IMAGE FORGERY DETECTION USING GABOR FILTERS AND DCT

Ghulam Muhammad[1]*, M. Solaiman Dewan*[2]*, M. Moniruzzaman*[3]*, Muhammad Hussain*[1]*, and M. Nurul Huda*[4]

[1]College of Computer and Information Sciences, King Saud University, Riyadh, Saudi Arabia
{ghulam, mhussain}@ksu.edu.sa
[2]Tofa Limited, London, United Kingdom. shisdew@gmail.com
[3]Teraways Pvt. Ltd., Jurong West Street 64, Singapore. mzamanbd@gmail.com
Department of Computer Science and Engineering, United International University, Dhaka, Bangladesh

Abstract— Determining the authenticity of an image has become crucial due to a widespread use of images in various media to covey real or fake messages. In this paper, an image forgery detection method based on Gabor filters and discrete cosine transform (DCT) is proposed. The output of this method is to determine whether an image is authentic or forged. In this method, first, the input image is converted to gray scale image. Second, several Gabor filters with different scales and orientations are applied to the image. Then the DCT from all the filter outputs (subbands) is calculated. The first *N* coefficients of the DCT from all the subbands are concatenated to form the feature vector. Some feature selections are used to find optimal feature set. Support vector machine (SVM) is used as a classifier. In the experiments, the proposed method outperforms some state-of-the-art methods of image forgery detection.

Keywords— image forgery detection, Gabor filters, discrete cosine transform, support vector machine

I. INTRODUCTION

The security concern of digital content has arisen a long time ago and various techniques for validating the integrity of digital images have been developed. As a result of such development, different forensics-related questions arise such as, how an image was acquired? Was it captured using digital devices (cameras and scanners) or artificially generated using computer software? Is it authentic or it has undergone any kind of manipulation after capturing? The answers to such forensics questions are related to tracing the origin of the digital image to its creation process. The field of digital images forensics has emerged and developed over the past few years as a solution to these growing challenges. The forensic analysis for digital images provides helpful information to law enforcement, security, and intelligence agencies [1].

Two major manipulations can be done on images, which are copy-move and splicing. In copy-move forgery, a part or several parts of an image are copied and pasted in another part(s) of an image. If the copy-paste process involves the same image, it is called simply copy-move image forgery. However, if the copy-paste process involves more than one image, it is called splicing. While doing forgery, some types of transformation such as rotation, scaling, can be done on the copied part before pasting. In most of the cases, various post-processing such as blurring, adding noise, etc. are applied on the pasted region to hide the forgery in the naked eyes.

Many techniques have been proposed to detect digital image forgery. These techniques can be divided into two major groups, which are intrusive and non-intrusive. In intrusive (active) techniques, some sort of signature (watermark, extrinsic fingerprint) is embedded into a digital image, and authenticity is established by verifying if the true signature matches the retrieved signature from the test image [2]. This approach is limited due to the inability of many digital cameras and video recorders available in the market to embed extrinsic fingerprints [3]. The limitations of intrusive techniques have motivated the need for non-intrusive (blind) techniques to validate the authenticity of digital images [4]. These techniques exploit different kinds of intrinsic fingerprints such as sensor noise of the capturing device or image specific detectable changes for detecting forgery. There are many challenges in blind techniques, for instance, reducing false positive rates (i.e., an authentic image being detected as a forged image), making the system fully automated, localizing the forgery, detecting forgery of any type of image format (compressed or uncompressed), increasing the robustness and reliability, etc.

There are mainly two types of blind image forgery detection methods, which are detection on the image level where the methods only detect image as an authentic or forged one (without localization), and detection on the pixel or block level that specifies the forged area (with localization). The work of this paper concentrates on image forgery detection without localization.

Over the last ten years, many researchers have proposed different approaches for detecting digital image forgery. Most of the techniques involved in these approaches are based on image processing and pattern recognition. Some popular approaches include the moment-based approach [5, 6], the forgery type specific approach [7, 8], the local feature-based approach [9, 10] and the color-based approach [11, 12]. Despite of the attractiveness of this field of research and the huge number of studies that had been done during the last few years, more effort is still needed, since there is no perfect copy- move forgery detection scheme with high robustness against all kinds of post processing operations and geometric translations (such as JPEG compression, blurring, noise addition, shifting, scaling, rotation, etc.). Many of the proposed methods show excellent results with a specific type of tampering operation, but the efficiency is degraded with the presence of another operation.

