Copy-Move Image Forgery Detection using Ring Projection and Modi_ed Fast Discrete Haar Wavelet Transform

Mohd Dilshad Ansari and Satya Prakash Ghrera

Department of Computer Science & Engineering
Jaypee University of Information Technology, Waknaghat, Solan(HP), India.
m.dilshadcse@gmail.com, sp.ghrera@juit.ac.in

Abstract: In the recent years,Wavelet transform has been proved to be a very useful tool for image processing. Modified fast haar wavelet transform (MFHWT) is one of the approach which reduces the calculation work in haar transform (HT) and fast haar transform (FHT). In the present communication, we applied modified fast haar wavelet on an input image to yields a highly reduced dimension representation. In this way, the number of image blocks of an image can be drastically reduced which improves the time efficiency of subsequent lexicographical sorting and similarity matching. This reduced dimension representation is split into fixed-size overlapping blocks and then ring projection transform is performed to each block for extract their features into a row vector. These extracted feature vectors are arranged in a matrix. Then, the feature vectors are sorted by a lexicographical order so that similar blocks would be consecutive. Finally, the duplicated blocks are filtered out by calculating the similarity value of correlation coefficient between two adjacent blocks. Obtained results show the performance of proposed algorithm, which is able to detect forgery with less computational time and also reduced dimension drastically as well as memory needed for the detection process of copy move image forgery.

Keywords: Copy-move image forgery detection, Haar wavelet transform, Ring projection transform, Similarity criterion, Feature extraction.

1. Introduction

In recent years, the popularity of digital cameras, smart phones and tablets has made the acquisition of digital images easier. In addition to that, modern photo editing software package such as Photoshop makes it relatively easy to create digital image forgeries, on which people almost cannot perceive the difference between the original image and its tampered version. There is speedy enlarge in digitally manipulated image forgeries in social media and on the internet. These kinds of activities decreasing the credibility of digital image, so there must be some algorithm which can provide the authenticity of digital images. In literature, there are mainly two types of image authentication methods: Active and passive methods. In the active methods, the digital image requires preprocessing of image such as watermark embedding or signature generation, which limits their application in practice. To overcome active methods passive method came into the picture, techniques do not need any digital signature to be generated or to embed any watermark. Passive methods are further categories into five categories as shown in figure 1 [1, 2, 12]:

The copy-move image forgery is most common approach used to create a digital image forgery, in which a specific block of image is copied and then pasted it into another region in the same image to achieve information hiding. Because the copied block comes from the same image, its important properties, such as noise, color palette and texture, will be compatible with the rest of the image and thus will leads to a great challenge in detecting, locating the tampered parts. For copy-move forgery detection various methods have been proposed that are mainly based on either block based technique or key point matching techniques are shown in figure 1 [2, 3, 8, 11, 17, 23, 24].

Received: August 24th, 2016. Accepted: September 23rd, 2017
DOI: 10.15676/ijeei.2017.9.3.9

