Evaluation of Image Forgery Detection Using Multi-scale Weber Local Descriptors

Sahar Q. Saleh[1], Muhammad Hussain[1], Ghulam Muhammad[1], and George Bebis[2]

[1] College of Computer and Information Sciences, King Saud University, Riyadh 11543, Saudi Arabia Department of Computer Science and Engineering
[2] University of Nevada at Reno, USA
{mhussain,ghulam}@ksu.edu.sa, bebis@cse.unr.edu

Abstract. In this paper, a detailed evaluation of multi-scale Weber local descriptors (WLD) based image forgery detection method is presented. Multi-scale WLD extracts the features from chrominance components of an image, which usually encode the tampering information that escapes the human eyes. The WLD incorporates differential excitation and gradient orientation of a center pixel around a neighborhood. In the multi-scale WLD, three different neighborhoods are chosen. A support vector machine is used for classification purpose. The experiments are conducted on three image databases, namely, CASIA v1.0, CASIA v2.0, and Columbia color. The experimental results show that the accuracy rate of the proposed method are 94.19% for CASIA v1.0, 96.61% for CASIA v2.0, and 94.17% for Columbia dataset. These accuracies are significantly higher than those obtained by some state-of-the-art methods.

Keywords: image forgery detection, Weber local descriptors, image splicing, copy-move forgery.

1 Introduction

Nowadays, we are living in an age, where digital imaging has grown and developed to become the widespread technology. With the increasing applications of digital imaging, different types of software are introduced for image processing. Such software can do an alteration in digital image by changing blocks of an image or combining two images with no showing the effect of the modification in the forged image. The most commonly used forgery is copy-move forgery (CMF), where a region within an image is copied and moved to another region in the same image in order to conceal an important object from the original image. The copied block may be changed by any kind of pre-processing such as rotation, scaling, additive noise, etc. to suit the copied area with the whole image. In another type of forgery, one part of an image is copied and pasted to another image. This type of forgery is called image splicing.

Many techniques have been developed for authenticity checking of the digital images. These techniques can be divided into intrusive (active) and non-intrusive (blind or passive) [1]. In active techniques, particular data is embedded in the digital

G. Bebis et al. (Eds.): ISVC 2013, Part II, LNCS 8034, pp. 416–424, 2013.

images for supporting multimedia digital authentication and rights safety. If the image contents are modified, the embedded data is also changed. The image authenticity is verified by checking whether the true signature corresponds to the signature that is retrieved from the suspicious test image. These techniques are restricted because of the inability of many digital cameras to embed the signature. Due to the restrictions of active techniques, the researchers tend to develop non-intrusive techniques for validating the authenticity of digital images. These techniques examine images with no embedded data such as signatures or watermarks, and result whether these images are authentic or tampered.

An improved DCT (discrete cosine transform)-based technique was proposed in [2] to discover CMF in digital images. The image is subdivided into blocks, and the DCT is computed. The DCT coefficients are lexicographically sorted, and compared with different blocks. The proposed technique is robust against JPEG compression, additive white Gaussian noise, or blurring distortion. Cao et al [3] proposed an improved DCT-based method to locate the duplicated regions in a given image. The method uses the circle block for representing the DCT coefficient's array.

Noise pattern based image forgery detection method was proposed in [4]. Noise pattern is obtained by subtracting the denoised image from the input image. Then, histograms of noise from different segments of the image are compared to find the distortion caused by image forgery. Peng et al [5] also used sensor pattern noise to detect image forgery. Instead of using the histogram, they use four statistical measures, namely, variance, entropy, signal-to-noise ratio, and average energy gradient, from the noise pattern. He et al in [6] proposed a method relied on approximate run length (ARL) to detect CMF. Firstly, the edge-gradient array of a given image is calculated, and then the ARL is computed along the edge-gradient orientation. Zhao *et al* used chrominance spaces with RLRN (run-length run-number) for CMF detection [7]. The input color image is transformed into the YCbCr color mode. Then RLRN is used to extract the features from the de-correlation of the chrominance channels. Support vector machine (SVM) was used for classification purpose. This method gave better performance with JPEG image format than the TIFF image format. Shi *et al* proposed statistical features based on 1D and 2D moments, and transition probability features based on Markov chain in DCT domain for image splicing detection [20]. In CASIA v2.0 database [16], the method achieves 84.86% accuracy. Later, He *et al* improved the method by combining transition probability features in DCT and DWT domains [21]. For classification, they used SVM - recursive feature elimination (RFE). Their method obtains 89.76% accuracy on the CASIA v2.0 database.