In this paper, we propose an image forgery detection method based on Gabor filters and discrete cosine transform

(DCT). Gabor filters can decompose an image into many subbands having different orientations and scales. DCT is then applied to find the compact energy of the subbands. Support vector machine (SVM) is used as a classifier.

The rest of the paper is organized as follows. Section II describes the proposed method; Section III gives experimental results with discussion, and Section IV draws some conclusion.

II. PROPOSED METHOD

Figure1 shows a block diagram of the proposed image forgery detection method using Gabor filters and DCT. In the following, we describe the steps in detail.

First, a color image is converted into YCbCr chrominance space, where Y is the luminance, and Cb and Cr are the chrominance components. The Cb and Cr are the blue difference and the red difference, respectively. Luminance channel is more sensitive to human eyes than the chrominance channels. As forgery is hard to detect in naked human eyes, chrominance channels are more suitable for forgery detection [13]. Therefore, we concentrate only on Cb and Cr channels.

In the second step, the Gabor filter transform (GFT) is applied to any of the chrominance components. GFT is a powerful multi-scale and multi-orientation image decomposition technique. Gabor filters are biologically motivated convolution kernels and their response is found to be similar to receptive fields of neurons in the visual cortex [14]. An interesting property of these filters is that they possess optimal joint localization both in frequency and spatial domains. A 2-dimesional Gabor filter can be defined as follows [15]:

$$g(x,y) = \frac{1}{2\pi\sigma_x\sigma_y} e^{\left[-0.5\left(\frac{\bar{x}^2}{\sigma_x^2}+\frac{\bar{y}^2}{\sigma_y^2}\right)\right]} e^{\left(2\pi j W \bar{x}\right)} \qquad (1)$$

Where σ_x and σ_y are the scaling parameters, W is the central frequency of the sinusoidal wave and is termed as the orientation of the filter. In general, a Gabor filter is a Gaussian kernel modulated by an oriented sinusoidal wave. In order to get the texture properties of an image, Gabor filters can be tuned with different orientations and scales [16].

In this paper, we use Gabor filters with three different scales and five different orientations. The scales are 2, 3, and 4, while the orientations are 0, $\pi/5$, $2\pi/5$, $3\pi/5$, and $4\pi/5$. Figure 2 shows the kernels of the Gabor filters used in this paper. The relationship between the scale and the frequency is given the following formula:

$$freq(i) = \frac{f_{\max} = 0.2}{\left(\sqrt{2}\right)^{i-1}}, i = 1,2,....,S \qquad (2)$$

The third step is the feature extraction; DCT is applied on each filter output The DCT represents an image as a sum of cosine of different frequencies [17]. In other words, it transforms the image from spatial domain (set of intensity values) to frequency domain (set of frequency coefficients). The frequency domain provides a better representation in sense of which information is visually significant than others. DCT has the property that it concentrates this information in only few coefficients (low frequencies). The DCT transforms an array of pixel values to an array of coefficients of frequencies. The top-left coefficient represents the low frequency information and known as DC or average component, while the other coefficients give the high frequency information (AC components). The bottom-right coefficient represents the highest frequency [17]. In our experiments, we extracted first 20 DCT coefficients in zig-zag order (see Figure 3) from each subband.

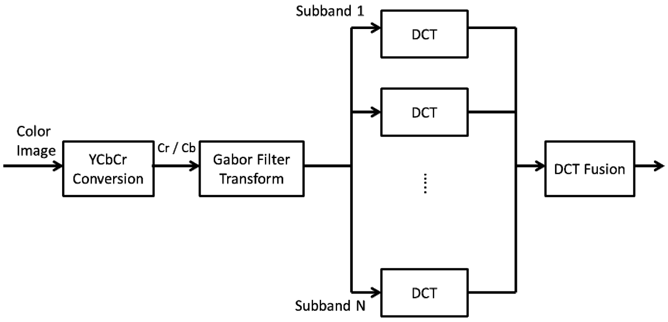

Figure 1. Block diagram of the proposed GFB and DCT based image forgery detection method.

