Indian Journal of Science and Technology, *Vol 9(22), DOI: 10.17485/ijst/2016/v9i22/89227, June 2016*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

RST Invariant Image Forgery Detection

Gulivindala Suresh[1]* and Chanamallu Srinivasa Rao[2]

[1]Department of ECE, JNTUK University College of Engineering, Kakinada - 533003, Andhra Pradesh, India; suresh.g@gmrit.org

[2]Department of ECE, JNTUK University College of Engineering, Vizianagaram - 535003, Andhra Pradesh, India; ch_rao@rediffmail.com

Abstract

Background/Objectives: Copy-Move Forgery Detection (CMFD) is a very prevalent approach used to detect copy and pasted portions of the same image. The copied portion is rotated, flipped or scaled. The detection method should be invariant to rotation, scaling and translation. Many CMFD methods came into existence; however, some methods fail to withstand attacks such as Contrast adjustment, Gaussian blur and JPEG Compression. Although the methods are able to resist the attacks, they are computationally complex. This paper proposes a Rotation, Scaling, Translation (RST) invariant image forgery detection. **Methods**: Local Binary Pattern (LBP) is applied on the low frequency content of Discrete Wavelet Transform (DWT) decomposed image for feature extraction. **Findings**: The proposed method is invariant to rotation, scaling and translation attacks on the pasted portions of the image and able to resist post-processing attacks and has low computational effort. It is evaluated qualitatively and quantitatively on a CASIA database. Morphological operations are performed to reduce the false alarms. The correct detection ratio is in the range of 80% to 99% and false detection ratio in the range of 7% to 30%. **Applications**: There is a great demand to detect the forgery, which aids in the digital forensic analysis, in legal document substantiation, and various other fields.

Keywords: Computational Complexity, Discrete Wavelet Transform, Image Forgery, Local Binary Pattern, Localization

1. Introduction

The swift growth of digital image editing software leads to the creation of large amount of doctored images spreading in our daily lives. Sophisticated imaging devices and user friendly photo-editing applications ease the tampering process of digital images. The digital image credibility has a significant role in several applications: surveillance systems, forensic analysis, journalism and criminal examination[1]. The image forgery detection can be achieved in two ways: one is active approach and another is a passive approach. In the first approach, the forgery identification involves pre-processing of original image earlier to its usage. Digital image watermarking and signatures also plays a key role in detecting and localizing the forgeries in the image. The drawback of signature or watermarking technology is to embed a specific signature or watermark in the cover image. That is pre-processing of the media data is required, which restricts the scope of their usage[2]. The passive method depends on image statistical characteristics or features.

Copy-Move tampering is a very common method of tampering digital image where in some portion of an image is copied and pasted at some other location in the same image. In general, this is done with intent to conceal a region or an object in the image. The copied portions are within the image, so the changes in texture, variations in intensity or any statistical property may match with the remaining portion of the original image. Hence, it is challenging for detecting the forged portion based on HVS[3]. An exhaustive search can be used to identify the significant features of copied and pasted portions on

*Author for correspondence

(a) The original image. (b) The forged image.

Figure 1. Copy Move Forgery.

the tampered image. This mechanism needs more time for detection and is computationally complex[4]. Therefore, similarity measure can be used on the identical image regions for detecting the forgery successfully[4]. Figure 1(a) and 1(b) illustrates Copy move forgery.

In [5] designed an effective CMFD algorithm based on DCT coefficients as features. But it has failed to identify duplicated regions when the image is distorted by additive noise. The CMFD method proposed in [6] can withstand additive noise. This method is based on Principal Component Analysis (PCA) and differs mainly in representing the overlapped image blocks. It is an improved one when compared to[5] in terms of noise resistance but with low detection accuracy. In [7] proposed a method to ease the overall effort of computation. DWT is used to decompose the image to obtain low frequency components (*LL*), mid-frequency components (*LH*, *HL*) and high frequency components (*HH*). The low frequency content (*LL* band) is chosen as much information is available and SVD is employed over the fixed sized blocks of band. Since the number of blocks are reduced the overall process has speeded up.

