on IEEE International Symposium Circuits and Systems*, 1, pp. 216–219.

Valantinas, J., Zumbakis, T. (2007). On the application of invariant image parameters to fractal encoding of bi-level images. *Informatica*, 18(3), 463–478.

Wang, J.-X., Lu, Z.-M. (2009). A path optional lossless data hiding scheme based on VQ joint neighboring coding. *An International Journal on Information Sciences*, 179(19).

Wu, C.-P., Kuo, C.-C. J. (2002). Comparison of two speech content authentication approaches. In: *Proceedings on SPIE Security and Watermarking of Multimedia*, Vol. 4, pp. 158–169.

Zhu, B. (1998). *Coding and Data Hiding for Multimedia*. PhD thesis. University of Minnesota.

Zhu, B., Swanson, M.D., Tewfik, A.H. (2004). When seeing isn't believing. *Signal Processing Magazine*, 21(2), 40–49.

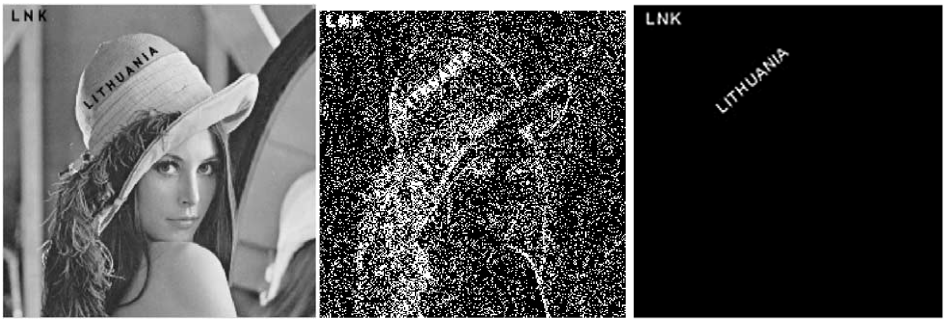
R.Baušys, prof. habil.dr., is full time professor, head of Graphical Systems Department, Vilnius Gediminas Technical University. Current research interests: intelligent GIS, multimedia security, medical image analysis, Lithuanian language animation.

A. Kriukovas was awarded the PhD degree on informatics engineering in the Department of Graphical Systems, Faculty of Fundamental Sciences, Vilnius Gediminas Technical University in 2010. He is currently working in Department of Graphical Systems, VGTU. His main research interests include image security, watermarking, image digital signature, Fourier transformation, wavelet transformations, superzoom, extended reality.

Bendrinėms ryškumo keitimo atakoms atsparus pikselių tikslumo atvaizdų pažeidimų lokalizavimo metodas

Romualdas BAUŠYS, Artūras KRIUKOVAS

Straipsnyje analizuojamas atvaizdo blukinimo ar ryškinimo atakoms atsparus autentikavimo metodas su pusiau jautriu paskirų pikselių pažeidimų lokalizavimu. Pasiūlyta nauja vaizdo transformacija, suteikianti invariantiškumą blukinimui ar ryškinimui. Pasiūlytas naujas atvaizdo autentiškumo vertinimo metodas, suteikiantis tiek binarinį, tiek procentinį vertinimą – taip pat integruojantis žmogaus nuomonę. Pažeidimų lokalizacija suteikia apsaugą visiems pikselių bitams. Atvaizdo parašo dydis yra mažesnis nei 10% originalaus vaizdo dydžio.



Attacked image, sharpened

Tamper localization map, watermarking approach

Tamper localization map, proposed method

Fig. 2. Tamper localization, comparison with watermarking based method.

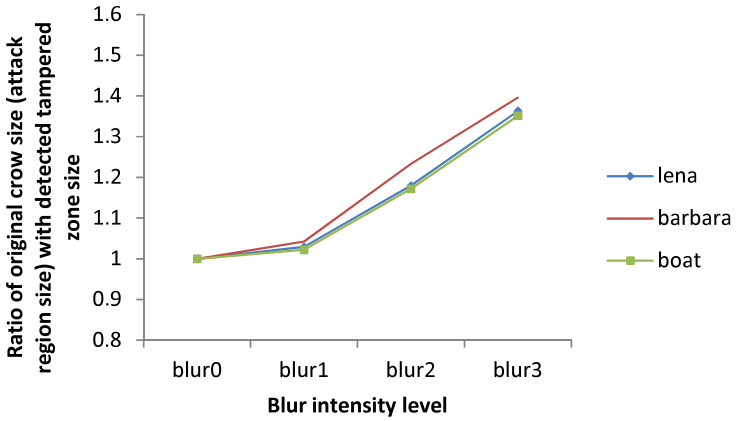


Fig. 3. Size of damaged region detection dependency on blur intensity, average case.

5. Conclusions

In the paper we address the problem of robust image authentication together with semi-fragile pixel-wise tamper localization. A new method for the solution of the problem is proposed. The method is invariant to content-preserving image modifications – blurring, sharpening – and presents pixel-wise sensitivity to content-changing modifications. A new modified phase only filter transformation is proposed. The transformation is loosely based on the phase of Fourier transform and ensures invariance to blur/sharpen image processing operations while retaining spatial reference information. A new method for semi-fragile pixel-wise tamper localization is proposed. The method is based on the new modified phase only filter transformation. This gives the required robustness against general image processing operations – blurring, sharpening – and retains pixel-wise fragility to other processing – like object addition or removal – intact, resulting in semi-fragility against general image processing. A robust image authentication method is developed. The method features both binary and percentage measures for authenticity