

Robust Zero Watermarking for Still and Similar Images Using a Learning Based Contour Detection

Shahryar Ehsaee and Mansour Jamzad^(✉)

Department of Computer Engineering,
Sharif University of Technology, Tehran, Iran
Ehsaee@ce.sharif.edu, jamzad@sharif.edu

Abstract. Digital watermarking is an efficacious technique to protect the copyright and ownership of digital information. Traditional image watermarking algorithms embed a logo in the image that reduces its visual quality. A new approach in watermarking called zero watermarking doesn't need to embed a logo in the image. In this algorithm we find a feature from the main image and combine it with a logo to obtain a key. This key is securely kept by a trusted authority. In this paper we show that we can increase the robustness of digital zero watermarking by a new counter detection method in comparison to Canny Edge detection and morphological dilatation that is mostly used by related works. Experimental results demonstrate that our proposed scheme is robust against common geometric and non-geometric attacks including blurring, JPEG compression, noise addition, Sharpening, scaling, rotation, and cropping. The main advantage of the proposed method is its ability to distinguishable key for images taken from the same scene with small angular rotation and minor displacement.

Keywords: Zero-watermarking · Copyright protection · Canny edge detection · Counters detection · Hierarchical Image Segmentation

1 Introduction

Digital watermarking is an efficient technique to protect the copyright and ownership of digital information. In the traditional methods of image watermarking, the Information of original image will be distorted by means of embedding the watermark in the image. Most watermarking methods, no matter in spatial domain or frequency domain, modify the original data while embedding the watermark.

A new watermarking approach named zero watermarking is proposed to watermark the image by not actually apply any modification in the image. Zero-watermarking is different from traditional digital image watermarking, which constructs a key (secret data) from the watermark and the information extracted from the image. This key is securely saved in a trusted authority.

In Zero-watermarking a set of features expressed as binary data are extracted from the image XOR ed with the watermark (logo) and a key is produced. This key is kept in a trusted Authority (TA). Zero-watermarking can successfully solve the conflict between invisibility and robustness. In this paper we first show that we can reach higher

robustness with the new learning based counter detection method then we compare the results with Canny edge detection method. Also we show that with this learning based counter detection method we can reach good results for the image taken from different point of views.

The aim of this work is to watermark these images so that their identity could be distinguishable although they are very similar. In this paper we first show that by using new learning based contour detection method we can reach higher robustness compared with traditional Canny edge detector mostly used by related works. And also we show that with this contour detection method we can reach good results for the image taken from different point of views from the same scene.

2 Previous Works

2.1 Canny Edge Detection Method

Canny edge detection method due its high performance and flexibility is used in many applications. Its high performance in zero-watermarking has been shown in several related works. In this work we show that the new Learning based detection method that will be explained in the following has a better performance compared with Canny.

Zero watermarking with Canny edge detection has two main steps:

- **Image Registration:**

We apply Canny edge detector to the image to obtain an edge image.

$$E_o = \text{CannyEdge} (o, [T_H, T_L], \sigma) \quad (1)$$

o is the main image and T_H and T_L are the low and high thresholds. σ is the standard derivation for Canny edge detector. It is explained in [1] to how to choose these values for results.

After applying Canny edge detection in input image morphological dilatation with radius disk of size 3 is used because the edges that are obtained from previous step are very thin.

$$E_{od} = \text{Dilation} (E_o, \text{disk}, 3). \quad (2)$$

Then the logo is permuted and XOR ed with the E_{od} and a key is produced. Figure 1 shows the steps:

- **Verification procedure:** In this step the logo is retrieved without using the main image.

We first get the key from the Trusted Authority. Canny edge detection is used to extracting the binary feature from the attacked image. A dilation operation with radius disk of size 3, as a structuring element is used to thicken the edge width of the binary feature. Then this image is XOR ed with the key taken from the trusted Authority(TA) to extract the logo. Finally, the verifier can visually verify the accuracy of retrieved logo and validate the ownership of the test image. Figure 2 shows the steps of verification procedure.