Undecimated wavelet transforms (UWT) based image forgery detection was proposed in [8]. Approximation and detailed coefficients of the UWT from overlapping blocks of an image are used to find the similarity between the blocks. The method is robust against JPEG compression and a certain degree of rotation and scaling. Scale invariant feature transform (SIFT) based forgery detection methods are proposed in [9], [10], [11]. They are quite robust against rotation and scaling post-processing. Two good surveys can be found in[1], [12].

In this paper, we give a detailed evaluation of a method based on a multi-scale Weber's law descriptor [13] and SVM [14] for detecting image forgery. The forgery can be either copy-move or spliced. The proposed method is evaluated on three publicly available image databases designed for forgery detection.

The rest of the paper is organized as follows. Section 2 presents the image forgery detection method, Section 3 gives experimental results with discussion, and finally, Section 4 draws some conclusion.

2 Forgery Detection Method

Fig. 1 shows a block diagram of the proposed image forgery detection method. In the first step, input color image is converted into the YCbCr color space. Image forgers generally do image tampering in RGB color-space and attempt to wrap manipulated traces. YCbCr color space stores the color in terms of its luminance and chrominance. The human eyes are less sensitive to chrominance than luminance; however, even a tampered image looks natural, some tampered traces are left in the chrominance channels [7]. In the second step, the chrominance component (either Cb or Cr) is used to extract image features in the form of Weber local descriptors (WLD) [13]. Multi-scale WLD is introduced where the histograms from different operators of variation (P, R) are concatenated and used to represent the image features; P is the count of the neighbors, and R is the spatial-scale for the operator. In the last step, SVM based classifier is used to classify the input image as authentic or forged.

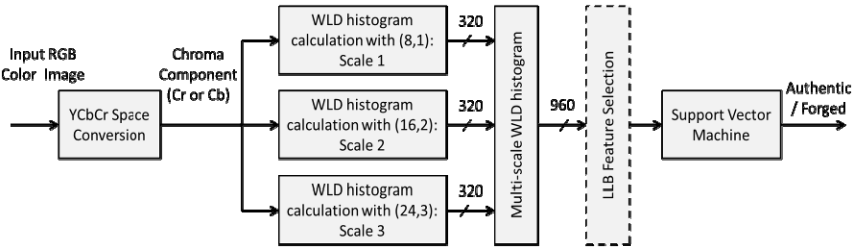

Fig. 1. Block diagram of the proposed image forgery detection method

WLD is a robust local descriptor, which is based on the fact that human sensitivity of a sample relies on the change of the original stimulus intensity [13]. WLD descriptor is described below for feature extraction purpose. WLD based on Weber's law has two components: differential excitation (D) and orientation (Φ).

Ernst Weber viewed that the ratio of the increase threshold to the intensity of the background is a constant. It is formulated as

$$\frac{\Delta x}{x} = C \tag{1}$$

Where x is the initial stimulus-intensity, Δx is the increase in threshold (noticeable distinction), and C is a constant.

