Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 58 (2015) 76 – 83

Procedia Computer Science

Second International Symposium on Computer Vision and the Internet (VisionNet'15)

Image forgery detection based on Gabor Wavelets and Local Phase Quantization

Meera Mary Isaac[a]*, M Wilscy[b]

[a]*Department of Computer Science,University of Kerala, Kariavattom, Trivandrum, 695581, India*
[b]*Department of Computer Science,University of Kerala, Kariavattom, Trivandrum, 695581, India*

Abstract

Image Forgery detection has become a hot area of research as a result of the increasing number of forged images circulating around in the Internet and other social media and due to the legal and social issues that they are creating. The key problem faced by the researchers is to categorize an image as forged or authentic and to localize the forgery. Several methods were proposed, but a proper method which can accurately detect image forgery is yet to be invented. Here, we propose a novel image forgery detection technique by taking texture information of the image as a distinguishing feature. The method relies on Gabor wavelets and Local Phase Quantization (LPQ) which can extract relevant texture features which are fed as input to a Support Vector Machine for classification. The results indicate an accuracy of over 99% on both CASIA v1 and the DVMM color dataset. It outperforms similar state-of-art methods in solving image forgery detection.

Peer-review under responsibility of organizing committee of the Second International Symposium on Computer Vision and the Internet (VisionNet'15)

Keywords: Image forensics; Gabor Wavelets; Local Phase Quantization; SVM classifier.

1. Introduction

The advancement of image processing technology has made images an integral part of our daily lives. They have helped images to migrate from canvas and papers to cameras, computers and mobile devices. Recently with the advent of sophisticated image processing software (Photoshop, GIMP etc.) and image capturing devices (cameras

* Corresponding author. Tel.: +91-9446516190.
E-mail address: meerathu@gmail.com

Peer-review under responsibility of organizing committee of the Second International Symposium on Computer Vision and the Internet (VisionNet'15)
doi:10.1016/j.procs.2015.08.016

etc.), images have become much easier to be captured, stored and edited. Although image editing software are a boon to our society, there is always an other side where a wrongfully edited image, i.e. a forged one, can become a catalyst for raising serious social issues. For example, a forgery which is performed by editing an image which has to be presented as a proof in court can mislead a court of law. This forces a strong need to correctly detect and localize image forgeries.

Digital image forensics[1] is a prominent and emerging research field whose aim is to validate the authenticity of images by using suitable techniques which can detect and localize image forgeries. Image Forensics is divided into two categories: active (intrusive) and passive (non-intrusive). Active forgery detection methods (digital watermarking[2], digital signatures[3]) inserts a pre-computed code as a part of the image data before it is transferred to the outside world. At the receiving side this code is verified with the original inserted code for authenticity. The major drawback of this method is the requirement of special tools to embed the pre computed code as a part of the image before it is sent out. The more popular technique is the blind image forgery detection method where a priori information like watermark etc. is absent in the forged image. Some technique which distinguish forged images from its non-forged version like the statistical discrepancies, change in sensor noise pattern, change in lighting direction etc. are examined for clues which can lead to traces of forgery.

Image Forgery itself is of two types: cloning (copy-move) and splicing. Copy-move forgery is performed by replacing a part of the given image by another portion which is taken from the same image. In image splicing, the copied region and the pasted region belongs to a different images. The purpose of the image forgery is to duplicate or conceal a certain object into an image or to make false propaganda[4]. Forging an image is usually accompanied by post-processing operations like JPEG compression, adding noise and image blurring or geometric operations such as scaling, shifting and rotation increases the detection tasks difficult. Copy-move forgery detection methods can be block-based or key point based. A block-based method[5, 6], divides the image into fixed sized units for which a suitable feature is identified. This feature can be used for comparison assuming that a forged block with the same feature values will be repeated within the same image. A key-point based method[7] identifies specific key-points within an image and analyze features from these key-points which is used for similarity checking. A forgery detection method detects and outputs an image as forged or authentic[4, 8] or it detects and localizes the forgery.