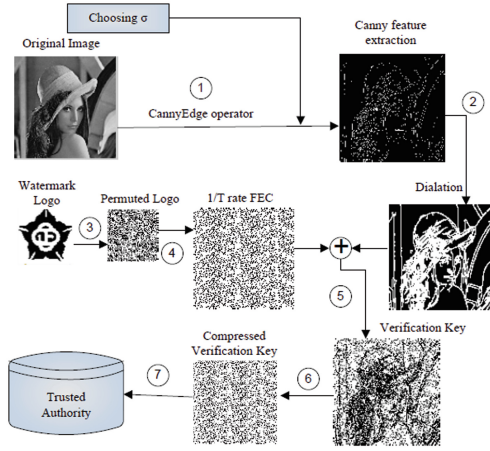


Fig. 1. Image registration steps using canny edge detector [1]

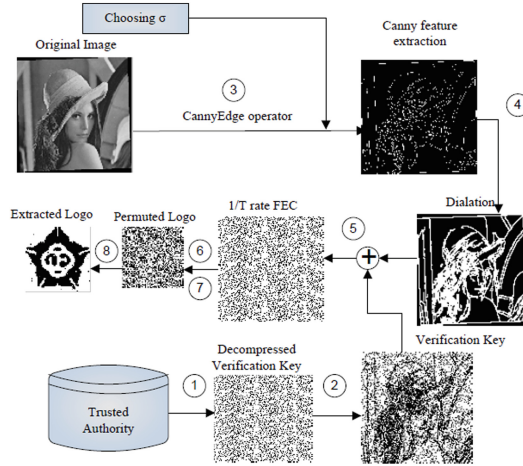


Fig. 2. Verification Procedure using canny edge detector [1]

3 Learning Based Contour Detection and Hierarchical Image Segmentation [2]

This is a unified approach to contour detection and image segmentation. Contributions include:

- A high performance contour detector, combining local and global image information.
- A method to transform any contour signal into a hierarchy of regions while preserving contour quality.

Early approaches to contour detection, through local measurements, aim at quantifying the presence of a boundary at a given image location. The Roberts, Sobel, and Prewitt operators detect edges by convolving a grayscale image with local derivative filters. Marr and Hildreth use zero crossings of the Laplacian of Gaussian operator. The Canny detector also models edges as sharp discontinuities in the brightness channel, adding non-maximum suppression and hysteresis thresholding steps [3].

3.1 Learning Based Contour Detection

As a starting point for contour detection, we consider the work of Martin et al. [4], who define a function $P_b(x, y, \Theta)$ that predicts the posterior probability of a boundary with orientation Θ at each image pixel (x, y) by measuring the difference in local image brightness, color, and texture channels. In this section, we review these cues, and then introduce the multi-scale version of the P_b detector. The basic building block of the P_b contour detector is the computation of an oriented gradient signal $G(x, y, \Theta)$ from an intensity image I . This computation proceeds by placing a circular disc at location (x, y) split into two half-discs by a diameter at angle Θ . For each half-disc, we histogram the intensity values of the pixels of I covered by it. The gradient magnitude G at location (x, y) is defined by the χ^2 distance between the two half-disc histograms g and h :

$$\chi^2(g, h) = \frac{1}{2} \sum \frac{(g(i) - h(i))^2}{(g(i) + h(i))} \quad (3)$$

We then apply second-order Savitzky-Golay filtering [5] to enhance local maxima and smooth out multiple detection peaks in the direction orthogonal to Θ . This is equivalent to fitting a cylindrical parabola, whose axis is orientated along direction Θ , to a local 2D window surrounding each pixel and replacing the response at the pixel with that estimated by the fitting a cylindrical parabola.