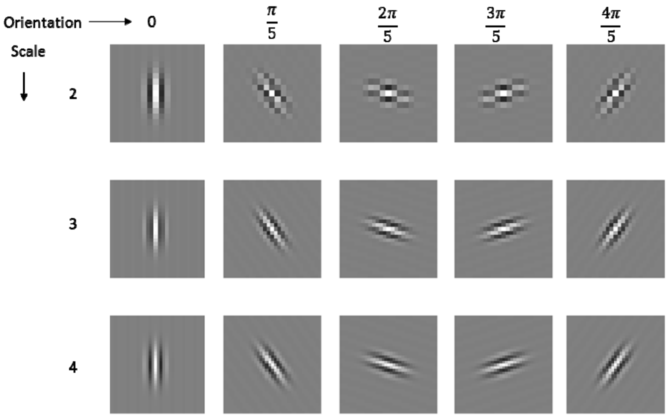

Figure 2. Gabor filters' kernels used in the proposed method.

In the fourth step, two different data reduction methods were used for feature selection, which are 0-norm and local learning based (LLB) [18]. 0-norm ranks the features based on the statistical significance, while LLB removes features that contain redundant information. A cascading of the two methods is used to enhance the performance of the proposed method. In the cascading, first, 0-norm is applied followed by the LLB, and the threshold for the LLB is set to 10^{-10}. In the final step of the proposed method, the SVM classification with RBF (radial basis function) kernel and 10-fold cross-validation is used to evaluate the performance.

1	2	6	7	15	16	28	29
3	5	8	14	17	27	30	43
4	9	13	18	26	31	42	44
10	12	19	25	32	41	45	54
11	20	24	33	40	46	53	55
21	23	34	39	47	52	56	61
22	35	38	48	51	57	60	62
36	37	49	50	58	59	63	64

Figure 3. The zig-zag order of the DCT coefficients.

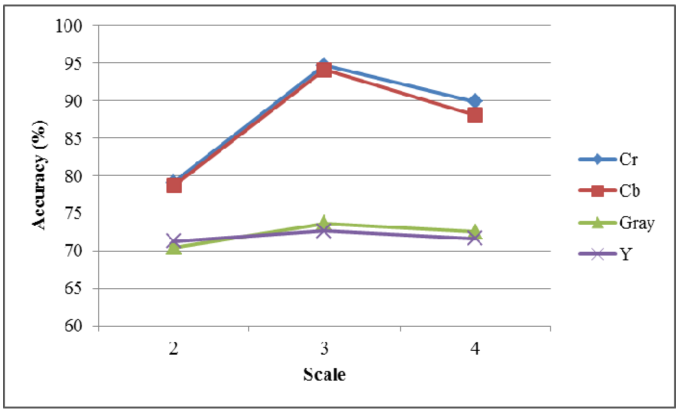

Figure 4. Effect of the scales of the Gabor filters.

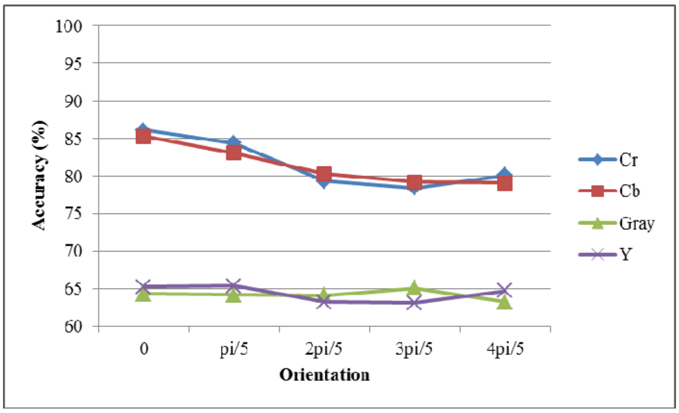

Figure 5. Effect of the orientations of the Gabor filters.