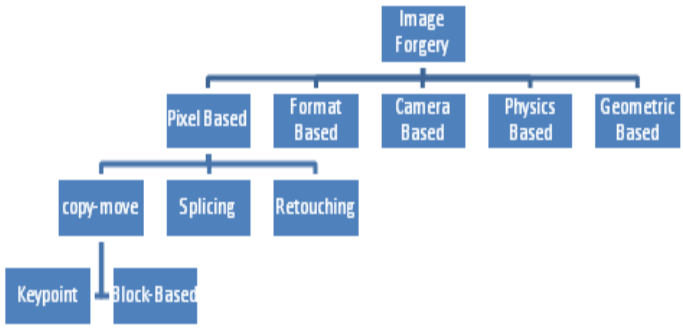

Figure 1. Image forgery detection techniques

A. Key-point based algorithm

The key-point based approaches depend on the extraction of local interest points (key-points) from local interest regions with high entropy without any image sub-blocking. Best key-points should be efficient for computing and capable of identifying different locations in the image regions. The robust in detection of geometric transformations, illumination changes, noise and other distortions. The major advantage of key-point based approaches is that they have high detection rates in duplicated regions, which exhibit a rich structure such as image regions, but still struggle to reduce the false matches in the flat regions like sky and ocean, etc. Huang et al. [15] developed copy move forgery detection using Scale invariant feature transform (SIFT) algorithm in 2009. In this paper, authors introduced SIFT algorithm to find the duplicate region with scale and rotation. Best bin first search (BBF) techniques have been used for finding possible duplicate key-points. Further, nearest neighbor distance ratio (NNDR) is
used to increase the detection rate or accuracy. This algorithm is able to detect key-points even if image is noisy or compressed. Similar methods have been developed by various authors using SIFT and SURF algorithm such as Battiato et al. [21], Amerini et al. [22], Lin et al. [17] etc.

B. Block Based Methods

Block based approaches are very popular and able to detect forgery regions accurately. First image is divided into a overlapping sub-blocks. Then, efficient features (feature vector) are extracted from each block with the help various feature extraction and dimension reduction methods (DWT, DCT, SVD and PCA etc.). Compared these feature vectors to find the possible forgery regions.

The first block based method is introduced by Fridrich et al.[1]. Discrete cosine transform is used to extract the features, lexicographical sort the feature vector for finding the similar blocks. This method is take too much computational time and not able to detect if some attack are applied on image like rotation and scaling. Afterwards, to overcome this method Popescuet et al.[2] developed a similar method for detecting copy-move regions. Principal component analysis has been used for feature extraction and dimension reduction. Ansari et al.[13, 14] have proposed dignified method for extracting features from input image, further extracted feature vector can be used to detect copy-move forgery detection. Additionally, they have also developed edge detection [29, 30] techniques, copy-move forgery can be identify after edge detection. G. Li et al.[3] developed a sorted neighborhood method based on discrete wavelet transform (DWT) and singular value decomposition (SVD), afterwards Li Kang et al. [20] also used improved SVD for forgery detection. The SVD method suffers from the drawback that the computation of SVD takes lot of time and it is computationally complex. Lin et al. [17] used PCA as well as radix sort and Wang et al. [26] developed hybrid approach, used DWT and DCT for detecting copy-move forgery region, similarly Zhang et al. [19] used DWT, Ghorbani et al. [16] used DWT and DCT.

In this paper, we only focus our attention on block-based methods for CMFD. First, applying modified fast haar wavelet transform(MFHWT) on an input image to yield a highly reduced dimension representation. This highly reduced dimension representation is split into fixed-size

overlapping blocks and ring projection transform(RPT) is performed to each block for representing their features. Then, the feature vectors are sorted by a lexicographical order so that similar blocks would be consecutive. Finally, the duplicated blocks are filtered out by the similarity measure of correlation coefficient.

2. Modified Fast Haar Wavelet Transform

In this section, we discuss the concept of modified fast haar wavelet and ring projection transforms. Haar Transform (HT) is memory efficient and exactly reversible without the edge effects. Nowadays haar transform technique is widely used in image compression. The HT is one of the simplest and basic transformation from the space domain to a local frequency domain. A HT decomposes a signal into two components, one is called average (approximation) or trend and the other is known as difference (detail) or fluctuation.

An explicit formula for the values of first average sub-signal, $a1 = (a1; a2; \cdots an=2)$ at one level for a signal $f = (f1; f2; \cdots fn)$ of length n is given by

$$a_k = \frac{f_{2k-1} + f_{2k}}{\sqrt{2}}, \quad k = 1, 2, \ldots, n/2. \tag{1}$$

and the first detail sub-signal, $d1 = (d1; d2; : : : dn=2)$ at the same level is given as

$$d_k = \frac{f_{2k-1} - f_{2k}}{\sqrt{2}}, \quad k = 1, 2, \ldots, n/2. \tag{2}$$