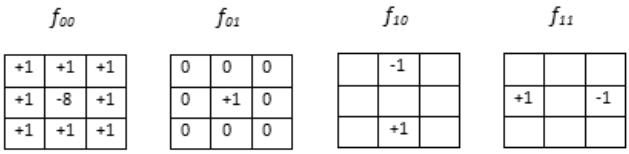

Fig. 2. Filters used in WLD calculation

A differential excitation (D) is used to change the intensity of each pixel in an image. The $D(p_c)$ for a pixel p_c is calculated as follows:

Step1: Compute the difference between the pixel p_c and its neighbours via the filter (f_{00}) in Fig. 2.

$$k_s^{00} = \sum_{i=0}^{N-1} (\Delta p_i) = \sum_{i=0}^{N-1} (p_i - p_c) \tag{2}$$

where p_i is the ith neighbour of pixel p_c and N is the number of neighbours.

Step2: Calculate the proportion of the differences to the current pixel intensity by the outputs of the filter (f_{00}) and (f_{01}) in Fig. 2.

$$I = \frac{k_s^{00}}{k_s^{01}} = \sum_{i=0}^{N-1} \left(\frac{p_i - p_c}{p_c} \right) \tag{3}$$

The differential excitation $D(p_c)$ of the current pixel p_c is

$$D(p_c) = \arctan\left[\sum_{i=0}^{N-1} \left(\frac{p_i - p_c}{p_c} \right) \right] \tag{4}$$

WLD orientation component is the gradient orientation, Φ (p_c), and it is calculated as follows:

$$\Phi(p_c) = \arctan\left(\frac{k_s^{11}}{k_s^{10}} \right) \tag{5}$$

where, k_s^{11} and k_s^{10} are the outputs of the filters f_{11} and f_{10}.

Later, Φ is mapped to Φ' and is quantized into T dominant directions. After calculating differential excitation and gradient orientation, WLD histogram is formed. In WLD histogram, there are three parameters that affect on optimizing the results: the number of dominant orientations (T), the number of differential excitation segments (M), and the number of bins in sub histogram segments Hm,t (S).

In the proposed multi-scale WLD, differential excitation and gradient orientation are calculated in three different neighborhoods, which are (8,1), (16,2), and (24,3), where the first component inside the parenthesis corresponds to the number of neighboring pixels and the second component is the radius of the neighbors from the center pixel (scale). The histograms from these three neighborhoods are fused to produce the multi-scale WLD histogram.

Local learning based (LLB) feature selection technique is applied to the whole feature vector to reduce the dimension [15]. The main design of this technique is to

decompose a randomly complicated non-linear problem into a group of locally linear problems by using local learning, and the feature relevance is learned globally in the maximum margin framework.

3 Experiments

The proposed method is evaluated in three publicly available databases that are designed for image forgery detection. The three databases are CASIA TIDE v1.0 and v2.0 [16], and Columbia authentic and spliced color image database [17].

Different scales with various numbers of neighborhoods in the WLD are used. We name the scaling from C1 to C7, where C1 means (8, 1), C2 corresponds to (16, 2), C3 refers to (24, 3), C4 is a combination of (8, 1) and (16, 2), C5 is a combination of (8, 1) and (24,3), C6 is a combination of (16, 2) and (24, 3), and finally, C7 is the combination of all the scales (8, 1), (16, 2) and (24, 3). For (T, M, S) parameters of WLD, various combinations are tried and finally fixed to (4, 4, 20) that gives the optimal result.

Performance of the proposed method with SVM classification by employing RBF kernel and polynomial kernel has been evaluated using a 10-fold cross validation. The polynomial kernel performs better than the RBF kernel in our experiments, so we report results only with polynomial kernel. Grid search method is used to find the optimal parameters of SVM. LIBSVM is utilized for SVM implementation [18]. The performance of the method is given in terms of accuracy (averaged over ten iterations).

3.1 Experiments with CASIA v1.0

CASIA v1.0 dataset has 800 authentic images and 921 forged images of which 459 are copy-move forged and the remaining are spliced. Scaling and rotation have been applied on some of the forged images. All the images have the size of 384×256 pixels, and they are in JPEG format.