III. EXPERIMENTAL RESULTS AND DISCUSSION

In the experiments, three databases, which are CASIA v1.0 [8], and CASIA v2.0 [8] are used. First, a detailed experiment on the proposed method is presented using the CASIA v1.0 database. Then comparisons are provided with the CASIA v2.0 databases.

A. *Experiments with CASIA v1.0 Database*

CASIA v1.0 dataset has 800 authentic images and 921 forged images of which 459 are copy-move forged and the remaining are spliced. All the images have the size of 384×256 pixels, and they are in JPEG format. In the experiments, a randomly selected 25% of the whole dataset samples are used for the feature selection step. The LIBSVM toolbox [19] is then used for the classification. The optimal values for the RBF kernel parameter 'sigma' and the optimization parameter 'C" of SVM are automatically set by an intensive grid search process using the training set. The performance of the proposed method is given in terms of accuracy averaged over 10 iterations of the SVM.

Intensive experiments are carried out to test the performance of the proposed method. Many combinations of different image representations (grayscale, Y, Cr and Cb), GFT subbands are used in the evaluation, in order to notice how the performance is affected by different Gabor filter scales, orientations and image components. The following three investigations are without feature selection.

Effect of the Gabor filter scale

In this experiment, the performances of three different subbands, which are at different scales, with the combined orientations (all the five orientations) are studied. The feature vector length in this case is 20×5 (the number of DCT coefficients × number of orientations). In all the channels, scale 3 has the highest accuracy. The accuracy of the scale 3 in Cr channel is 94.7%. The accuracy of the same channel decreases to 89.9% in the scale 4, followed by 79.1% in the scale 2. Figure 4 shows the effect of the scales using four different image components.

Effect of the Gabor filter orientation

The histograms of the three scales within each orientation are concatenated to form a feature vector of length 20×3. Figure 5 shows the accuracy of the five orientations in different channels. The accuracy of the first orientation is higher than those in other orientations.

Effect of combining all the subbands

This experiment studies the performance of combining all the subbands of GFT by concatenating all the DCT histograms across all the subbands. The length of the feature vector in this case is 20×15 (=300). The performances of the four different channels are 96.13% for Cr, 93.76% for Cb, 74.34% for Y, and 75.2% for gray. It is clear that the combination of all subbands achieves the highest accuracy for each channel, where Cr and Cb have superior performances over Y and gray.

After the feature selection the number of features is reduced from 300 to 70 on the average. In this case, the accuracies using Cr, Cb, Y, and gray are 96.21%, 94.34%, 75.58%, and 76.22%, respectively.

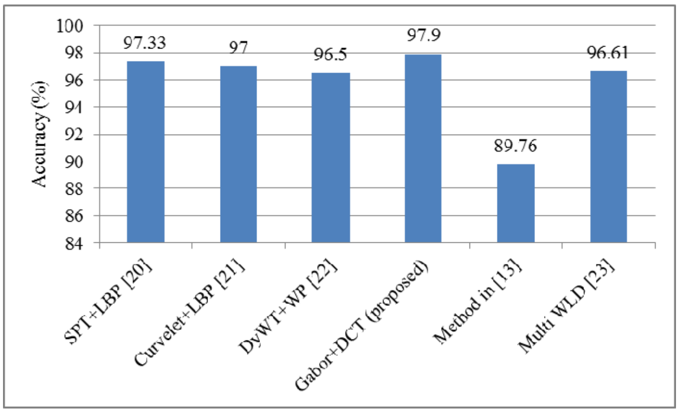

Figure 6. Accuracies (%) of the compared methods using CASIA v2.0 database.

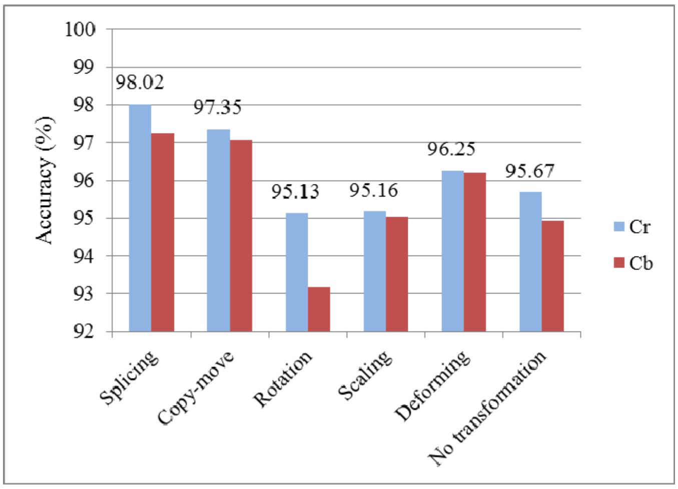

Figure 7. Accuracies (%) of the proposed method in different cases of CASIA v2.0 database.