Wavelet decomposition of the images is used due to its inherent multiresolution characteristics. The basic idea of using discrete wavelet transform is to reduce the size of the image at each level, e.g., a square image of size $2j \times 2j$ pixels at level L reduces to size $2j=2\times2j=2$ pixels at level $L+1$. At each level, the image is decomposed into four sub images. The sub images are labeled LL, LH, HL and HH. LL (approximation area) includes information about the global properties of analyzed image. Removal of spectral coefficients from this area leads to the biggest distortion in original image. LH (horizontal area) includes information about the vertical lines hidden in image. Removal of spectral coefficients from this area excludes horizontal details from original image. HL (vertical area) contains information about the vertical lines hidden in image. Removal of spectral coefficients from this area eliminates vertical details from original image. HH (diagonal area) includes information about the diagonal details hidden in image. Removal of spectral coefficients from this area leads to minimum distortions in original image.

Roeser and Jernigan [4] introduced the Fast Haar Transform computationally efficient and effective algorithms which reduce the tedious work of calculations. FHT involves addition, subtraction and division by 2. Its application in atmospheric turbulence analysis, image analysis, signal and image compression has been discussed in [5]. Modified fast and exact algorithm for fast haar transform has been discussed in [6].

In MFHWT, first average sub-signal, $a1 = (a1; a2; : : : an=4)$ at one level for a signal $f = (f1; f2; : : : fn)$ of length n is given by

$$a_k = \frac{f_{4k-3} + f_{4k-2} + f_{4k-1} + f_{4k}}{4}, \quad k = 1, 2, \ldots, n/4 \tag{3}$$

and the first detail sub-signal, $d1 = (d1; d2; : : : dn=4)$ at the same level is given as

$$a_k = \begin{cases} \frac{(f_{4k-3}+f_{4k-2})-(f_{4k-1}+f_{4k})}{4}, & k = 1, 2, \ldots, n/4 \\ 0, & k = n/2, 2, \ldots, n. \end{cases} \tag{4}$$

Bhardwaj and Ali [7] used the same concept of finding averages and differences to extended for 2-D images in addition of considering the detail coefficients 0 for $n=2$ elements at each level. The MFHWT is faster in comparison to FHT and reduces the calculation work. In MFHWT, we get the values of approximation and detail coefficients one level ahead than the FHT and HT. At

each level in MFHWT, we need to store only half of the original data used in FHT, due to which it becomes more and more memory efficient. The most noticeable fact is that the MSE and PSNR values of reconstructed images are as good as in HT and FHT. An example image along with its wavelet transform applied up to level 3 is shown in Figureure 2.

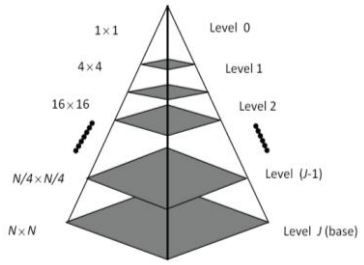

Figure 2. *MFHWT Decomposition*

A. Ring Projection Transform (RPT) for Features Extraction

In order to make matching invariant to rotation, the RPT [8, 9, 10, 11] process was proposed. The RPT transforms a 2-D image into a rotation-invariant representation in the 1-D ring projection space. Let us denote a template, whose size is $m \times n$, by $T(x; y)$. The RPT process of the template is given as follows: First, the center point of $T(x; y)$, denoted as $(xc; yc)$, is derived, and subsequently, the template $T(x; y)$ Cartesian frame is transformed into a polar frame based on the following relations:

$$x = r \cos \Phi; \tag{5}$$
$$y = r \sin \Phi; \tag{6}$$

where, $r = \text{Int}[(x - xc)2 + (y - yc)2]1/2; r \in [0; R]; R = \min(M; N)$ and $\Phi \in [0; 2\pi]$.

