GAUSSIAN SCALE-SPACE FEATURES FOR SEMI-FRAGILE IMAGE AUTHENTICATION

Mathias Schlauweg and Erika Müller

Institute of Communications Engineering,
Faculty of Computer Science and Electrical Engineering, University of Rostock,
Rostock 18119, Germany

ABSTRACT

In this paper, we propose a new robust image hashing approach to be used for semi-fragile image authentication. We use a texture-based feature, the so-called gray-level blob in Gaussian scale-space, which is invariant to scaling, rotation, and translation. It is associated with the image content and thus independent of image geometry. Furthermore, we show that our new approach is robust against a variety of signal processing operations, such as lossy compression, contrast and luminance enhancement, blurring, sharpening as well as noise adding.

Index Terms — Digital watermarking, Gaussian scale-space, texture-based feature points, RST-invariant

1. INTRODUCTION

Today's rapid evolution of multimedia technology and the progress of computer networks along with the development of the Internet bring many advantages in the creation and distribution of image content. But with the ability of easy copying, transmitting and editing digital images the need for image content protection increases. Digital images can be modified or forged by a wide variety of available manipulation software, and hence it is rather difficult to tell if a picture is the original one.

The integrity of a digital image is important in fields such as forensics, medical imaging and military or industrial photography. For instance, courts make decisions affecting an individual's liberty based, in part, on images presented as evidence. The burden of proof of authenticity always lies with the person seeking to admit. He must provide other evidence to support this authenticity. Thus, it is important to maintain the integrity of images from capture to final use.

To prevent illegitimate tampering and fraudulent use of modified images authentication techniques were introduced. As known from the classical cryptography, to verify the exact data integrity, a signature may be generated from the source signal by the use of secure hash functions and encryption. A recipient decrypts the signature and matches it with the hash generated from the received signal. If even one bit of the signal has been modified, it will no longer match the signature, so any tampering can be detected. But this so-called fragile property is sometimes not practical when considering distribution of images. For instance, lossy compression has to be performed to reduce the amount of data or signal processing is applied to correct gamma, to denoise or to resample an image. These manipulations change the pixels but not the content and hence not the authenticity.

To tolerate certain kinds of signal processing semi-fragile authentication methods for digital images have been developed. The aim is to allow admissible manipulations such as JPEG compression, but to reject malicious manipulations that change the visual content. Commonly used techniques extract features representing the image content and re-embed these features as watermark information into host image data [1]–[7]. Some approaches involve image positions of edges, contours or zero-crossings in the spatial domain whose existence is proved during the verification process. Other methods are based on single coefficients or relationships between pairs of different coefficients in the transform domain (e.g., DCT, DWT, or DFT). Often, these methods are only robust against a very small set of non-malicious signal processing operations.

Our new image hashing approach uses texture elements (*Texel*) to describe the image content in a robust but also fragile and secure way. In this paper, we propose to use gray-level blobs in Gaussian scale-space as features for semi-fragile image authentication.

In Section 2, we describe approaches commonly used for hashing image content with the objective of image authentication. Afterwards, in section 3, we propose our new semi-fragile feature generation based on texture elements. Experimental results and analyses are given in section 4. We show that our new approach is not only robust against lossy compression, noise, blurring, sharpening, contrast and luminance enhancement but also geometric distortion as well as cropping and hence image printing/scanning. Finally, section 5 concludes the work.

2. FEATURES FOR IMAGE AUTHENTICATION

To describe images in a semi-fragile manner image hashing and authentication methods use robust feature points. Another possible approach is the use of coefficients in the

transform domain or relationships between pairs of different coefficients. The disadvantage of the latter one is robustness against only a small set of signal processing operations. Often, these approaches are either robust against lossy compression or geometric distortion. In contrast, feature points (image positions of edges, contours, etc.) are known to be robust against a wide range of operations.

Kutter *et al*. formulated some properties that a feature should have [8]. In addition to robustness against compression, multiplicative and additive noise, a suitable feature should withstand a wide range of geometrical transformations (rotation, translation, scaling, etc.). Further, it should be possible to detect the same (remaining) feature points at the same positions if the host image has been cropped.

We proposed a completely new feature to be used for image authentication. Based on the idea of Kutter *et al*., extended to Gaussian scale-space, our new feature turned out to be very robust against a wide range of signal processing operations as shown in what follows.