B. Experiments with CASIA v2.0 Database

Table 2 shows the performance of the proposed method on CASIA v2.0 database. This database consists of 7491 authentic and 5123 forged images of JPEG, BMP, and TIFF format, where image sizes varying from 240×160 to 900×600 pixels. The proposed method achieves 97.9% accuracy (after feature selection), which is a significant jump from all other reported accuracies on this full database. We compare our proposed method with some of the state-of-the-art methods such as methods using steerable pyramid transform [20], curvelet transform [21], dyadic wavelet transform and Weber pattern [22], Markov features [13], and multiscale Weber local descriptor (WLD) [23]. The accuracies of these methods on the full CASIA v2.0 database are shown in Figure 6.

We also performed several experiments on CASIA v2.0 database using spliced only, copy-move only, rotation only, scaling only, deforming only, no transformation only images. The accuracies using these cases represent the strength of the proposed method in different forgery situations. Figure 7 shows the results with Cr and Cb channels.

In another experiment, we implemented the method described in [24] in Cr channel and compared the performance with the proposed method. In [24], the authors used LBP and DCT in a grayscale image. The implementation gave 91.38% accuracy on CASIA v2.0 database. Wei *et al*. reported 95.6% accuracy on CASIA v2.0 using stationary distribution of Markov chain; however, it is not clear whether they used the whole database or not [25]. Nevertheless, our proposed method outperformed this method as well.

IV. CONCLUSION

Gabor filter and DCT based image forgery detection method has been proposed. Different color components such as chrominance, luminance, and gray are evaluated. The proposed method is tested on CASIA v1.0 and v2.0 databases. Experimental results show that the proposed method outperforms some of the state-of-the-art methods of forgery detection. In a future study, we will apply the proposed method to localize the forgery.

ACKNOWLEDGMENT

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] A. Swaminathan, M. Wu, K. J. R. Liu, “Digital Image Forensics via Intrinsic Fingerprints,” IEEE Trans. Inf. Forensics Security, vol. 3, no. 1, 101-117, March 2008.

[2] C. Zhang, L. L. Cheng, Z. Qiu, and L. M. Cheng, "Multipurpose Watermarking Based on Multiscale Curvelet Transform," IEEE Trans. Inf. Forensics Security, vol. 3, no. 4, pp. 611–619, December 2008.

[3] H. Farid, "Exposing Digital Forgeries From JPEG Ghosts," IEEE Trans. Inf. Forensics Security, vol. 4, no. 1, pp. 154–160, 2009.

[4] Chen, L., Lu, W., Ni, J., Sun, W., & Huang, J., “ Region duplication detection based on Harris corner points and step sector statistics,” Journal of Visual Communication and Image Representation, 24(3), pp. 244-254, 2013.

[5] B. Mahdian and S. Saic, "Detection of copy-move forgery using a method based on blur moment invariants," Forensic Science International, vol. 171, no. 2, pp. 180–189, 2007.

[6] S-J. Ryu, M-J. Lee, and H-K. Lee, "Detection of Copy-Rotate-Move Forgery Using Zernike Moments," Information Hiding 2010, Lecture Notes in Computer Science 6387, Springer-Verlag Berlin Heidelberg, p. 51–65, 2010.

[7] X. Feng, I.J. Cox, and G. Doerr, "Normalized energy density-based forensic detection of resampled images," IEEE Transactions on Multimedia, Vol. 14(3), pp. 536-545, 2012.

[8] J.F. O'brien and H. Farid, "Exposing photo manipulation with inconsistent reflections," ACM Trans. Graph., vol. 31(1), pp. 4:1-4:11, 2012.