The ring-projection of image $T(x; y)$ at radius r, denoted by $PT(r)$, is defined as the mean value of $T(r \cos \_; r \sin \_)$ at the specific radius r. That is,

$$P_T(r) = \frac{1}{2\pi r} \int_0^{2\pi} T(r \cos\theta,\ r \sin\theta) \tag{7}$$

Taking the mean of stimulus values for each specific ring reduces the effect of noise. The discrete representation of $PT(r)$ is given by

$$P_T(r) = \frac{1}{S_r} \sum_{i=1}^{n} T(r \cos\theta_k,\ r \sin\theta_k) \tag{8}$$

where Sr is the total number of pixels falling on the circle of radius $r = 0; 1; 2; \cdots; R$. Since $PT(r)$ is defined as the mean of pixel intensities along the circle, centered on the template, whose radius is r (as shown in Figureure 3), $PT(r)$ values of all rings in the template have equal importance in the computation of correlation [10]. Furthermore, since a RPT is constructed along circular rings of increasing radii, the derived one dimensional ring projection template is invariant to rotation of its corresponding two dimensional image template.

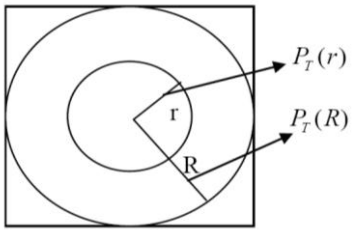

Figure 3. *Concept of RPT template*

The correlation coefficient is a measurement of the strength of the linear relationship between two variables or sets of data. For the matching process, the normalized correlation (NC) is adopted in the measurement of similarity. Let $PT = [PT(0); PT(1); PT(2); \cdots PT(R)]$ and $PS = [PS(0); PS(1); PS(2); \cdots PS(R)]$. Then normalized correlation coefficient between two different RPTs *PT* and *PS* is given by the formula:

$$\langle P_T, P_K \rangle = \frac{\left[(R+1)\sum_{r=0}^{R} P_T(r)P_S(r) - \sum_{r=0}^{R} P_T(r)\sum_{r=0}^{R} P_S(r)\right]^2 \times 100}{\left\{(R+1)\sum_{r=0}^{R} P_T(r)^2 - \left[\sum_{r=0}^{R} P_T(r)\right]^2\right\}\left\{(R+1)\sum_{r=0}^{R} P_S(r)^2 - \left[\sum_{r=0}^{R} P_S(r)\right]^2\right\}} \quad (9)$$

The value of $\langle PT ; PK \rangle$ is unaffected by rotations and linear changes (constant gain and offset) between two different RPTs *PT* and *PS*. In addition, the dimensional length of the ring projection vector is only $R + 1$. This significantly reduces the computational complexity for $\langle PT ; PK \rangle$.

3. Copy-Move Forgery Detection (CMFD) Method

In block-based CMFD methods, most of the algorithm frameworks are similar to the approach proposed by Popescu et al. [2]. In these approaches lot of computational effort are required for dimension reduction, matching control and similarity filtering. In general, as test images grow larger, the nature of CMFD algorithms required many iterations and comparisons e.g., Suppose that a gray-scale image is of size $m \times n$ pixels can be partitioned into small overlapping blocks of size $b \times b$ pixels, then total number of image blocks are $N = (m-b+1)\times(n-b+1)$ generated by sliding the window of $b \times b$ pixels over the whole image by one pixel each time from upper left to bottom right corner. MATLAB excels in working with matrices, however is less optimized when faced with multiple loops. Therefore, it will be highly important that the loops were kept to a minimum as possible. Moreover, CMFD method would become computationally prohibitive when the large number of image blocks which inevitably leads to extremely high computational burden for subsequent feature extraction and similarity matching. Therefore, the key point to reduce the computational cost, the task of CMFD is normally conducted on a reduced image size; however, information loss is inevitable.