In this work, a passive technique for image forgery detection is proposed for classifying the input image as forged or not. The proposed method can detect the presence of any type of forgery i.e. copy-move or splicing on the image and is based on Gabor Wavelets[9] and Local Phase Quantization(LPQ)[10]. In this method, Gabor Wavelet Transform (GWT) at different scales and orientation is applied on the chroma component of the input image. Local Phase Quantization values are obtained for each of the Gabor images (sub bands) from the first step. The LPQ values from various sub bands obtained are concatenated to generate a single feature vector which is fed as input to the Support Vector Machine (SVM) for classification. This forgery detection method is evaluated on two publically available benchmark datasets for image forgery detection: Casia v1.0[11] and DVMM (colour)[12]. Our experimental results reveals a better performance across the datasets than other state-of-the-art methods. The rest of this paper is arranged as follows. Section 2 gives a detailed literature review in this field. Section 3 describes the image forgery detection system which is proposed in detail. The experimental results and analysis are given in Section 4. Finally, Section 5 summarizes the conclusion.

2. Review of related researches

Passive image forgery detection mechanisms have gained much popularity among the research community as they are simpler and do not require any explicit information (like water mark, digital signature etc.) about the image. Among passive techniques, the most popular are the copy-move forgery detection methods. Fridrich et al.[6] used discrete cosine transformation (DCT) for obtaining feature vectors from overlapping image blocks which was followed by a similarity checking using block matching. Popescu and Farid[5] used Principal Component Analysis (PCA) for representing overlapping image blocks. Luo et al.[13] extracted intensity features from image blocks which are robust against stronger attacks and post-processing operations like jpeg compression, blurring etc. Myrna et al. [14]

used phase correlation and log-polar coordinates to identify and locate copy – move forgery. The methods discussed above are block based which are complex in terms of time and space. Key point based methods are much efficient and require less computation time. Huang et al.[15] and Amerini et al.[7] detected cloned areas in images using Scale Invariant Feature Transform (SIFT). Both methods were robust against post-processing operations. Methods based on SURF[16] and ORB[17] could also detect cloned regions with translation, scaling and rotation.

Image forgery detection techniques which classify images as forged or authentic extract features from training image sets and use this information to perform classification. A method for detecting image splicing was identified by Zhao et al.[8] which used gray level run length run number (RLRN) vectors in chroma channel as the feature vector. They attained an accuracy of 94.7% on CASIA v1dataset using SVM as classifier. Muhammad et al.[4] developed a method using Steerable Pyramid Transform, Local Binary Pattern and SVM for image forgery detection. It is robust across various datasets and could detect both spliced and copy-move forged images. Hussain et al.[19] identified Weber Local Descriptor (WLD) as prominent feature for detecting image forgery and attained an accuracy of 96.2% on CASIA v1dataset. Al Hammidi et al. [20] used Curvelet Transform and Local Binary Pattern as features to detect different types of image forgeries. They obtained an accuracy of 93.4% with Casia v1 dataset. The proposed method using Gabor Wavelet transform and LPQ is explained in the following section.

3. Gabor and LPQ based image forgery detection system

The aim of our work is to identify forged images from a given set of input images. For this purpose, we extract texture features from the input image for classification, assuming that image forgery disturbs the texture information of an image. The texture features can be best modeled using Gabor wavelets which is capable of decomposing an image into several sub bands having different scales and orientation. This results in a collection of Gabor images for each scale and orientation. A Local Phase Quantization operator is applied to each of the Gabor images to obtain a blur invariant local texture information. Figure 1 shows the block diagram of the proposed method for image forgery detection.