Figure 3 shows an example. This computation is motivated by the intuition that contours correspond to image discontinuities and a histograms provide a robust

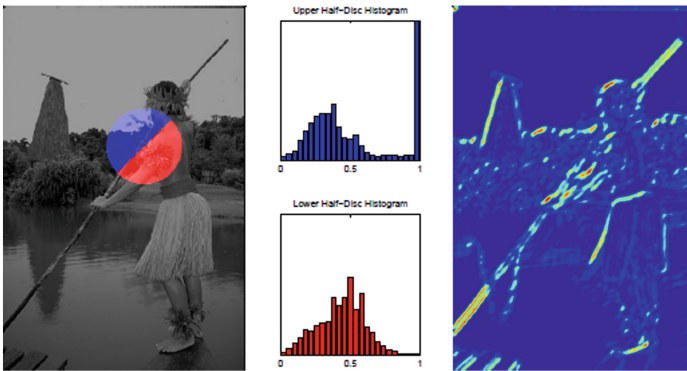


Fig. 3. Oriented gradients and their histograms

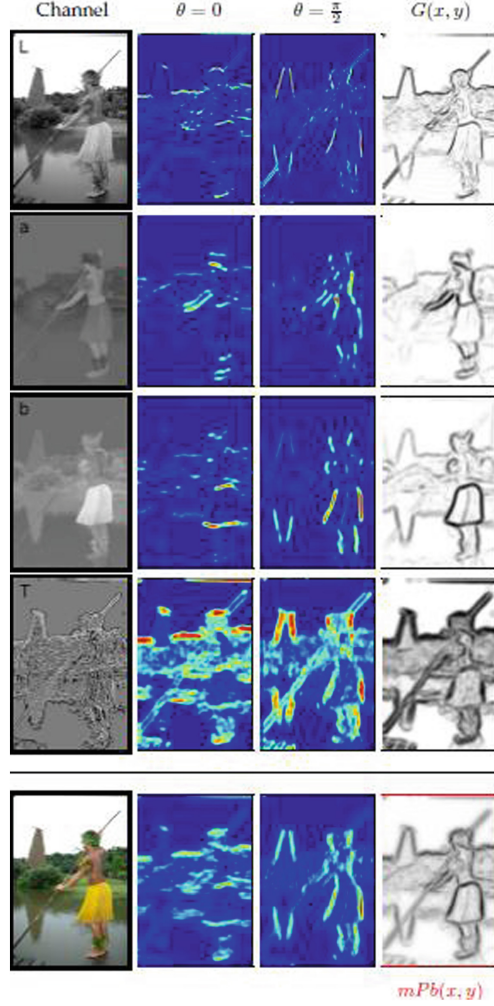


Fig. 4. Multiscale Pb. Left Column, Top to Bottom: The brightness and color a and b channels of Lab color space, Rows: Next to each channel, we display the oriented gradient of histograms

mechanism for modeling the content of an image region. A strong oriented gradient response means a pixel is likely to lie on the boundary between two distinct regions. The Pb detector combines the oriented gradient signals obtained from transforming an input image into four separate feature channels and processing each channel independently. The first three correspond to the channels of the CIE Lab colorspace, which we refer to as the brightness, color a, and color b channels. For grayscale images, the brightness channel is the image itself and no color channels are used. The fourth channel is a texture channel, which assigns each pixel a texton id. These assignments are computed by another filtering stage which occurs prior to the computation of the oriented gradient of histograms. This stage converts the input image to grayscale and

convolves it with the set of 17 Gaussian derivatives and center-surround filters. Each pixel is associated with a (17-dimensional) vector of responses, containing one entry for each filter. These vectors are then clustered using K-means. The cluster centers define a set of image-specific textons and each pixel is assigned an integer id in $[1; K]$ of the closest cluster center. Experiments show choosing $K = 32$ textons is sufficient. We next form an image where each pixel has an integer value in $[1, K]$, as determined by its texton id. An example can be seen in Fig. 4 (left column, fourth panel from top). On this image, we compute differences of histograms in oriented half-discs in the same manner as for the brightness and color channels. Obtaining $G(x, y, \Theta)$ for arbitrary input I is thus the core operation on which our local cues depend.

Figure 5 compares this new contour detection with other edge and contour detection methods.