In [4] discussed a CMFD technique to overcome the computational complexity. This algorithm uses DWT for feature extraction and the replicated portions are recognized with the help of Phase Correlation parameter. In [8], a method to reduce the processing time by using multi-hop jump (MHJ) technique to jump over certain "unnecessary testing blocks" (UTB) is discussed. Firstly, DWT is applied on the image and Fast Walsh Hadamard Transform (FWHT) is used on overlapping blocks of equal size. Finally, the use of MHJ technique improves the range matching. The method proposed in [9] is able to identify with small feature vector and improved the performance but was unsuccessful in identifying multiple copy move forgeries. In [10], discussed a passive technique using dyadic wavelet transform (DyWT) and it provides improved performance than DWT. In [11] established a technique using DWT and SIFT to identify copy-move forgeries. In [12] systematically used DWT with DCT to identify the forged portion. Even though the technique is capable of handling various clone forgery, the time-complexity is more.

Other than Moments[13–15], Local Binary Pattern (LBP) can be exploited for detecting image forgeries. In [16] developed a technique, in which the Local Binary Pattern is used to obtain textural features and the features are sorted lexicographically. The duplicated regions are recognized by calculating the similarity of textural features. The LBP operator scans the forged image, the number of overlapping blocks are more in number, results in a high computational effort. In [22], addressed this problem by applying LBP on *LL* band of DWT decomposed image. But, only qualitative evaluation is proposed.

Our proposed method used DWT and LBP is similar to [22] but quantitative evaluation is performed to calculate CDR and FDR. The proposed method is invariant to rotation, scaling, translation and also to post-processing attacks. The use of morphological operators such as erosion and dilation minimized the false alarms.

2. Proposed Method

The vital component of any CMFD technique is to detect the copy-pasted portions in a given image by identifying duplicated regions in that image. As the forged portion can be of different shape and size, it is certainly difficult to compare every pair of region with all possible shapes and dimensions. In order to reduce the number of blocks, LBP features are obtained from LL band of the image.

The process description of our method is given in Figure 2. Firstly, the forged image D of size is transformed to gray scale image I by the following equation (1).

$$I = 0.2989 \times R + 0.5870 \times G + 0.1140 \times B \quad (1)$$

2.1 Discrete Wavelet Transform

Discrete Wavelet Transformation (DWT) decomposes at multilevel, which localize the signal both in space and frequency. This nature of localization leads to various useful applications like image feature extraction, data compression, denoising and so on[7,23]. The key idea to make use of DWT is to decrease the image size at each level, as DWT decomposes an image of $2^j \times 2^j$ size at the present scale L to $2^{j/2} \times 2^{j/2}$ size at the next scale L+1. The decomposition at a level, results in four down-sampled images. This down-sampled image contains low frequency components (LL), mid-frequency components (LH, HL) and high frequency components (HH). The LL band contains approximation

or coarse level coefficients and this (LL) band is used in further image decomposition. These obtained sub images are synthesized to reconstruct the original image.

In our method, the first level decomposed image is taken and the low frequency content (LL band) is chosen as much information is available in the band. The selection of LL band reduces ¾ of computational process.

2.2 Dividing into Fixed-size Blocks

In our method, the image under test is partitioned into fixed size $b \times b$ pixels which are overlapped blocks. Here, in order to detect the duplicated region accurately, the size of the block must be less than the duplicated region. As LL_{K-L} band is partitioned into fixed size blocks, the process of sliding will produce $(K-b+1)\times(L-b+1)$ overlapping blocks.

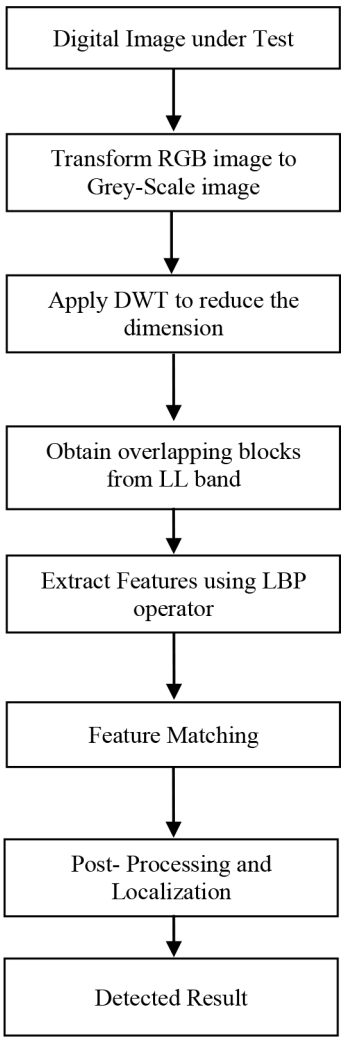

Figure 2. Flow diagram of the proposed method.