3. OUR FEATURE DETECTION

Our new feature, the gray-level blob, is a texture element that can be found in most natural images. It is a raise or decrease of gray pixel values similar to a 2D-Gaussian curve, detectable in the Gaussian scale-space by the scale-invariant detector proposed in [9]. Due to this scale-space approach the detector is theoretically scale-invariant.

To find gray-level blobs the image I_{orig} is filtered in Gaussian scale-space using so-called *LOG*-filter[1] masks (see Eq. (1)), where the scale σ_r is parameterized by the value $\sigma_r = \{\sigma_r \in \mathbb{R} : \sigma_{\min} \le \sigma_r \le \sigma_{\max}, r \in \mathbb{N} : r \le R, R \in \mathbb{N}\}$. Because the kernel structure is similar to a Mexican sombrero, this filter is also known as *Mexican Hat*. The resulting, e.g., R = 16, matrices are normalized using Eq. (3) to get scale invariance for the magnitudes of the filtering result. The search space for σ_r has to be limited to $\sigma_{\min}$ and $\sigma_{\max}$ to get a trade-off between robustness and computational effort. During detection, these scales are normalized[2] depending on the image size to find the same blobs in a scaled image.

$$LOG(x,y,\sigma_r) = \left(\frac{x^2+y^2}{2\cdot\pi\cdot\sigma_r^{\,6}} - \frac{1}{\pi\cdot\sigma_r^{\,4}}\right)\cdot e^{-\frac{(x^2+y^2)}{2\cdot\sigma_r^2}} \qquad (1)$$

$$I_{LOG}(x,y,\sigma_r) = LOG(\sigma_r) * I_{orig}(x,y) \qquad (2)$$

$$I^*_{LOG}(x,y,\sigma_r) = \sigma_r^{\,2}\cdot I_{LOG}(x,y,\sigma_r) \qquad (3)$$

[1] The abbreviation *LOG* stands for Laplacian of the Gaussian, where the filter kernel is created by applying the Laplace operator to Gaussian functions, normalized to zero mean.

[2] $\bar{\sigma}_{\min} = \sigma_{\min}\cdot\max(X,Y)/512$ and $\bar{\sigma}_{\max} = \sigma_{\max}\cdot\max(X,Y)/512$, where X and Y are the image dimensions.

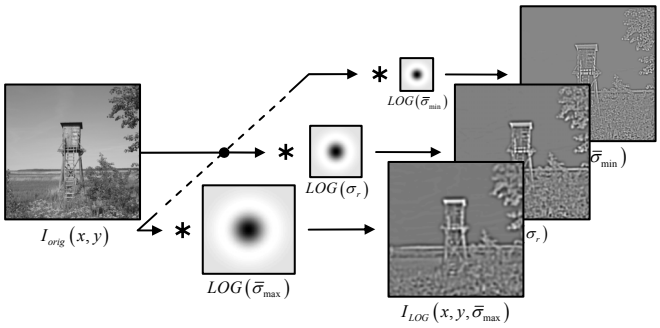

Fig. 1. Image filtered using *LOG*-filter with different scales.

Afterwards, from all R results at every pixel position (x,y) the optimal scale $\sigma_{opt}(x,y)$ is selected that yields the biggest magnitude value $I_{LOG_{opt}}(x,y)$:

$$\sigma_{opt}(x,y) = \arg\max_{\sigma_r} \left| I^*_{LOG}(x,y,\sigma_r) \right| \qquad (4)$$

The corresponding magnitude $I_{LOG_{opt}}(x,y)$ is stored for this position, too. Fig. 2 shows the results for an example image.

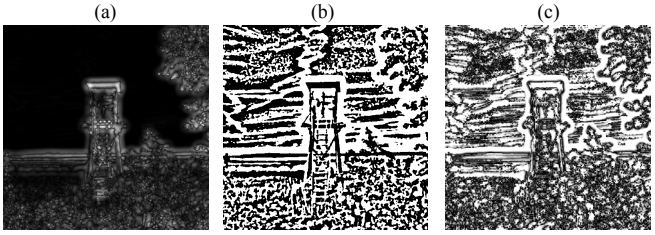

Fig. 2. Final selection result for the filtered image: (a) Magnitude of $I_{LOG_{opt}}$, (b) sign of $I_{LOG_{opt}}$, and (c) the scale σ_{opt}.

This blob detection is theoretically invariant to scaling, rotation, translation, and horizontal/vertical mirroring of the image. Further, except for (gray-value pixel range [0…255]) clipping, also changes of luminance should be accepted.