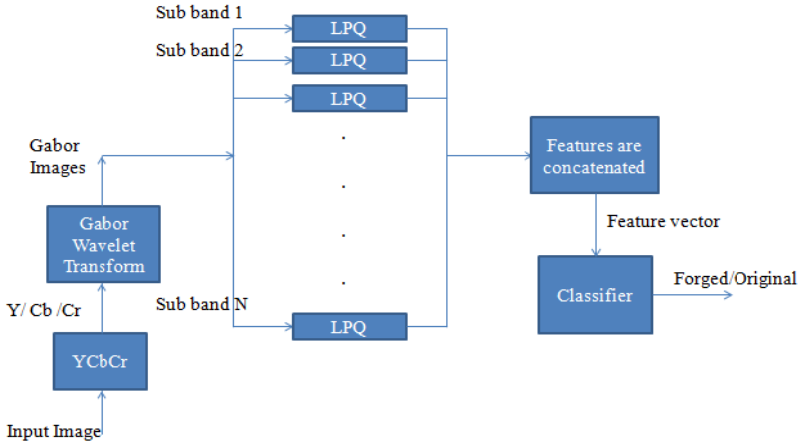

Figure 1. Block diagram of the proposed method

3.1. *Pre-processing*

Given a colour image, it is converted to YCbCr color space. Here Y is the luminance component and Cb and Cr are the chrominance components. A forged image can be thought of as an image with some hidden information related to forgery within it. This hidden information in the form of irregular edges which occur during a copy-move operation or an image splicing operation can be better detected in chrominance channels[8]. So in this

method we concentrate on one of the chrominance channel, Cr alone. Cb can also be considered for experiments. The RGB to YCbCr conversion using the Rec. BT.709 is performed using equation 1.

$$\begin{bmatrix} Y \\ Cb \\ Cr \end{bmatrix} = \begin{bmatrix} 0.2126 & 0.7152 & 0.0722 \\ -0.1146 & -0.3854 & 0.5 \\ 0.5 & -0.4542 & -0.0458 \end{bmatrix} . \begin{bmatrix} R \\ G \\ B \end{bmatrix} \quad (1)$$

Here Y denotes the brightness component and Cb and Cr stands for the blue(B) minus brightness(Y) component and the red(R) minus brightness(Y) component respectively. R, G and B are the Red, Green and Blue components of the input image.

3.2. Gabor Wavelet Transform

In the second step, a Gabor Wavelet Transform (GWT) is applied on the Cr channel. GWT is being widely used in computer vision[21], texture analysis [22] and face recognition[23]. It is a powerful image decomposition method which possess multi-scale and multi-orientation properties. GWT has an optimal resolution in both frequency and spatial domain [22]. A Gabor filter is a Gaussian kernel which is modulated by an oriented sinusoidal wave. The 2D Gabor filter function, $\psi_{\mu,\nu}(z)$ is defined as in equation 2.

$$\psi_{\mu,\nu}(z) = \frac{||k_{\mu,\nu}||^2}{\sigma^2} e^{-\frac{||k_{\mu,\nu}||^2 z^2}{2\sigma^2}} \left[e^{ik_{\mu,\nu} z} - e^{-\frac{\sigma^2}{2}} \right] \quad (2)$$

Here z = I(x, y) where the horizontal and vertical coordinates are represented by x and y respectively; The scale and orientation of the filter kernel is represented by ν and μ. $\|\cdot\|$ represents the norm operator; σ represents the ratio of the Gaussian window width to the wavelength which is the standard deviation of Gaussian window of the filter kernel. $k_{\mu,\nu}$ denotes the wave vector which is equal to $k_\nu e^{i\varphi\mu}$ here $k_\nu = \frac{k_{max}}{f^\nu}$ and $\varphi\mu = \frac{\pi\mu}{8}$, here 8 different orientations are chosen. The maximum frequency is denoted by k_{max} and f^ν gives the spatial frequency between kernels.

The proposed method use 5 scales and 8 orientation of Gabor wavelets which yields a total of 5*8 i.e. 40 Gabor images for each input image. We use $\nu = \{0,1,2,3,4\}$ and $\mu = \{0,1,2,3,4,5,6,7\}$, $\sigma = 2\pi$, $k_{max} = \frac{\pi}{2}$ and $f = \sqrt{2}$ [10, 12-14]. In order to obtain a Gabor image, convolve input image I and the Gabor kernel $\psi_{\mu,\nu}$ as follows:

$$G_{\mu,\nu}(z) = I(z) * \psi_{\mu,\nu}(z) \quad (3)$$

Convolution is a local operator which is used to multiply two arrays of numbers of same dimensionality to produce a resultant array. The input image I and the Gabor kernel $\psi_{\mu,}$ which are the two input arrays, are convolved to obtain the resultant array $G_{\mu,\nu}(z)$.