Fig. 3 shows the effect of different WLD scales in Cr channel. For individual scale (C1, C2, C3), C3 performs the best. In the case of multi-scale, C7, which is the combination of all the three scales, has the highest detection accuracy. With Cr channel, C7 achieves 92.62% accuracy, while with Cb channel, it obtains 88.66% (not shown). Therefore, it is experimentally proved that the multi-scale WLD performs better than the single scale WLD in the case of image forgery detection. Each single scale WLD produces 320 features (bins in the histogram), so C7 has a total of (320×3=) 960 features. All the subsequent results are with C7.

In the next experiment, Cr and Cb histograms are combined to see the accuracy. We call this combination as feature level fusion (FLF) and the feature vector is of dimension 1920 (=960×2). After feature selection, this dimension is reduced to 770. In the experiments, three cases are considered: testing with spliced images, testing

with copy-move images, and testing with the whole dataset. Fig. 4. shows the detection accuracies (%). FLF performs better than individual chrominance channel, and it achieves 94.19% accuracy for the full CASIA v1.0 dataset. False positive rate and false negative rate is 6.3% and 3.7%, respectively. Splicing detection accuracy (94.52%) is higher than copy-move forgery detection accuracy (92.08%). Fig. 5. shows the ROC curve of the proposed method on the full dataset. For comparison purpose, we implemented the method described in [19] and evaluated it on the full CASIA v1.0 dataset using Cr channel. The method [19] obtains 78.53% accuracy, which is much less than 92.62% achieved by the proposed method using Cr.

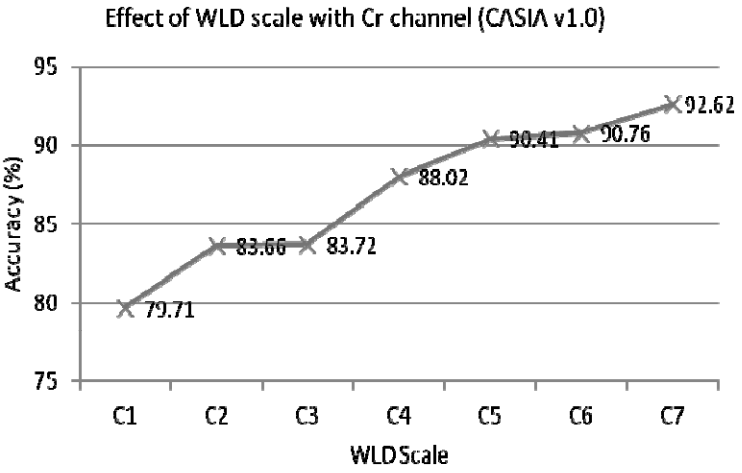

Fig. 3. Accuracy of splicing detection using chrominance channel, Cr, in different scales of WLD

3.2 Experiments with CASIA v2.0

CASIA v2.0 database consists of 7491 authentic and 5123 forged images of JPEG, BMP, and TIFF format, where image sizes vary from 240×160 to 900×600 pixels. Scaling and rotation have been applied on some of the forged images. The experiments are performed with the full dataset. Table 1 shows the result of the proposed method in terms of accuracy (%) with standard deviation (sd) and area under curve (AUC). The best performance (accuracy = 96.61%) is achieved with the Cb channel. It is noted that no feature selection is applied in the experiments in Table 1. The performance of the proposed method is far superior to that of the other state of the art methods [20], [21] evaluated in full CASIA v2.0. Table 2 shows a comparison of accuracies between the methods.