Based on this idea, we propose a boosting scheme to reduce the computational overhead and number of estimated blocks each time and it turns out to increase time and memory efficiency dramatically. The proposed method has been applied on gray images as follows:

1. Read the input image, if the input image is *RGB*, then converts it into gray scale version by $I = 0{:}228R + 0{:}587G + 0{:}114B$.
2. Apply MFHWT up to specified level '*L*' to the gray image.
3. Overlapping blocks of size $b \times b$ are created in the *LLL* image with one pixel shifting and the total number of overlapping blocks is given by $Novr = (M - b + 1) \times (N - b + 1)$.
4. The blocks with minimum contrast value are ignored as they are unstable over image variations and leads to false positive results. Therefore, in order to reduce the false positive results, we ignore those blocks, where contrast value is less than the predefined threshold.

Hence, if the contrast value of each overlapping $b \times b$ is less than the predefined *'CTR'*, then we ignore it, otherwise we apply the following steps:

(a) Transform each overlapping $b \times b$ into a $1-D$ RPT vector of size $R + 1$.

(b) The feature vectors extracted from Step (a) are arranged in a matrix, denoted as A with the size of $(M-b+1)(N-b+1) \times R+1$.

(c) In the mean while, we form another matrix P of two columns for storing top-left coordinates.

5. End
6. Apply lexigraphical order to the matrix A so that similar blocks are consecutively sorted.
7. For every adjacent rows of matrix A,
   (a) Compute the normalized correlation coefficient between the pair of sorted rows using the equation (9)
   (b) If the computed correlation coefficient exceeds a preset threshold value *'C't*, then extract the corresponding blocks position from the matrix P, and marked the location of these forged blocks are in the original image by setting pixel values to zero.
8. end

4. Results and Discussion

In this section, we present the experimental procedure and determine the performance of proposed method in terms of accuracy, true positive rate (TPR)and false positive rate(FPR).The experiments were carried out on Matlab R2013a, 4 GB RAM and core i3 processor. To determine the performance of proposed method and its quality, a realistic database can be constructed. We have composed a database of 100 images, where 50 images are forged and 50 images are original. This database having different type of image format and various resolutions like 256 × 256, 512 × 512, 640 × 480 etc. The forged images are constructed with the help of Photoshop, In which the forge area or object is randomly selected and pasted into the same image. Also, we have applied various attacks on tempered image like scaling, rotation and blurring. The performance of the proposed technique can be observe by calculating True Positive Rate (TPR), False Positive Rate (FPR), and Accuracy.

$$\text{Accuracy} = \frac{\text{Number of identified images}}{\text{Number of forged images}} \times 100$$

$$\text{True Positive Rate(TPR)} = \frac{\text{Number of forged images identified as forged}}{\text{Number of forged images}}$$

$$\text{False Positive Rate(FPR)} = \frac{\text{Number of original images identified as original}}{\text{Number of original images}}$$

The performance of proposed method is depicted in Table 1, Table 2 and Table 3, which shows that proposed method perform better than state of the art techniques [1, 2]. Table 1 shows the accuracy of proposed algorithm with normal forgery and various attacks. The accuracy of proposed algorithm in normal forgery, blurring attack and rotation attack were 95 %, 89 % and 87 % respectively. The overall accuracy of proposed method was 90.75 %. Additionally, Table 2 shows proposed algorithm is able to reduce dimensions drastically in comparison to other reported methods[1, 2, 16, 18, 22, 25]. If the dimension of the algorithm is less, then definitely it will take less computational time, that is why proposed algorithm is taking less computational time as compare to other existing algorithm as shown in Table 3. The images shown in Figure. 4 represents the result of copy move forgery detection marked on the tampered image with predefined threshold CTR and without CTR. The row is composed of four images: original image, tampered image, result image with CTR 2 and CTR 1 from left to right. First, the original image is decomposed at level 1 by applying MFHWT. The parameters in this experiment were set as: $Ct = 0{:}98$, $CTR = 2$, $b = 7$. The detection process taking 6 seconds which shows that proposed method is highly efficient with respect to computational time and successfully able to

detect forgery region. However, if we apply proposed algorithm by taking the blocks whose contrast is minimum, then we obtained false positive results and more time are required for forgery detection process. The detection result with following parameter values $Ct = 0{:}98$, $CTR = 1$, $b = 7$ and the required
time is 8 seconds.