2.3 Features

Local Binary Pattern (LBP) is a spatial operator useful for describing the spatial structure of the grey images[17]. The texture T of a grey image is the joint distribution of the grey levels of P (P > 1) in a local neighbourhood. The texture T can be calculated using the following equation.

$$T = t\left(g_c, g_1, ..., g_{P-1}\right) \tag{2}$$

To obtain textural features at different scales, operators with varied sizes of local neighbourhoods are available and are illustrated in Figure 3. The symbol (P; R) defines pixel neighbourhood, P as number of pixels in that neighbourhood and R represents the radius of a circular neighbourhood. In[18], shown that for P=8 many uniform patterns of a rotated version are possible. Hence, a different pattern can be given as

$$LBP_{P,R}^{riu2} = \begin{cases} \sum_{P=0}^{P-1} s(g_P - g_C), \; if \; U(LBP_{P,R}) \le 2P+1 \\ P+1, \qquad\qquad otherwise \end{cases} \tag{3}$$

Where $LBP_{P,R}^{riu2}$ have P+2 textural features.

After operating with $LBP_{P,R}^{riu2}$, histogram of LL_{K-L} is given below.

$$H^{riu2}(m) = \sum_{i=1}^{K}\sum_{j=1}^{L} f(LBP_{P,R}^{riu2}(i,j), m), m \in [1, M] \tag{4}$$

$$f(x,y) = \begin{cases} 1, & x = y \\ 0, & otherwise \end{cases} \tag{5}$$

Where M is the number of $LBP_{P,R}^{riu2}$ independent values $P+2$. These $P+2$ values serve as the feature vector. In this work, using eq. (4) rotation invariant features are extracted for each fixed block and arranged them in a row. In similar approach, features are obtained for $(K-b+1)\times(L-b+1)$ blocks. All the features are sorted lexicographically and kept in the form of an array S where it consists of $(K-b+1)\times(L-b+1)$rows and $P+2$columns.

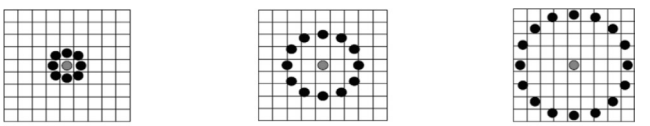

Figure 3. LBP for different neighbourhoods and sampling points.

2.4 Feature Set Matching

The duplicated blocks have similar features; the similarity metric among the features of all the rows is to be computed. Due to lexicographical sorting, only adjacent r rows are taken into account for matching. The related blocks with distance greater than b are considered for similarity measure using Euclidean distance.

The duplicated portion is identified accurately, by calculating the distance threshold T_d , similarity threshold T_S and r are precomputed. The duplicated block feature set available in the i^{th} row S_i, the distance for the adjacent r rows are calculated and the minimum distance designated by $D(i,\beta)$ [16].

$$D(i,\beta) = \min\left\{D(i,i+1), D(i,i+2), ..., D(i,i+r)\right\} \quad (6)$$

The obtained $D(i,\beta)$ is compared with similarity threshold T_S and if $D(i,\beta)$ is smaller than T_S then the corresponding blocks are treated as properly matched. The two corresponding blocks locations are stored. This process of similarity measure is repeated for all the rows of matrix. Initially detected pair of blocks are stored in a set σ.

2.5 Final Detection

The set σ consists of all the matched block pairs, the duplicated regions can be highlighted by marking the regions. For this, those locations are marked as white on black background in a binary image. This initial process consists of false alarms and those are eliminated by using morphological operators such as erosion and dilation. The erosion operator of size equal to block size is taken and is applied on the initial detection map. The marked patches on the initial detection map which are less than the block size are erased. The dilation operator is used to make the markings as large as its original size.

