ELECTRONICS AND ELECTRICAL ENGINEERING
ISSN 1392 – 1215 *2009. No. 3(91)*
ELEKTRONIKA IR ELEKTROTECHNIKA

ELECTRONICS
T170
ELEKTRONIKA

Blur Resistant Image Authentication Method with Pixel-wise Tamper Localization

R. Baušys, A. Kriukovas
Department of Graphical Systems, Vilnius Gediminas Technical University,
Saulėtekio al. 11, Vilnius, Lithuania; phone: +370 5 2744848; email: romas@fm.vgtu.lt

Introduction

Over the last decade we faced expansion of digital imagining technologies. This expansion enabled effortless modification of digital images – leading us to face new threats and challenges on image authentication.

Watermarking methods provide solution to global image authentication – at a price of introducing additional changes to the original image. Limited ability to remove these additional changes appear in lossless watermarking methods. But if any image processing has occurred, changes introduced by lossless watermarking usually become irrevocable [1, 2].

Digital signature methods keep the original image intact. An important feature for special applications, i.e. medical. However traditional binary image authentication is not always enough. In order to identify tampered and trusted regions of the image, tamper localization is required. Pixel-wise resolution is preferred in order to exactly pin-point modified pixels. Acceptance of standard image processing is also desirable.

There are very few papers on digital signature tamper localization with the respect to invariance against blur/sharpen processing. Block-based tamper localization method is presented in [3]. The paper mentions being the first hashing method that can localize image tampering. Another method with pixel-wise tamper localization is presented in [4].

Resistance to blurring/sharpening operations is not directly mentioned in [3]. Our analysis does not confirm the method supports such image processing operations.

Partial resistance against small-intensity blur/sharpen operations may be enabled in restore capable digital signature methods, although this resistance usually achieved as "side-effect" [4, 5].

Image hashing methods [6] based on extracted features – edges, feature points, image moments – show quite good robustness against blurring/sharpening. However, pixel-wise tamper localization based on these methods is not possible.

More works on pixel-wise tamper localization are in watermarking section. Illegal watermark structure modification or restoration of original image [1] allows for pixel-wise tamper localization, although global nature of blur/sharpen operations makes it hardly compatible with watermarking methods. Watermarking methods capable at least partially resist affirmative image modifications, such as blurring, are based on global image structure and loose pixel-wise tamper localization resolution.

Our goal is to present digital signature method with pixel-wise tamper localization ability, capable to resist blur/sharpen procedures, as usually image blurring or sharpening does not influence essence of the image. A lot of watermarking/digital signature methods fail to implement pixel-wise resolution against limited blurring or sharpening operations considering their effect on binary matrices of the image.

In this paper we present blur/sharpen resistant method for image authentication and pixel-wise tamper localization. The method is implemented on a digital signature basis as we see this basis more advantageous over watermark basis [4]. If the same technique would be applied on watermark, it data structures may not survive malicious modifications and allowable general image processing.

Theoretical foundations

Our objective was to create a digital signature method capable to withstand some standard image processing modifications (like blurring and sharpening) and at the same time remain sensitive to malicious image attacks with pixel-wise tamper localization. In other words our method should be able to locate tampered regions with pixel-wise resolution even if the whole image before or after the attack was additionally blurred or sharpened.

In order to achieve our goal we designed a special modified phase only filter transformation (MPOF) invariant to image blurring/sharpening [7].

In digital image processing 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:

$$g(x) = (f * h)(x), \qquad (1)$$

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:

$$G(u) = F(u) \cdot H(u), \quad (2)$$

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 (2), resulting in:

$$|G(u)| = |F(u)| \cdot |H(u)|, \quad (3)$$

$$\angle G(u) = \angle F(u) + \angle H(u), \quad (4)$$

where (3) and (4) 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:

$$\angle H(u) = \begin{cases} 0, & if\ H(u) \geq 0, \\ \pi, & if\ H(u) < 0. \end{cases} \quad (5)$$

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

This property became one of key steps in our new modified phase only filter transformation (MPOF) that provides semi-invariance over standard blur/sharpen image processing operations.