Further, we have applied various attacks such as rotation, scaling and blurring attack. The forgery detection results are shown in figure 5, figure 6 and figure 7. To verify the robustness against rotation attack, one duplicated region with rotation angles of 45 degree is applied and proposed algorithm is able to detect forgery region as shown in figure 5. Figure 6 shows tampered image was distorted by different processing operations such as Gaussian blurring (with mean =0; _ = 0:01), Rotation with angle 180 degree and scale with some factor. Figure 7 shows copy of a single object is pasted multiple times in the forged image and proposed algorithm is able to detect all objects efficiently without any postprocessing operation. Similarly, forgery are being identified on other images also as shown in figure 8 and figure 9.

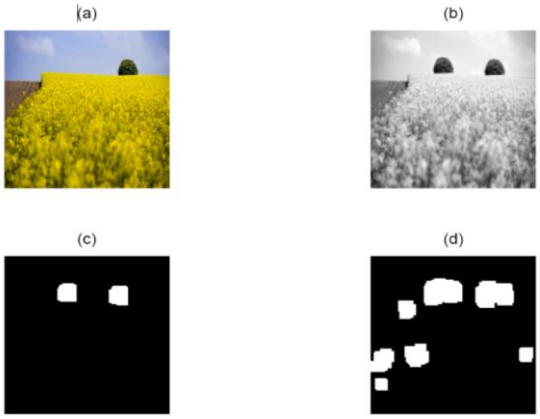

Figure 4. (a) Original image, (b) Forged image, (c) Forgery detection with CTR=2 and (d) Forgery detection with CTR=1.

Figure 5. Detection of duplicated region with a rotation angle of 45; (a) original image, (b) forged image of (a), and (c) Result of forgery detection 12

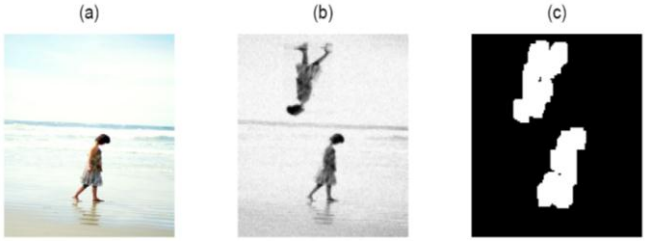

Figure 6. Gaussian blurring (with mean = 0; σ = 0:01), Rotation with angle 180 degree and scale factor=120; (a) original image, (b) forged image of (a), and (c) result of forgery detection

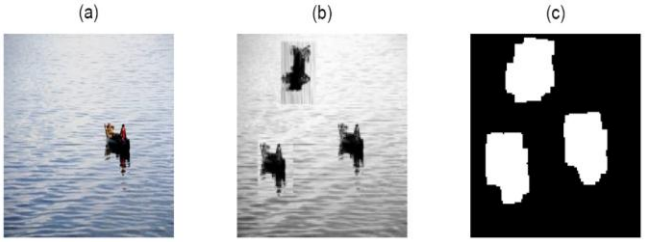

Figure 7. Multi-paste forgery detection (a) Original image, (b) forged image of (a), and (c) result of forgery detection

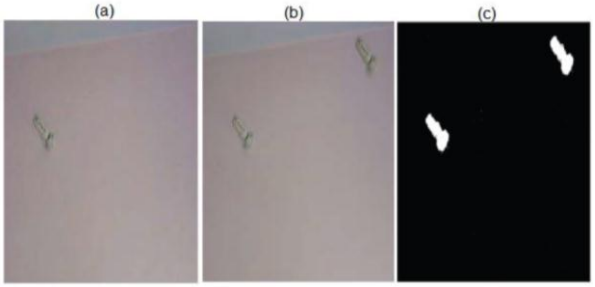

Figure 8: (a) Original image, (b) forged image of (a), and (c) result of forgery detection