3. Experimental Results and Discussions

The affine attacks and other post-processing attacks such as JPEG compression, Contrast Variation and Gaussian blur are performed using Pixlr tool. The experimentation is carried out on CASIA database[19] with MATLAB R2013b. In the experimentation, the parameters P, R, r, T_S and T_d are taken as 24, 3, 30, 8.5 and 18 respectively. Initially, the forged image without attack is considered and the result is shown in Figure 4(a), Figure 4(b) and Figure 4(c).

a) Forged image b) Initial detection map c) Final result

Figure 4. CMFD using the proposed method without any attack.

3.1 Performance on Affine Operations

The proposed method can handle rotation, flipping, translation, and scaling operations. In the experimentation, the copied regions are subjected to affine operations prior to their placement in the target regions. It is obvious from the Table 1 that our method can effectively locate the tampered region even the copied portion is affected by affine operations. The copied portion is rotated either clockwise or anti-clockwise 90° and as well flipped horizontally or vertically. For all these rotation attacks, our method is able to detect and locate the forgery.

Similarly, the copied portion is scaled at scaling factors like 1.2, 1.1, 0.9 and 0.8 and pasted in the target region of the image. The qualitative analysis from Table 1 illustrates that our method can detect and locate the forgery. The false alarms are more for this attack even after post-processing.

3.2 Performance on Post-processing Attack

The proposed method is evaluated by disturbing the forged image with several post-processing attacks such as contrast variation, JPEG compression and Gaussian Blur. For contrast variation, the contrast of the CMF image is adjusted with different quantities –20, –10, +10 and +20.

In JPEG compression attack, the CMF image is compressed with 5 different quality factors 50, 60, 70, 80 and 90. In the case of Gaussian blur, the window size is varied from 3×3 to 11×11. The Table 2 illustrates the proposed method's robustness for post-processing attacks.

3.3 Quantitative Analysis

Similarly, the robustness of our method is further evaluated by calculating the parameters, Correct Detection Rate (CDR) and False Detection Rate (FDR) as given in [20]. The correct detection rate gives how accurately the tampered region is detected, whereas the FDR gives the amount of false alarms while detecting the tampered region. The values of *CDR* and FDR are presented in Table 3.

Table 1. Performance on affine operations.

Type of Attack	Forged image	Ground Truth	Initial Detection map	Final Result
Translation				
Left Rotate				
Right Rotate				
Flip Horizontal				
Flip Vertical				
Scaling 1.2				
Scaling 1.1				
Scaling 0.9				
Scaling 0.8				

$$CDR = \frac{|C_1 \cap C_2| + |M_1 \cap M_2|}{|C_1| + |M_1|} \quad (7)$$

$$FDR = \frac{|C_1 \cup C_2| + |M_1 \cup M_2|}{|C_1| + |M_1|} - CDR \quad (8)$$

where C_1 is the copy region, M_1 is the tampered region, while C_2 and M_2 are the detected copy region and detected tampered region respectively.

It is observed from the Table 3 that the CDR is high for all the post-processing attacks. For quality factor 50, the value of CDR is 0.8019 and as the quality factor increases the CDR also has increased. In practice, the quality factor of JPEG images is more than 50; hence our method is capable of handling JPEG compression. For the Gaussian blur attack, the CDR value ranges from 0.86 to 0.96 and has less effect on the tampered region detection. Similarly, our method shows that it can also handle contrast adjustment on the CMF image and this is possible with the exploit of LBP operator. The variation of detection ratio (DR) i.e. CDR and FDR for different post-processing attacks is plotted and is shown in the Figures 5–8.

Table 2. Robustness of the method for various post-processing attacks.

Type of Attack	Forged image	Ground Truth	Initial Detection map	Final Result
Contrast + 20				
Contrast +10				
Contrast -10				
Contrast-20				
JPEG QF-50				
JPEG QF-60				
JPEG QF-70				
JPEG QF-80				
JPEG QF-90				
Blur 3x3				
Blur 5x5				
Blur 7x7				
Blur 9x9				
Blur 11x11				

3.4 Comparative Analysis

The proposed method is compared to earlier works which used DWT, LBP or a combination of these and is given in Table 4. The results illustrate that the proposed method is comparable with works based on only LBP [16] and on DWT

Table 3. Robustness of the method in terms of CDR and FDR.