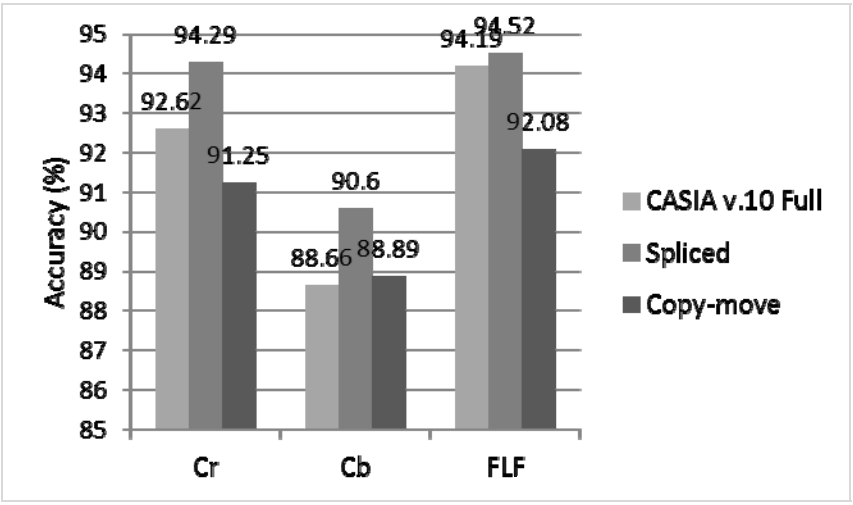

Fig. 4. Accuracy of the proposed method in CASIA v1.0

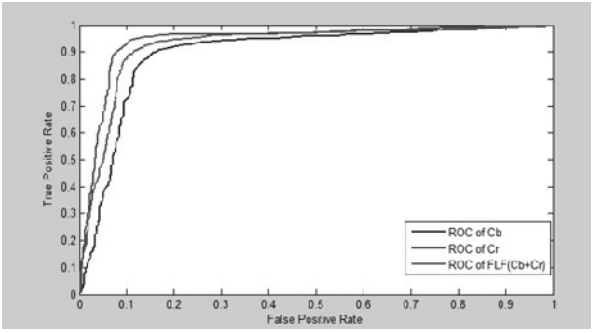

Fig. 5. ROC curves of the proposed method in CASIA v1.0

3.3 Experiments with Columbia Color

Columbia color image database consists of 183 authentic and 180 spliced images of TIFF format. The image size is 1152×768. Table 3 shows the results with feature selection. The proposed method with FLF achieves 94.17% accuracy, which is better than the previously reported best result by the method in [22]. The number of features in FLF after feature selection is 316.

Table 1. Performance of the proposed method in CASIA v2.0

Channel	Acc(%) ± sd	AUC ± sd
Cr	96.38 ± 0.36	0.966 ± 0.0049
Cb	96.61 ± 0.49	0.969 ± 0.0038
FLF	96.28 ± 0.675	0.96 ± 0.0076

Table 2. Accuracies of the three methods in CASIA v2.0

Proposed Method	Method [20]	Method [21]
96.61%	84.86%	89.76%

Table 3. Performance of the proposed method in Columbia

Channel	Acc(%) ± sd	AUC ± sd	Acc (%) of [22]
Cr	92.5 ±4.73	0.93 ± 0.05	93.14
Cb	92.78 ± 3.51	0.93 ±0.05	
FLF	**94.17** ± 3.57	0.93 ± 0.05	

4 Conclusion

A detailed evaluation of a multi-scale WLD based image forgery detection method is presented. WLD features are extracted from the chrominance channels of a color image. SVM is used for classification purpose. The best results achieved by the forgery detection method are 94.19% with CASIA v1.0, 96.61% with CASIA v2.0, and 94.17% with Columbia color image databases. These accuracies are better than some of the previously reported results in these databases. The performances of Cb and Cr channels are comparable, while their fusion gives the best result except in the case of CASIA v2.0. A future work will be to localize the forgery in a tampered image.

Acknowledgement. This work is supported by the National Plan for Science and Technology, King Saud University, Riyadh, Saudi Arabia under project number 10-INF1140-02.