Let *f(p,q)*, $0 \leq p,q \leq N-1$ be an image in non-negative Z^2 domain. Transformation MPOF for the image *f(p,q)* is defined as following:

1) 2D DFT of *f(p,q)* is calculated:

$$F_I(l,m) = DFT\{f(p,q)\}(l,m) = \sum_{p=0}^{N-1}\sum_{q=0}^{N-1} f(p,q) e^{-j\frac{2\pi}{N}(pl+qm)}. \quad (6)$$

2) Let A^1 be a matrix:

$$A^1(p,q) = 1; \quad 0 \leq p,q \leq N-1. \quad (7)$$

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

$$IDFT\{bA^1(l,m) e^{j\Theta f(l,m)}\} < 256, \quad (8)$$

where $\Theta_f(l,m)$ is phase of the signal calculated by

$$\Theta_X(w) = \tan^{-1}\left(\frac{\mathrm{Im}\{X(w)\}}{\mathrm{Re}\{X(w)\}}\right). \quad (9)$$

4) Transformation matrix *A* is generated:

$$A(p,q) = \begin{cases} bA^1 + 1, & \text{when q is even,} \\ bA^1 - 1, & \text{when q is odd.} \end{cases} \quad (10)$$

5) Inverse DFT is calculated:

$$f^d(p,q) = IDFT\{A(l,m) e^{j\Theta f(l,m)}\}(p,q). \quad (11)$$

Resulting image $f^d(p,q)$ is semi-invariable to blurring/sharpening operations on the original image *f(p,q)*.

Finally we propose the following digital signature generation method, capable to withstand common image processing modifications such as blurring or sharpening and providing pixel-wise tamper localization:

1) 5th LL level wavelet decomposition of the image *f(p,q)* is calculated – LL(*f(p,q)*).
2) Transformation MPOF for the image *f(p,q)* is calculated: T(*f(p,q)*) = MPOF(*f(p,q)*)
3) Transformed image T(*f(p,q)*) is permutated into T`(*f(p,q)*) according to a secret key K, in order to enable private key based image authentication and tamper localization process.
4) Resulting image T`(*f(p,q)*) is compressed with JPEG in order to achieve efficient size of the signature.
5) LL(*f(p,q)*) and T`(*f(p,q)*) are combined into one digital signature of the image *f(p,q)*.

We would like to notice that image authentication is separated from tamper localization. This structural separation is required to enable protection scheme against oracle attack [8]. Oracle attack makes extensive usage of image authentication engine changing the image pixels one-by-one until the modified image passes image authenticator. This attack is the most efficient when image authentication is based only on tamper localization function. In our case due to the fact that authentication function is implemented by different engine than tamper localization, oracle attack is disabled.

Wavelet LL decomposition was chosen to enable human opinion integration in authenticity establishment process as a backup option. Main technology used to establish authentication of the image in question can be PSNR or any other image comparison and evaluation metric [9]. 5th decomposition level was chosen as an optimal between acceptable quality and small size of the resulting decomposed picture.

Authentication of potentially modified image in question $f_m(p,q)$ is determined by 5th level wavelet decomposition phase:

1) Image in question $f_m(p,q)$ is decomposed into 5th level LL wavelet decomposition LL($f_m(p,q)$).
2) Original LL(*f(p,q)*) is extracted from the digital signature.
3) LL(*f(p,q)*) and LL($f_m(p,q)$) are compared, authentication of the image in question is established.

Tamper localization of the image in question is determined by the following procedure:

1) Transformation MPOF is calculated for the image in question: T($f_m(p,q)$) = MPOF($f_m(p,q)$).
2) Transformed image T($f_m(p,q)$) is permutated into T`($f_m(p,q)$) according to a secret key K.
3) Original transformed image T($f(p,q)$) is extracted from the digital signature.
4) T($f_m(p,q)$) is compared with T`($f_m(p,q)$) – this step results in a pixel-wise damage map.

Effectiveness of this procedure is studied in the following section.

Numerical experiments

Numerical experiments we performed had to establish some specific properties of the proposed technique.

First of all we analyzed the size of the signature as a function of MPOF transformation. We have achieved 70-90% compression rate without significant loss of information. Such effectiveness is implemented by applying JPEG compression algorithm to specially constructed image structures – this is best shown on image histograms. In Figure 1 histogram of standard image is represented. In Figure 2 histogram of transformed image MPOF($f(p,q)$) is presented. As we see, Figure 2 resembles half of Gaussian distribution centered on zero with most values being close at zero. This artificial structure is the key to high performance JPEG compression.