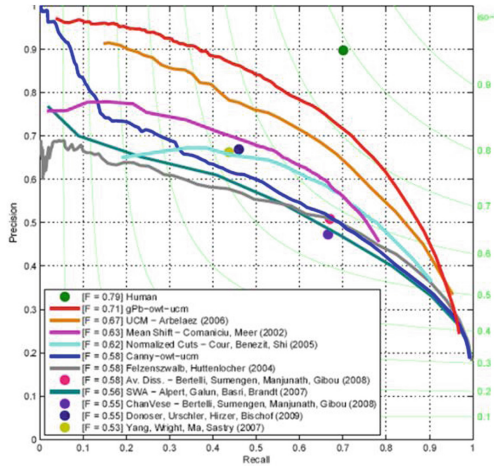


Fig. 5. Evaluation of segmentation algorithms on the BSDS300 Benchmark [2]

4 Results of Applying Canny Edge Detection and Learning Based Contour Detection Method

We should choose σ according to the complexity of the image to get the best result and we calculate the σ according to [1].

We use the same test image and binary logo as [6, 7] in our experiments for better comparison. Lena is of size 512×512 and the binary watermark logo is of size 64×64 as shown in Fig. 6.

We evaluate the quality between original image O and the attacked image \hat{O} by using PSNR. We use normalized cross correlation (NC) to evaluate the correctness of an extracted watermark (Tables 1 and 2).

As we can see the new learning based contour detection method increases the robustness especially in Quarter Cropping and rotation attack.



Fig. 6. (a) Test image Lena (b) Binary watermark logo

Table 1. PSNR and NC using Canny edge detector

	Rotation	Quarter Crop- ping	Sharpening	JPEG	Adding noise	Blurring
Attacked image						
PSNR(db)	11	10.23	23.1	30.9	17.2	33.1
Retrieved logo						
NC	.95	.83	.94	.99	.93	.97

Table 2. PSNR and NC using learning based contour detection

	Rotation	Quarter Crop- ping	Sharpening	JPEG	Adding noise	Blurring
Attacked image						
PSNR(db)	11	10.23	23.1	30.9	17.2	33.1
Retrieved logo						
NC	.99	.94	.95	.99	.98	.99

5 Watermark Similar Images

Suppose that some people are taking picture from the same scene at the same time. These pictures are very similar to each other so when we zero watermark these pictures the produced key are very similar to each which might cause difficulties in ownership

protection. The purpose is to find a feature that makes a key distinguishable so that the ownership can be protected.

As described in above the new learning based contour detection method has good results in images that are taken from different point of views. The purpose is to find distinct features from these images so that they could be watermarked without having problem in the ownership of the images. The feature that we used should be good enough to have different results in images that are taken from different point of view in the same scene. We want to show that the new learning based contour detection method has a much better results in these kinds of images than Canny edge detector that is mostly used for finding features in zero watermarking.

Since there is no databases for the images that are taken from different point of views we created one such database. We set a camera on a Tripod. There is a moving graded circular plate below this tripod so that we can move the plate and take picture from different angles.

Figure 7 show some images from our database. The image angles differ from each other by 5° . The first picture is at center of the plate (angle 0). Then we move the plate 5° to the right and take a picture, we move it by another 5° and take another picture, etc. We use the same procedure for the left side.

This database has 9 classes. In each class there are 5 pictures. The difference between these classes is that we move the camera set 10 cm to the left or right and then take 5 pictures at that new location as we explained above.



Fig. 7. Image samples from the database taken from different angle view

5.1 How It Works

At the first step we apply the learning based contour detection method to our databases. Since now we have binary features for our images that are XOR ed with a logo for each image. As a result a key produced which is compared to show how the watermarks in these images are similar to each other. We use the first image in the first class of our 9 class as a base image to compare the keys. We use the NC to estimate the numbers of bits that are the same in the keys. Less similar results are better. Because we can understand that these keys are more distinguishable.

In Tables 3 and 4 we show the results (NC value) obtained using Canny edge detector and the learning based contour detection method.