To also reach robustness against contrast changes we normalize the gray-value pixels I_{orig} prior to *LOG*-filtering using Eq. (5), where X and Y are the image dimensions.

$$I_{norm} = \frac{I_{orig}}{256}\left(\frac{1}{N}\sum_{x=1}^{X}\sum_{y=1}^{Y} I_{orig}(x,y)^2\right)^{1/2} \qquad (5)$$

After LOG-filtering, we choose the value $I_{LOG_{opt}}(x,y)$ with the biggest magnitude, which we call reference blob B_0. Now, in a successive selection process the algorithm looks for M more (largest) blobs, smaller than the reference blob. The list of chosen blobs is $B = \{B_i(x_i,y_i) : i = 1,2,...,M\}$, where (x_i,y_i) specifies a blob position. Thereby, around every single blob a circle is marked as "reserved region", where no other blob can be chosen from (see Fig. 3). The size of the circle is determined from the size of the corre-

sponding scale $\sigma_{opt}(x,y)$. In other words, the following inequality must be hold for any two blobs B_i and B_j within the list of chosen coordinates, where d_{ij} is the distance between both blobs:

$$\sigma_{opt}(x_i,y_i)+\sigma_{opt}(x_j,y_j)\le d_{ij} \tag{6}$$

$$d_{ij}=\sqrt{(x_i-x_j)^2+(y_i-y_j)^2} \tag{7}$$

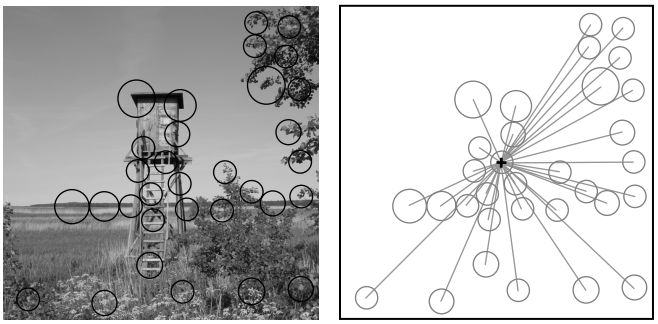

Fig. 3. Example image with M = 32 largest blobs selected, $\sigma_{\min}$ = 3, $\sigma_{\max}$ = 5.

Now, an authentication sequence is generated from the selected blob values that will be proved during image verification. For that, all M blob magnitudes are hashed and encrypted asymmetrically resulting in a digital signature. The hash process takes place in ascending order of distance to the reference point, marked by a cross in Fig. 3.

Prior to this, all magnitudes of the reference point as well as the other M–1 selected blobs have to be amplified by the value G_{base} to make sure that these points will be found again during signature verification.

To change the magnitude value of a blob a positive or negative *LOG*-mask, $LOG^*_{gain}(x,y,\sigma_{gain})$, is added to the blob in the pixel domain. This *LOG*-mask can be calculated using Eq. (8) and Eq. (9), where G_{diff} is the relative amplification (the difference between new and old *LOG*-magnitude). The scale for *LOG*-computation must be $\sigma_{gain}(x,y)=\sqrt{2}\cdot\sigma_{opt}(x,y)$.

$$LOG^*_{gain}(x,y,\sigma_{gain})=\frac{G_{diff}}{K}\cdot LOG_{gain}(x,y,\sigma_{gain}) \tag{8}$$

$$K=\sigma_{opt}{}^2\cdot\sum_{x=-x_{\max}}^{x_{\max}}\sum_{y=-y_{\max}}^{y_{\max}}LOG_{gain}(x,y)\cdot LOG_{opt}(x,y) \tag{9}$$

In Fig. 4, two cuttings around a distorted blob are visualized. It can be seen that the proposed blob feature has very high masking effect. Blobs can be understood as whole texture elements. Distortions are almost not perceivable.

As can be seen in the next section, blob amplifications smaller than $G_{base} = G_{diff} = 20$ are entirely sufficient to make our new feature detection robust against a variety of attacks.