[9] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, and G. Serra, "A SIFT-based forensic method for copy-move attack detection and transformation recovery," IEEE Trans. Information Forensics and Security, vol. 6(3), pp. 1099-1110, 2011.

[10] P. Kakar and N. Sudha, “Exposing Postprocessed Copy Paste Forgeries Through Transform-Invariant Features,” IEEE Trans. Information Forensics and Security, vol. 7(3), pp. 1018-1028, 2012.

[11] S. Bravo-Solario and A. K. Nandi, “Passive Method for Detecting Duplicated Regions Affected by Reflection, Rotation and Scaling,” European Signal Processing Conference, Glasgow, Scotland, 2009.

[12] Li, G., Wu, Q., Tu, D., Sun, S., “A Sorted Neighborhood Approach For Detecting Duplicated Regions in Image Forgeries based on DWT and SVD”, IEEE International Conference on Multimedia and Expo (ICME'07), pp. 1750-1753, 2007.

[13] Z. He, W. Lu, W. Sun, & J. Huang, “Digital image splicing detection based on Markov features in DCT and DWT domain,” Pattern Recognition, 45(12), pp. 4292-4299, 2012.

[14] J. G. Daugman, “Two-dimensional spectral analysis of cortical receptive field profiles”, Vis. Res., vol. 20, pp. 847-856, 1980.

[15] S. Zehan, G. Bebis, and M. Ronald, “Monocular precrash vehicle detection: features and classifiers,” IEEE Trans. Image Processing, vol. 15, pp. 2019-2034, 2006.

[16] M. Hussain, S. Khan, G. Muhammad, I. Ahmed, and G. Bebis, “Effective extraction of Gabor features for false positive reduction and mass classification in mammography,” Appl. Math. Inf. Sci. 8(1L), pp. 397-412, 2014.

[17] N. Ahmed, T. Natarajan, and K. R. Rao. "Discrete Cosine Transform," IEEE Transactions on Computers, vol. 23, pp. 90-93, 1974.

[18] Sun, Y., Todorovic, S., Goodison, S., “Local Learning Based Feature Selection for High Di-mensional Data Analysis”, IEEE Trans. Pattern Analysis and Machine Intelligence. 32 (9), pp. 1610-1626, 2010.

[19] Chang, C. C., Lin, C. J., LIBSVM - a library for support vector machine, 2010. down-loadable at http://www.csie.ntu.edu.tw/~cjlin/libsvm

[20] G. Muhammad, M. H. Al-Hammadi, M. Hussain, and G. Bebis, “Image forgery detection using steerable pyramid transform and local binary pattern", Machine Vision and Applications, DOI: 10.1007/s00138-013-0547-4, 2014.

[21] M. H. Al-Hammadi, G. Muhammad, M. Hussain, and G. Bebis, “Curvelet transform and local texture based image forgery detection,” International Symposium on Visual Computing (ISVC'13), Crete, Greece, July 29-31, 2013; G. Bebis et al. (Eds.): ISVC 2013, Part II, LNCS 8034, pp. 503–512, 2013.

[22] G. Muhammad, “Multi-scale local texture descriptor for image forgery detection,” IEEE International Conference on Industrial Technology (ICIT), pp. 1146-1151, Cape Town, South Africa, February 2013.

[23] M. Hussain, G. Muhammad, S. Q. Saleh, A. M. Mirza, and G. Bebis, “Image forgery detection using multi-resolution Weber local descriptors,” Eurocon2013, pp. 1570- 1577, Zagreb, Croatia, July 2013.

[24] Y. Zhang, C. Zhao, Y. Pi, and S. Li, "Revealing Image Splicing Forgery Using Local Binary Patterns of DCT Coefficients," in Communications, Signal Processing, and Systems. vol. 202, pp. 181-189; Q. Liang, W. Wang, J. Mu, J. Liang, B. Zhang, Y. Pi, and C. Zhao, Eds., ed: Springer New York, 2012.

[25] W. Wei, D. Jing, T. Tieniu, “Image tampering detection based on stationary distribution of Markov chain,” IEEE Intl. Conference on Image Processing (ICIP’10), pp. 2101-2104, 2010.