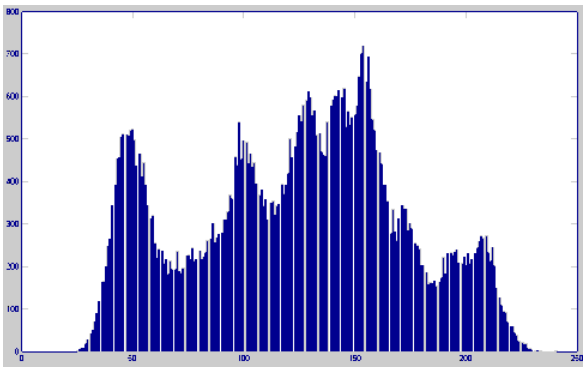

Fig. 1. Histogram of standard Lena image

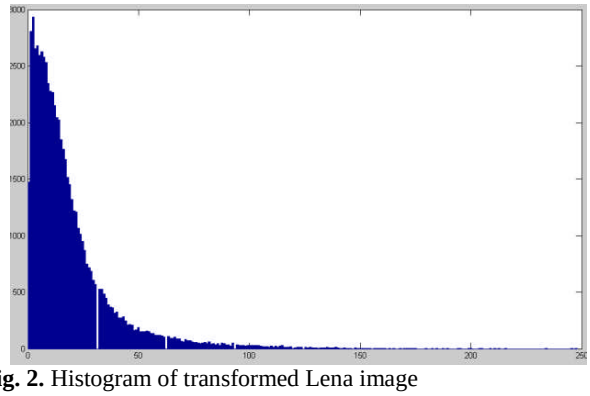

Fig. 2. Histogram of transformed Lena image

Secondly we evaluated how effectiveness of depends on parameter *b*. In Figure 3 curve of signature size at various *b* values is displayed. We see that signature size increases as *b* increases as well.

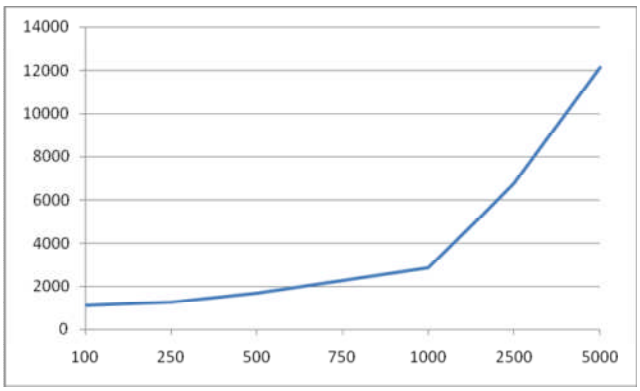

Fig. 3. Signature size (Y axis, bytes) dependency on parameter *b* value (X axis)

We also studied effectiveness of tamper localization on standard image cameraman. Figure 4 presents attacked cameraman – copyright label in right top angle was added, small image of crow was also added, as an object of photography. Tamper localization results are shown in figure 5. As we see, both modifications were detected correctly. Size of the signature is 16052 bytes, size of the initial image is 66132 bytes.

Fig. 4. Attacked image

Fig. 5. Tamper localization results

Finally we tested method with standard image Barbara. Fig. 6 shows attacked and additionally blurred (two iterations, standard Photoshop blurring) Barbara image. Size of the signature is 79309 bytes, size of the whole image 277360 bytes.

Fig. 6. Image of Barbara - attacked and blurred

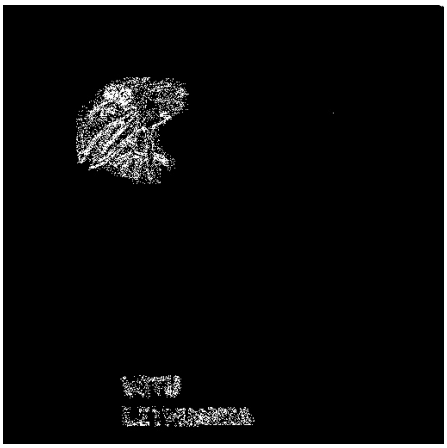

Fig. 7. Results of tamper localization

Results of tamper localization are presented in Figure 8. Please notice effectiveness of the method – intensive blurring does not affect the results of tamper localization. Despite of quite heavy blurring resulting in big pixel changes on global scale, the method is able to identify modifications and accuratelly locate tampered regions. Some noice on the tamper localizations appears due to high intensity blurring.