The entire Gabor image set obtained for a given input image I (z) is:

$$O = \{G_{\mu,\nu}(z) : \mu \varepsilon \{0,1,2,3,4,5,6,7\}, \nu \varepsilon \{0,1,2,3,4\}\}$$

$G_{\mu,\nu}(z)$ is a complex function with a real part $\boldsymbol{R}\{G_{\mu,\nu}(z)\}$ and an imaginary part $\boldsymbol{I}\{G_{\mu,\nu}(z)\}$. The magnitude of $G_{\mu,\nu}(z)$,

$$\|G_{\mu,\nu}(z)\| = \sqrt{(\boldsymbol{R^2}\{G_{\mu,\nu}(z)\} + \boldsymbol{I^2}\{G_{\mu,\nu}(z)\}} \quad (4)$$

The magnitude $\|G_{\mu,\nu}(z)\|$ is used for representing the features.

3.3. Local Phase Quantization

In the third step, each of the 40 Gabor images obtained for every input image is taken and the LPQ operator is applied to extract a blur and illumination invariant local texture pattern. LPQ was proposed by Ojansivu and Heikkila[10] and it is based on the blur invariance property of Fourier phase spectrum. LPQ takes a rectangular neighbourhood around every image pixel to calculate the 2D Short Term Fourier Transform(STFT) which gives the local phase information of the image.

Image blurring is a method to lower the edge content of the image to make a smooth transition from one colour to another. Blurring of an image in spatial domain, i.e. the blurred image g(x) is represented as a convolution between the original image f(x) and a point spread function (PSF) h(x). In frequency domain this is represented as:

$$G(\mathbf{u}) = F(\mathbf{u}) \,.\, H(\mathbf{u}) \tag{5}$$

G (**u**), F (**u**) and H (**u**) are the Discrete Fourier Transforms (DFT) of the blurred image, original image and the PSF respectively. **u** denotes the set of vector coordinates $[u , v]^T$. The magnitude and phase components can be separated and represented as follows:

$$\begin{aligned} &|G(\mathbf{u})| = |F(\mathbf{u})| \;.\; |H(\mathbf{u})| \text{ and} \\ &\angle G(\mathbf{u}) = \angle F(\mathbf{u}) + \angle H(\mathbf{u}) \end{aligned} \tag{6}$$

Here $\angle G(\mathbf{u})$ represents the phase of G(u).

When the PSF of the function is centrally symmetric, its Fourier Transform H is always real valued i.e.

$$\angle H(u) = \begin{cases} 0 \; if \; H(u) \geq 0 \\ \pi \; if \; H(u) < 0 \end{cases} \tag{7}$$

The equation 7 shows the blur invariance property i.e. $\angle G(\mathbf{u}) = \angle F(\mathbf{u})$ when H(u) =0. LPQ extracts the phase information by examining the local neighbourhood N_x of size M×M at each pixel position x of image f(x):

$$F(u, x) = \sum_{y \in N_x} f(x - y) e^{-j2\pi u^T y} = w_u^T f_x \tag{8}$$

Here w_u is the basis vector for 2-D DFT at frequency u and f_x is a vector containing all the M^2 samples from N_x.