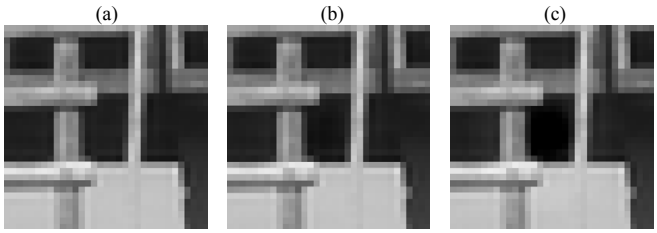

Fig. 4. Example image (3x zoomed view of the reference blob, marked by a cross in Fig. 3): (a) original, (b) blob manipulated by G_{diff} = 20, (c) blob manipulated by G_{diff} = 70.

4. EXPERIMENTAL RESULTS

To illustrate the properties of the proposed blob detection for a set of 60 different images we determined one largest blob (B_0) per image, applied a set of below shown attacks, and analyzed the effects. The scales are $\sigma_{\min}$ = 3, $\sigma_{\max}$ = 5.

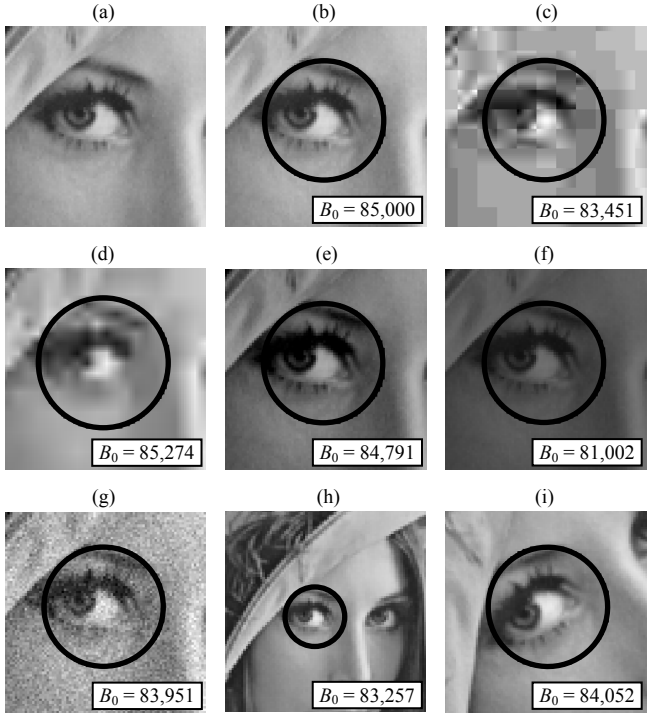

Fig. 5. Example image with largest blob: (a) original, (b) image with changed blob B_0 = 85. Detected largest blob after: (c) JPEG compression with QF = 5, (d) JPEG2000 compression using target rate r = 1/100, (e) luminance change, (f) contrast change, (g) additive Gaussian noise with σ = 10, (h) scaling by factor 0.5, (i) rotation by 36°.

Since the following figures show curves for different basic blob amplifications one can see that basic blob amplification is necessary. Otherwise, if G_{base} = 0 and if not the same blob is found during detection we obtain outlier results, where D is the attack induced distortion.

As can be seen in Fig. 6, the new blob detection is very robust against a variety of signal processing operations. Al-

ways, the same blobs are selected. The blob magnitude values only differ marginally. Blob amplifications smaller than $G_{base} = G_{diff} = 20$ are entirely sufficient to make our new feature detection robust. As illustrated in Fig. 4, this kind of distortion is not perceivable and hence a good compromise.

Since we quantize the magnitude values, apply hashing and encryption, a very useful authentication system is constructed. If the image is changed maliciously, the authentication sequence is disturbed, but otherwise, the sequence can always be retrieved and verified. The signature can be stored in a database or transmitted alongside the secured image in metadata or as a digital watermark.