Conclusions

In this paper a new digital signature based method for image authentication is presented. Novelties of proposed authentication technique include pixel-wise tamper localization with invariance to image enhancement modifications such as blurring or sharpening. Separated image authentication and tamper localization processes allows to ensure robustness against algorithmic attacks, such as oracle attack.

References

1. **Baušys R., Kriukovas A.** Reversible watermarking scheme for image authentication in feequency domain // 48th International Symposium ELMAR-2006 focused on Multimedia Signal Processing and Communications. – 2006 – P. 53–56.
2. **Vyšniauskas V.** Subpixel edge reconstruction using aliases pixel brightness // Electronics and Electrical Engineering. – 2008. – No. 8(88). – P. 43–46.
3. **Sun Q., Roy S.** Robust hash for detecting and localizing image tampering // IEEE International Conference on Image Processing. – 2007. – Vol. 6. – P. 117–120.
4. **Baušys R., Kriukovas A.** A new scheme for image authentication framework // Information Technology and Control. – 2008. – Vol. 37, No. 4. – P. 294–300.
5. **Boncelet C.** Image authentication and tamper proofing for noisy channels // IEEE Image Processing. – 2006. – P. 1985–1988.
6. **Sun Q., Roy S., Kalker T.** Performance analysis of locality preserving image hash // IEEE International Conference on Image Processing. – 2008. – P. 1268–1271.
7. **Horner J. L., Gianino P. D.** Phase-only matched filtering // Applied Optics. – 1984. – Vol. 23. – P. 812–816.
8. **Baušys R., Kriukovas A.** Vandens ženklų taikymas vaizdų autentiškumo užtikrinimui // Informacinės technologijos 2005: aktualijos ir perspektyvos. IV mokslinės praktinės konferencijos pranešimų medžiaga. – 2005. – P. 17–21.
9. **Sheikh H. R., Bovik A. C.** Image information and visual quality // IEEE Transactions on Image Processing. – 2006. – Vol. 15, No. 2. – P. 430–444.

Received 2008 12 14

R. Baušys, A. Kriukovas. Blur Resistant Image Authentication Method with Pixel-wise Tamper Localization // Electronics and Electrical Engineering. – Kaunas: Technologija, 2009. – No. 3(91). – P. 35–38.

A new digital signature based method for image authentication and pixel-wise tamper localization is proposed. The proposed method is resistant to image content preserving enhancement operations such as blurring or sharpening. Authentication function is implemented separately from tamper localization both to increase processing speed and to disable algorithmic oracle attack. Ill. 7, bibl. 9 (in English; summaries in English, Russian and Lithuanian).

Р. Баушис, А. Крюковас. Использование цифровой подписи для аутентификации изображениях // Электроника и электротехника. – Каунас: Технология, 2009. – № 3(91). – С. 35–38.

Предлагается метод цифровой подписи для удостоверения подлинности изображения и локализации изменений до отдельного пикселя. Предлагаемый метод является устойчивым при изменениях, не меняющих суть изображения, таких как увеличение или уменьшение яркости или туманности. Функция удостоверения подлинности реализована отдельно от функций локализации изменений, что ускоряет анализ и позволяет избежать алгоритмической атаки оракула. Ил. 7, библ. 9 (на английском языке; рефераты на английском, русском и литовском яз).

R. Baušys, A. Kriukovas. Atvaizdo autentiškumo tikrinimo metodas, leidžiantis lokalizuoti atvaizdo pažeidimus vieno pikselio tikslumu nepriklausomai nuo ryškumo // Elektronika ir elektrotechnika. – Kaunas: Technologija, 2009. – Nr. 3(91). – P. 35–38.

Aprašomas naujas skaitmeninio parašo metodas, skirtas atvaizdo autentiškumui patikrinti ir potencialiems vaizdo pažeidimams lokalizuoti vieno pikselio tikslumu. Siūlomas metodas yra atsparus atvaizdo esmės neiškraipantiems pakeitimams, tokiems kaip ryškumo ar miglotumo didinimas ar mažinimas. Autentiškumo funkcija sukurta nepriklausomai nuo pažeidimų lokalizavimo, siekiant padidinti analizės greitį ir išvengti algoritminės orakulo atakos. Il. 8, bibl. 9 (anglų kalba, santraukos anglų, rusų ir lietuvių k.).

DOI: 10.5755/j02.eie.10304