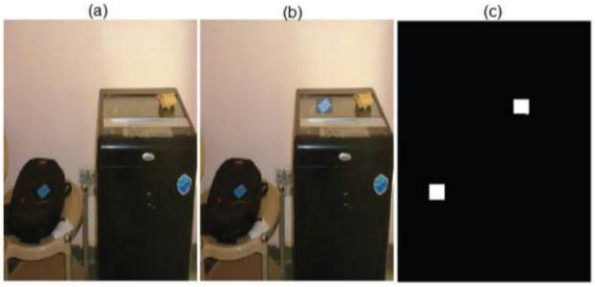

Figure 9: (a) Original image, (b) forged image of (a), and (c) result of forgery detection

Table 1. Accuracy Results

Forgery Type	No. of Images	Identified Correctly	Identified Incorrectly	Accuracy
Normal Forgery(50)	100	95	5	95 %
Forgery with Blurring (25)	100	89	11	89 %
Forgery with Rotation (25)	100	87	13	87 %
Forgery with Multiple objects (25)	100	92	8	92 %
Total	400	363	37	90.75 %

Table 2. Feature Dimension Comparison with Existing Algorithm

Methods	Extraction Domain	No. of Blocks	Feature Dimension
Fridrich et al. [1]	DCT	62001	64
Popescu et al. [2]	PCA	62001	32
Amerini et al. [22]	SIFT	2700 key points	128
Zimba et al. [25]	DWT-PCA	12789	16
Ghorbani et al. [16]	DWT-DCT	12769	16
Jiu Hu et al. [27]	Grouped DCT	45024	8
Lou et al. [18]	Spatial Domain	61009	5
Proposed	MFHWT-RPT	14641	4

Table 3. Execution Time (In Seconds) Comparison with Existing Algorithm

Methods	Extraction Domain	Blocks Size	Execution Time
Fridrich et al. [1]	DCT	8	294.96
Popescu et al. [2]	PCA	8	70.97
Xiaofeng et al. [26]	DWT-DCT	8	39.70
Proposed	MFHWT-RPT	8	5.80

5. Conclusion

In this paper, we have presented a novel method to detect copy-move image forgery based on a haar wavelet and ring projection transform method. By the comprises scheme of haar wavelet and ring projection transform, the time and memory efficiency can be greatly improved. Due to the inherently rotation-invariant feature of the RPT method, large angle rotation of tampered region can be successfully detected. The obtained results show the feasibility and effectiveness of the proposed method. In future work, one can apply the proposed method to detection the forgery in color, highly compressed and noisy images.

6. References

[1]. J. Fridrich, D. Soukal, and J. Lukas, "Detection of copy-move forgery in digital images," *Proceedings of the Digital Forensic Research Workshop*, Cleveland OH, USA, 2003.

[2]. A.C. Popescu and H.Farid, "Exposing digital forgeries by detecting duplicated image regions," Dartmouth College, Hanover, New Hampshire, USA: TR 2004-515, 2004.

[3]. G.Li, Q.Wu, D.Tu, and Shaojie Sun, "A sorted neighborhood approach for detecting duplicated regions in image forgeries based on DWT and SVD", *IEEE International Conference on Multimedia & Expo*, Beijing, China, pp. 1750-1753, 2007.

[4]. Roeser, P.R. and M.E. Jernigan, "Fast Haar Transform Algorithm. *IEEE Transactions on Computer*", C-31: pp.175–177, 1982.

[5]. Kaiser, G., "The Fast Haar Transform: Gateway to Wavelet", Potentials, IEEE, Vol.17(2), pp.34–37, 1998.

[6]. Chang, P. and P. Piau, "Modified Fast and Exact Algorithm for Fast Haar Transform", *Proceedings of World Academy of Science, Engineering and Technology*, Vol.26, pp.509–512, 2007.