The local Fourier coefficients are computed at four frequency points $u1 = [a, 0]^T$, $u2 = [0, a]^T$, $u3 = [a, a]^T$, and $u4 = [a, -a]^T$, where a is the first frequency below the first zero crossings of H(u) that satisfies $\angle G(u) = \angle F(\mathbf{u})$ for all H(u) ≥0. For each pixel position this results in a vector:

$$F_x^c = [F(u1, x), F(u2, x), F(u3, x), F(u4, x)] \tag{9}$$

The phase information in the Fourier coefficients is recorded by observing the signs of the real and imaginary parts of each component in F_x^c. This is performed using a simple scalar quantizer $q_j(x) = 1$, if $g_j(x) \geq 0$ and 0 otherwise where $g_j(x)$ is the j^{th} component of the vector $G_x = [\text{Re}\{F_x^c\}, \text{Im}\{F_x^c\}]$. The resulting quantized coefficients $q_j(x)$ are represented as integer values between 0-255 using binary coding $b = \sum_{j=1}^{8} q_j \; 2^{j-1}$. Histogram of the above integer value is used as a feature vector.

3.4. Feature fusion and Classification

The features obtained from step 3 are fused to form a single feature vector i.e. for each input image, we get a total of 40 Gabor images and for each Gabor image we get a 256 dimensional LPQ feature. A single feature vector is formed by concatenating the LPQ values of the 40 Gabor images for each image input. These features are then

normalized and fed into an SVM classifier. We use the Libsvm[24] library incorporated in the WEKA[25] (Weika Environment for Knowledge Analysis) for classification purpose.

SVM or Support Vector Machine is a supervised learning system developed by Cortes and Vapnik. It helps to separate the test samples into two classes (in our case forged is denoted by +1 and authentic is denoted by -1) by predicting its label (+1 or -1) with the help of training samples which falls into one of the category +1 or -1. SVM tries to build an optimal hyper plane with maximum margin which can separate the +1 and -1 samples in Euclidean space to ensure a high generalization performance. The real world data may not be linearly separable, in such cases, we use the kernel trick (using a kernel function) to transform the original space to a high dimensional space where the problem becomes linear. Here in our experiment, we have used the RBF (Radial Basis Function) kernel for this purpose.

WEKA is open source software written in Java and developed by university of Waikato, New Zealand. It has a collection of machine learning algorithms for data mining problems which includes algorithms for data pre processing, classification, clustering, association etc. WEKA LibSVM library is the LibSVM incorporated into the WEKA toolkit.

4. Experimental Results

The proposed method is evaluated on two benchmark datasets for image forensics: CASIA TIDE v1 and DVMM color. CASIA TIDE v1consists of 800 authentic images and 921 tampered images all of JPEG format. All the images are of size 384×256 pixels and fall into 8 different categories, some of which are animal, texture, plant etc. The forged images were created from the authentic images by randomly choosing images from different categories and performing copying and pasting operations. Sometimes, the copied part is rotated or scaled before the pasting operation. Out of the 921 tampered images, 459 are created by performing copy-move forgery and the rest by image splicing operation. The DVMM color image dataset consists of 183 authentic and 180 spliced images all in TIFF format. All the images present in this dataset are spliced images having a size of 1152× 768.

The performance of the proposed method is evaluated using the metrics, True Positive Rate (TPR), False Positive Rate (FPR), Accuracy (ACC) and area under the ROC curve (AUC), which are evaluated as per the following formulae.

$$TPR = (TP \div (TP + FN)) \tag{10}$$

$$FPR = (FP \div (FP + TN)) \tag{11}$$

$$ACC = 100 \times (TP + TN) \div (TP + TN + FN + FP) \tag{12}$$

Where True Positive (TP) is the number of forged images which are classified as forged images, False Negative (FN) is the number of forged images which are wrongly classified as authentic images, True Negative (TN) is the number of authentic images which are correctly classified as authentic images and False Positive (FP) is the number of authentic images which are wrongly classified as forged images. Accuracy (ACC) is the total percentage of correctly classified images. AUC is the area under the ROC curve whose value falls in the range 0 to 1. ROC curve represents the performance of a two-class classifier with respect to change in its discriminating threshold value. The above measures are calculated after performing a ten-fold cross validation of the input data. In ten-fold cross validation, we randomly divide the forged images and the authentic images into ten equal parts each. Ten rounds of cross-validation are performed and for each round we use one of the ten parts for validation and the remaining parts for training. On completing the ten rounds all ten parts are evaluated. Training and testing sets are disjoint in each round. The average accuracy over ten rounds is calculated to obtain the final cross-validation accuracy.