Type of Attack	CDR	FDR
Copy-Move	0.9970	0.1211
Rotate Left	0.9923	0.1406
Rotate right	0.9481	0.0724
Horizontal Flip	0.8804	0.3029
Vertical Flip	0.9003	0.2880
Scaling 1.2	0.9924	0.2957
Scaling 1.1	0.9211	0.3134
Scaling 0.9	0.9754	0.3779
Scaling 0.8	0.9709	0.3673
Contrast + 20	0.8749	0.2805
Contrast + 10	0.9027	0.2602
Contrast -10	0.9425	0.1590
Contrast-20	0.9630	0.1010
JPEG Quality Factor-50	0.8019	0.2034
JPEG Quality Factor-60	0.9048	0.3627
JPEG Quality Factor-70	0.9250	0.3067
JPEG Quality Factor-80	0.9578	0.3585
JPEG Quality Factor-90	0.9842	0.3680
Gaussian Blur 3x3	0.8631	0.1045
Gaussian Blur 5x5	0.9657	0.1855
Gaussian Blur 7x7	0.9602	0.2282
Gaussian Blur 9x9	0.9540	0.2247
Gaussian Blur 11x11	0.9496	0.2227

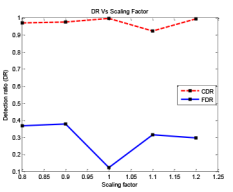

Figure 5. DR vs. scaling factor.

& FWHT [8] in terms of robustness and computational effort. The proposed method's computational effort is same as that of [8] but the proposed method is superior to [8] and [16] as it is robust to affine and post-processing attacks. The algorithm [16] used LBP on more number of blocks when compared to the proposed method. The [16] is robust to post-processing attacks only and not to affine operations, whereas our method is robust to post-processing and affine operations. In [21], the authors used SPT for image forgery detection, but failed in localization; the proposed

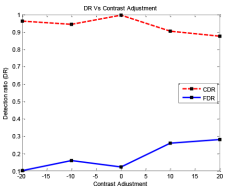

Figure 6. DR vs. contrast adjustment.

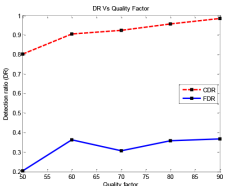

Figure 7. DR vs. quality factor.

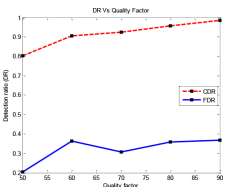

Figure 8. DR vs. blur mask size.

Table 4. Comparative analysis of the proposed method.

Algorithm	Feature representation	Number of overlapping blocks	Computational Effort	Feature size	Robust to Affine attacks
Bin Yang et al [8]	DWT & FWHT	57121	Low	64	No
Leida et al [16]	LBP (24,3)	245025	High	26	Rotation only
G.Muhammad et al [21]	SPT & LBP	245025	High	256	RST
Ch.S.Rao et al [22]	DWT & LBP (24,3)	57121	Low	26	Rotation only
Proposed Method	DWT & LBP(24,3)	57121	Low	26	RST

method overcomes this problem. In [22], effort is made to reduce the computational load when compared to [16] and can withstand rotation attack only. The proposed method is invariant to RST and post processing attacks.

4. Conclusions

A common and popular approach to tamper an image easily is Copy-move forgery. In order to reduce the computational effort only LL band is used in our method and robustness is evaluated based on LBP features. The good choice of both the thresholds can locate the duplicated portions even if the copied portion is affected by JPEG compression, contrast adjustment, blurring, region rotation and flipping. In the proposed method, the use of dilation and erosion morphological operators reduced the false alarms. The proposed method is invariant to affine operations, but the false alarms are more for scaling attack even after post-processing. The comparative analysis shows better performance when compared to other algorithms based on DWT, LBP or a combination of these.