Table 3. Results (NC value) of watermarking similar images using Canny edge detector

	Image1	Image2	Image3	Image4	Image5
Class1	1000	764.2136	727.7222	737.3734	726.2726
Class2	724.9756	719.6732	766.8381	725.9140	725.5478
Class3	749.3134	738.4567	759.4910	738.9069	727.9663
Class4	736.0458	722.4731	721.8933	738.5483	723.0148
Class5	713.9587	712.1658	752.9984	697.1283	697.1283
Class6	731.6208	772.3083	726.3184	752.6398	749.7482
Class7	712.6617	734.4589	734.4589	718.5593	766.6092
Class8	709.0378	714.8819	757.3166	760.2081	747.6501
Class9	714.3097	698.6084	755.5542	733.3374	744.4916

Table 4. Results (NC value) of watermarking similar images using learning based contour detection method

	Image1	Image2	Image3	Image4	Image5
Class1	1000	432.7698	398.1400	403.2669	460.4950
Class2	397.1481	436.9812	426.3077	450.9888	459.3430
Class3	403.2593	421.0587	405.1895	395.3934	442.0547
Class4	436.0123	403.5721	411.1710	462.8143	435.9436
Class5	399.6277	404.4876	421.7987	421.7987	394.3710
Class6	402.2064	386.0931	391.6397	389.9689	390.4343
Class7	457.7713	457.7713	387.0926	409.7519	449.1882
Class8	383.2016	380.5847	384.5825	385.2158	383.7509
Class9	383.5754	409.7443	388.0386	398.6359	460.4950

As seen in above tables, the NC s in new method are decreased very high. It shows the difference between the keys indicating the difference between zero-watermarked images. This supports the ability of the proposed method for providing ownership protection to very similar images.

This new learning based contour detection method returns the edges that are very similar to that the human can see. We showed that these edges are good features for watermarking similar images. In fact the more similarity between detected images to those perceived by humans, the more accurate results we will get in zero-watermarking. In Canny edge detection method we may get the best results by tuning the parameters but in the proposed method the best results are obtained without the need for parameter tuning.

6 Conclusion

Recently a new digital watermarking method called zero-watermarking has been proposed that does not degrade the quality of the host image. In this method binary features are extracted from the image. Then these binary features are combined with a watermark logo and a key is produced. This key is kept in a trusted authority for security and authentication. In this paper we first show that the learning based contour detection method has better results in watermark robustness compared to the traditional Canny edge detection. Then we show that the learning based contour detection method has reliable performance when zero-watermarking highly similar images (images that are taken from different angle views).

With this new algorithm we can watermark similar images. The produced keys are distinguishable enough for protecting the ownership of similar images. As we have shown, the Canny edge detection method features (that is mostly used in recent papers) are not good enough for watermarking similar images. Because the Canny method returns edges that are very similar to each other and cannot understand the overall changes of similar images.

References

1. Shakeri, M., Jamzad, M.: A robust zero-watermarking scheme using Canny edge detector. *Int. J. Electron. Secur. Digit. Forensics* **5**(1), 25–44 (2013)
2. Arbelaez, P., Maire, M., Fowlkes, C., Malik, J.: Contour detection and hierarchical image segmentation. *IEEE TPAMI* **33**(5), 898–916 (2011)
3. Shapiro, L.G., Stockman, G.C.: *Computer Vision*, Prentice Hall (2001)
4. Martin, D., Fowlkes, C., Malik, J.: Learning to detect natural image boundaries using local brightness, color and texture cues. *PAMI* **26**(5), 530–549 (2004)
5. Savitzky, A., Golay, M.J.E.: Smoothing and differentiation of data by simplified least squares procedures. *Anal. Chem.* **36**(8), 1627–1639 (1964)
6. Chen, T.H., Horng, G., Lee, W.B.: A publicly verifiable copyright proving scheme resistant to malicious attacks. *IEEE Trans. Ind. Electron.* **52**(1), 327–334 (2005)
7. Abdel-Wahab, M.A., Selim, H., Sayed, U.: A novel robust watermarking scheme for copyright-proving. In: *The 2009 International Conference on Computer Engineering and Systems, ICCES 2009*, art. no. 5383216, pp. 482–486 (2009)

Artificial Intelligence and Signal Processing
International Symposium, AISP 2013, Tehran, Iran,
December 25-26, 2013, Revised Selected Papers
Movaghar, A.; Jamzad, M.; Asadi, H. (Eds.)
2014, XII, 346 p. 150 illus., Softcover
ISBN: 978-3-319-10848-3