Table 1. illustrates the performance of the proposed method on CASIA TIDE v1 and DVMM (Color) datasets. It can be noted from the table that on both the datasets the accuracy rate is over 99% which clearly indicates the

Table 1. Performance of image forgery detection in Cr channel with two datasets using the proposed method

Dataset	TPR	FPR	ACC	AUC
CASIA TIDE v1	0.998	0.002	99.825	0.998
DVMM (Color)	0.994	0.011	99.449	0.995

aptness and ability of the features identified in the proposed method to clearly distinguish the forged images. We can also infer that texture features are indeed good candidates for forgery detection. Figure 2 shows the comparison of the accuracy of the proposed method with the current state-of-the-art methods. The results were obtained from corresponding papers of these methods. A summary of all the methods compared is given in Section 2. It is evident that our method is far superior compared to others in this category.

5. Conclusion

Image forgery detection based on Gabor Wavelet transform and Local Phase Quantization is proposed. The experiments are performed by taking the Cr channel in YCbCr color space and applying Gabor and LBP on the Cr image. The feature vector thus obtained is given as input to the SVM for classification. The method is tested on CASIA v1 and DVMM(color) datasets. The results of the proposed method shows that it outperforms the state-of-the-art methods in detecting image forgery with an accuracy of over 99%. One drawback of this method is the large diamensionality of the feature vector which leads to a larger processing time. This problem can be solved by performing dimensionality reduction of the present feature set, which we plan as a future enhancement to this work.

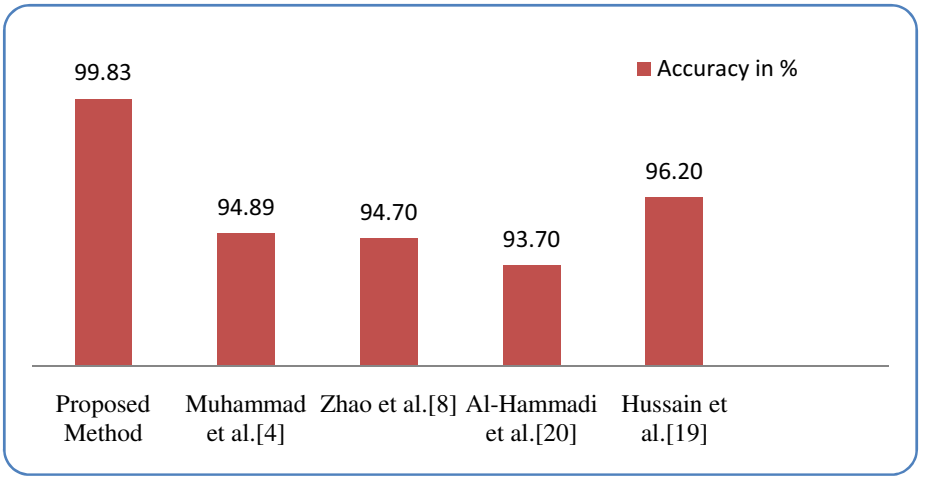

Figure 2. The Accuracy(%) of the proposed method compared to other methods using **CASIA v1** dataset.

References

1. Redi JA, Taktak W, Dugelay J-L. Digital image forensics : a booklet for beginners. Multimed Tools Appl Oct 2010. 2010;
2. Lu C-S, Liao H-Y. Multipurpose watermarking for image authentication and protection. Image Process IEEE Trans On 2001 ;10(10):1579–92.
3. Lu C-S, Liao H-Y. Structural digital signature for image authentication: an incidental distortion resistant scheme. Multimed IEEE Trans On. 2003;5(2):161–73.
4. Muhammad G, Al-Hammadi MH, Hussain M, Bebis G. Image forgery detection using steerable pyramid transform and