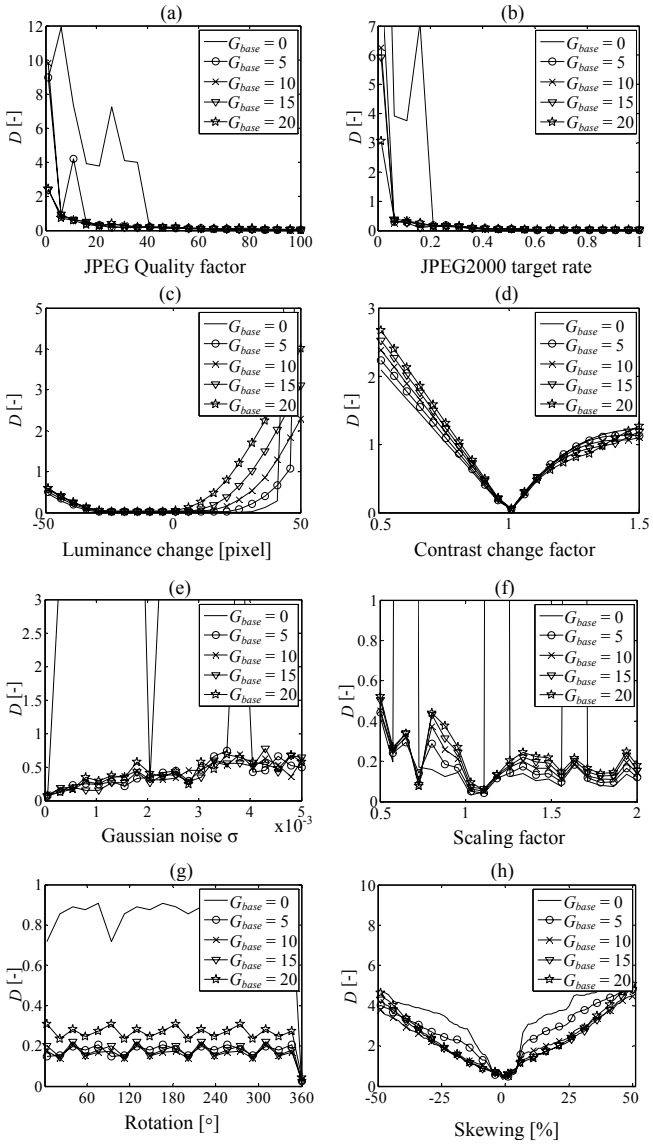

Fig. 6. Results of single blob robustness test: (a) JPEG compression, (b) JPEG2000 compression, (c) luminance change, (d) contrast change, (e) additive Gaussian noise, (f) scaling, (g) rotation, (h) horizontal image skewing.

Beyond image authentication, our new blob feature detection can also be employed for image indexing or duplicate finding, in the future.

5. CONCLUSION

This paper presents a new robust image content hashing approach for semi-fragile image authentication. Based on the so-called gray-level blob in Gaussian scale-space, a feature is proposed that is invariant to scaling, rotation-, and translation. It is associated with the image content and thus independent of image geometry. Furthermore, it is shown that our new approach is robust against a variety of signal processing operations, such as lossy compression, changes of luminance and contrast, blurring, sharpening as well as noise adding and hence image printing/scanning.

6. REFERENCES

[1] Ö. Ekici, B. Sankur, B. Coşkum, U. Nazi, and M. Akcay, "Comparative evaluation of semifragile watermarking algorithms," *Journal of Electronic Imaging*, 13, pp. 209-216, Jan. 2004.

[2] B. B. Zhu, M. D. Swanson, and A. H. Tewfik, "When seeing isn't believing," *IEEE Signal Processing Magazine*, 21, pp. 40-49, 2004.

[3] C. Rey and J.-L. Dugelay, "A Survey of Watermarking Algorithms for Image Authentication," *EURASIP Journal of Applied Signal Processing*, 6, pp. 613-621, March 2002.

[4] J. Fridrich, "Security of Fragile Authentication Watermarks with Localization," In *Proc. of SPIE*, 4675, pp. 691-700, Jan. 2002.

[5] M. Schlauweg, D. Pröfrock, and E. Müller, "JPEG2000-Based Secure Image Authentication," In *Proc. of Multimedia & Security Workshop*, Geneva, Switzerland, pp. 62-67, Sept. 2006.

[6] C. Y. Lin and S.-F. Chang, "Semi-fragile Watermarking for Authenticating JPEG Visual Content," In *Proc. of SPIE*, 3971, pp. 140-151, Jan. 2000.

[7] P. Meerwald, "Quantization Watermarking in the JPEG2000 Coding Pipeline," In *Proc. of Int. Conference on Communication and Multimedia Security*, pp. 69-79, May. 2001.

[8] M. Kutter, S. K. Bhattacharjee, and T. Ebrahimi, "Towards Second Generation Watermarking Schemes," In *Proc. of Int. Conference on Image Processing*, Kobe, Japan, pp. 320-323, Oct. 1999.

[9] T. Lindeberg, "Feature Detection with Automatic Scale Selection," *International Journal of Computer Vision*, 30 (2), pp. 77-116, Nov. 1998.