References

1. Mahdian, B., Saic, S.: A bibliography on blind methods for identifying image forgery. Signal Processing: Image Communication 25(6), 389–399 (2010)
2. Huang, Y., Lu, W., Sun, W., Long, D.: Improved DCT-based detection of copy-move forgery in images. Forensic Science International 206(1), 178–184 (2011)
3. Cao, Y., Gao, T., Fan, L., Yang, Q.: A robust detection algorithm for copy-move forgery in digital images. Forensic Science International 214(1), 33–43 (2012)
4. Muhammad, N., Hussain, M., Muhamad, G., Bebis, G.: A non-intrusive method for copy-move forgery detection. In: Bebis, G., et al. (eds.) ISVC 2011, Part II. LNCS, vol. 6939, pp. 516–525. Springer, Heidelberg (2011)
5. Peng, F., Nie, Y.-Y., Long, M.: A complete passive blind image copy-move forensics scheme based on compound statistics features. Forensic Science International 212(1), e21–e25 (2011)

6. He, Z., Sun, W., Lu, W., Lu, H.: Digital image splicing detection based on approximate run length. Pattern Recognition Letters 32(12), 1591–1597 (2011)
7. Zhao, X., Li, J., Li, S., Wang, S.: Detecting digital image splicing in chroma spaces. In: Kim, H.-J., Shi, Y.Q., Barni, M. (eds.) IWDW 2010. LNCS, vol. 6526, pp. 12–22. Springer, Heidelberg (2011)
8. Muhammad, G., Hussain, M., Bebis, G.: Passive copy move image forgery detection using undecimated dyadic wavelet transform. Digital Investigation (2012)
9. Amerini, I., Ballan, L., Caldelli, R., Del Bimbo, A., Serra, G.: A SIFT-Based Forensic Method for Copy–Move Attack Detection and Transformation Recovery. IEEE Transactions on Information Forensics and Security 6(3), 1099–1110 (2011)
10. Huang, H., Guo, W., Zhang, Y.: Detection of copy-move forgery in digital images using SIFT algorithm. In: Pacific-Asia Workshop on Computational Intelligence and Industrial Application, PACIIA 2008, pp. 272–276. IEEE (2008)
11. Ling, H., Zou, F., Yan, W.-Q., Ma, Q., Cheng, H.: Efficient image copy detection using multi-scale fingerprints (2011)
12. Farid, H.: Image forgery detection. IEEE Signal Processing Magazine 26(2), 16–25 (2009)
13. Chen, J., Shan, S., He, C., Zhao, G., Pietikainen, M., Chen, X., Gao, W.: WLD: A robust local image descriptor. IEEE Transactions on Pattern Analysis and Machine Intelligence 32(9), 1705–1720 (2010)
14. Cristianini, N., Shawe-Taylor, J.: An introduction to support vector machines and other kernel-based learning methods. Cambridge University Press (2000)
15. Sun, Y., Todorovic, S., Goodison, S.: Local-learning-based feature selection for high-dimensional data analysis. IEEE Transactions on Pattern Analysis and Machine Intelligence 32(9), 1610–1626 (2010)
16. CASIA image tampering detection evaluation database (CASIA TIDE) v1.0 and v2.0, `http://forensics.idealtest.org`
17. Ng, T.-T., Chang, S.-F., Sun, Q.: A data set of authentic and spliced image blocks. Columbia University, ADVENT Technical Report, 203-2004 (2004)
18. Chang, C.-C., Lin, C.-J.: LIBSVM: a library for support vector machines. ACM Transactions on Intelligent Systems and Technology (TIST) 2(3), 27 (2011)
19. Wang, W., Dong, J., Tan, T.: Image tampering detection based on stationary distribution of markov chain. In: 2010 17th IEEE International Conference on Image Processing, ICIP, pp. 2101–2104. IEEE (2010)
20. Shi, Y.Q., Chen, C., Chen, W.: A natural image model approach to splicing detection. In: Proceedings of the 9th Workshop on Multimedia & Security 2007, pp. 51–62. ACM (2007)
21. He, Z., Lu, W., Sun, W., Huang, J.: Digital image splicing detection based on Markov features in DCT and DWT domain. Pattern Recognition (2012)
22. Zhao, X., Li, S., Wang, S., Li, J., Yang, K.: Optimal chroma-like channel design for passive color image splicing detection. EURASIP Journal on Advances in Signal Processing 2012(1), 1–11 (2012)