5. References

1. Mahdian B, Stanislav S. A bibliography on blind methods for identifying image forgery. Signal Processing: Image Communication. 2010; 25(6):389–99.
2. Zhang J, Feng Z, Su Y. A new approach for detecting copy-move forgery in digital images. 11th Proceedings IEEE Singapore International Conference on Communication Systems, Guangzhou; 2008 Nov. p. 362–66.
3. Shivakumar BL, Baboo SS. Detecting copy-move forgery in digital images: a survey and analysis of current methods. Global Journal of Computer Science and Technology. 2010; 10(7):61–5.
4. Khan S, Kulakarni A. A reduced time complexity for detection of copy-move forgery detection using discrete wavelet transform. International Journal of Computer Applications. 2010; 6(7):31–6.
5. Fridrich J, Soukal D, Lukas J. Detection of copy-move forgery in digital images. Proceedings Digital Forensic Research Workshop, Cleveland, OH, USA; 2003 Aug. p. 1–10.
6. Popescu AC, Farid H. Exposing digital forgeries by detecting duplicated image regions, Darmouth College: USA; 2004.
7. Li G, Wu Q, Tu D, Sun S. A sorted neighbourhood approach for detecting duplicated regions in image forgeries based on DWT and SVD. Proceedings IEEE International Conference on Multimedia and Expo, Beijing, China; 2007 Jul 2–5. p. 1750–53.
8. Yang B, Sun X, Chen X, Zhang J, Li X. An efficient forensic method for copy-move forgery detection based on DWT-FWHT. Radio Engineering. 2013; 22(4):1098–105.
9. Huang Y, Lu W, Sun W, Long D. Improved DCT-based detection of copy-move forgery in images. Forensic Science International. 2011; 206 (1–3):178–84.
10. Muhammad G, Hussain M, Khawani K, Bebis G. Blind copy move forgery detection using dyadic undecimated wavelet transform. Proceedings IEEE 17th International Conference on Digital Signal Processing, (DSP), Confu; 2011 Jul 6–8. p. 1–6.
11. Hashmi MF, Hambarde AR, Keskar AG. Copy move forgery detection using DWT and SIFT features. 13th Proceedings IEEE International Conference on Intelligent Systems Design and Applications, Bangi. 2013 Dec. p. 188–93.
12. Ghorbani M, Firouzmand M, Faraahi A. DWT-DCT (QCD) based copy-move image forgery detection. Proceedings 18th International Conference on Systems, Signals and Image Processing, Sarajevo; 2011 Jun. p. 1–4.
13. Mahadian B, Saic S. Detection of copy-move forgery using a method based on blur moment invariants. Forensic Science International. 2007; 171(2–3):180–89.
14. Ryu SJ, Lee MJ, Lee HK. Detection of copy-rotate-move forgery using Zernike Moments. Proceedings 12th International Conference on Information Hiding; 2010. p. 51–65.
15. Liu GJ, Wang JW, Lian SG, Wang ZQ. A passive image authentication scheme for detecting region-duplication forgery with rotation. Journal of Network and Computer Applications. 2011; 34(5):1557–65.
16. Li L, Li S, Zhu H. An efficient scheme for detecting copy-move forged images by Local Binary Patterns. Journal of Information Hiding and Multimedia Signal Processing. 2013; 4(1):46–56.
17. Ojala T, Pietikainen M, Maenpaa T. Multiresolution gray-scale and rotation invariant texture classification with local binary patterns. IEEE Transactions on Pattern Analysis and Machine Intelligence. 2002; 24(7):971–87.
18. Li Z, Liu GZ, Yang Y, You JY. Scale and rotation-invariant local binary pattern using scale-adaptive texton sub uniform based circular shift. IEEE Transactions on Image Processing. 2012; 21(4):2130–40.
19. CASIA. Image tampering detection evaluation database [Internet]. [Cited 2014 Sep 17]. Available from: http://forensics.idealtest.org.
20. Li L, Li S, Zhu H, Wu X. Detetcing copy-move forgery under affine transforms for image forensics. Computers and Electrical Engineering. 2014; 40(6):1951–62.

21. Muhammad G, Al-Hammadi MH, Hussain M, Bebis G. Image forgery detection using steerable pyramid transform and local binary pattern. Machine Vision and Applications. 2014; 25(4):985–95.
22. Rao CS, Babu SBGT. Image authentication using local binary pattern on the low frequency components. Microelectronics, Electromagnetics and Telecommunications. 2016; 372: 529–37
23. Deepa M, Saravanan T. Automatic image registration using 2d-discrete wavelet transform. Indian Journal of Science and Technology. 2016 Feb; 9(5):1–3. Doi no:10.17485/ijst/2016/v9i5/58101.