local binary pattern. Mach Vis Appl. 2014; 25(4):985–95.
5. Popescu AC, Farid H. Exposing digital forgeries by detecting duplicated image regions. Dept Comput Sci Dartm Coll Tech Rep TR2004-515. 2004
6. Fridrich AJ, Soukal BD, Lukáš AJ. Detection of copy-move forgery in digital images. in Proceedings of Digital Forensic Research Workshop. Citeseer; 2003.
7. Amerini I, Ballan L, Caldelli R, Del Bimbo A, Serra G. A sift-based forensic method for copy–move attack detection and transformation recovery. Inf Forensics Secur IEEE Trans On. 2011;6(3):1099–110.
8. Zhao X, Li J, Li S, Wang S. Detecting digital image splicing in chroma spaces. Digital Watermarking. Springer; 2011. p. 12–22.
9. Lee TS. Image representation using 2D Gabor wavelets. Pattern Anal Mach Intell IEEE Trans On. 1996;18(10):959–71.
10. Ojansivu V, Heikkilä J. Blur insensitive texture classification using local phase quantization. Image and signal processing. Springer; 2008. p. 236–43.
11. CASIA Tampered Image Detection Evaluation Dataset. Available from: http://forensics.idealtest.org:8080/
12. Hsu Y-F, Chang S-F. Detecting image splicing using geometry invariants and camera characteristics consistency. Multimedia and Expo, 2006 IEEE International Conference on. IEEE; 2006. p. 549–52.
13. Luo W, Huang J, Qiu G. Robust detection of region-duplication forgery in digital image. Pattern Recognition, 2006 ICPR 2006 18th International Conference on. IEEE; 2006. p. 746–9.
14. Myrna AN, Venkateshmurthy MG, Patil CG. Detection of region duplication forgery in digital images using wavelets and log-polar mapping. Conference on Computational Intelligence and Multimedia Applications, 2007 International Conference on. IEEE; 2007. p. 371–7.
15. Huang H, Guo W, Zhang Y. Detection of copy-move forgery in digital images using SIFT algorithm. Computational Intelligence and Industrial Application, 2008 PACIIA'08 Pacific-Asia Workshop on. IEEE; 2008. p. 272–6.
16. Shivakumar BL, Baboo LDSS. Detection of region duplication forgery in digital images using SURF. IJCSI Int J Comput Sci Issues. 2011;8(4).
17. Zhu Y, Shen X, Chen H. Copy-move forgery detection based on scaled ORB. Multimed Tools Appl. 2015;1–13.
18. Muhammad G, Al-Hammadi MH, Hussain M, Mirza AM, Bebis G. Copy move image forgery detection method using steerable pyramid transform and texture descriptor. EUROCON, 2013 IEEE. IEEE; 2013. p. 1586–92.
19. Hussain M, Muhammad G, Saleh SQ, Mirza AM, Bebis G. Image forgery detection using multi-resolution Weber local descriptors. EUROCON, 2013 IEEE. IEEE; 2013. p. 1570–7.
20. Al-Hammadi MH, Muhammad G, Hussain M, Bebis G. Curvelet transform and local texture based image forgery detection. Advances in Visual Computing. Springer; 2013. p. 503–12.
21. Hamamoto Y, Uchimura S, Watanabe M, Yasuda T, Mitani Y, Tomita S. A Gabor filter-based method for recognizing handwritten numerals. Pattern Recognit. 1998;31(4):395–400.
22. Jain AK, Farrokhnia F. Unsupervised texture segmentation using Gabor filters. Systems, Man and Cybernetics, 1990 Conference Proceedings, IEEE International Conference on. IEEE; 1990. p. 14–9.
23. Shen L, Bai L. A review on Gabor wavelets for face recognition. Pattern Anal Appl. 2006; 9(2-3):273–92.
24. Chang C-C, Lin C-J. LIBSVM: a library for support vector machines. ACM Trans Intell Syst Technol TIST. 2011;2(3):27.
25. Hall M, Frank E, Holmes G, Pfahringer B, Reutemann P, Witten IH. The WEKA data mining software: an update. ACM SIGKDD Explor Newsl. 2009; 11(1):10–8.