[7]. Bhardwaj A. and Ali R., "Image Compression Using Modified Fast Haar Wavelet Transform", *World Applied Sciences Journal*, Vol.7(5): pp.647–653, 2009.

[8]. D. M. Tsai and C. H. Chiang, "Rotation-invariant pattern matching using wavelet decomposition", *Pattern Recogn. Lett*. Vol.23, pp.191–201,2002.

[9]. Y. Y. Tang, H. D. Cheng, and C. Y. Suen, "Transformation-ring projection (TPR)algorithm and its VLSI implementation", *Int. J. Pattern Recognit. Artif. Intell*. Vol.5, pp.25–56, 1991.

[10]. Y. Y. Tang, B. F. Li, H. Ma, and J. Liu, "Ring-projection-wavelet fractal signatures:a novel approach to feature extraction*", IEEE Trans. Circuits Syst., Analog DigitalSignal Process*., Vol.45, pp.1130–1134, 1998.

[11]. M. S. Choi and W. Y. Kim, "A novel two stage template matching method for rotationand illumination invariance", *Pattern Recogn*. Vol.35, pp.119–129, 2002.

[12]. Ansari, Mohd Dilshad, S. P. Ghrera, and Vipin Tyagi. "Pixel-Based Image ForgeryDetection: A Review." *IETE Journal of Education*, Vol.55(1),pp.40-46, 2014.

[13]. Ansari, M.D. and Ghrera, S.P. "Intuitionistic fuzzy local binary pattern for featuresextraction", *Int. J. Information and Communication Technology*. In Press

[14]. Ansari, Mohd Dilshad, and Satya Prakash Ghrera. "Feature extraction method fordigital images based on intuitionistic fuzzy local binary pattern." *In System Modeling & Advancement in Research Trends (SMART)*, International Conference, pp. 345-349.IEEE, 2016.

[15]. H. Huang, W. Guo, and Y. Zhang, "Detection of Copy-Move Forgery in Digital Images Using SIFT Algorithm," *Pacific-Asia Workshop on Computational Intelligence and Industrial Application*, vol.2, pp. 272-276, 2008.
[16]. Ghorbani, M., Firouzmand, M., & Faraahi, A. "DWT-DCT (QCD) Based Copymove Image Forgery Detection", *18th International Conference on Systems, Signals and Image Processing (IWSSIP)*,pp. 1-4, 2011.
[17]. Lin, H.-J., Wang, C.-W., Kao, Y.-T, "Fast Copy-Move Forgery Detection," *WSEAS Trans. Signal Process*, pp.188-197, 2009.
[18]. Luo W Q, Huang J. W., Qiu G P., "Robust Detection of Region-Duplication Forgery in Digital Image", *Proceedings of 18th International Conference on Pattern Recognition (ICPR 2006)*, pp. 746-749,2006.
[19]. Zhang, J., Feng, Z., Su, Y., "A New Approach for Detecting Copy-Move Forgery in Digital Images," *IEEE Singapore Int. Conf. Comm. Sys*., China, pp. 362-366, 2008.
[20]. Li Kang, Xiao-Ping Cheng, "Copy-move Forgery Detection in Digital Image," *3rd International Congress on Image and Signal Processing (CISP2010), IEEE Computer Society*, pp. 2419-2421, 2010.
[21]. Battiato, S. Farinella, G.M. Messina, E. Puglisi, G. "Robust image alignment for tampering detection". *IEEE Ttans. Inf. Forensics Secur*. , Vol.7, pp.1105-1117, 2012.
[22]. Amerini, I., Ballan, L., Caldelli, R., Del Bimbo, A. and Serra, G. "A sift-based forensic method for copymove attack detection and transformation recovery", *IEEE Ttans. Inf. Forensics Secur*.,vol.6, pp.1099-1110, 2011.
[23]. Ibrahim, R.W., Moghaddasi, Z., Jalab and H.A., Noor, "R.M. Fractional differential texture descriptors based on the machado entropy for image splicing detection", Entropy, vol. 17, pp.4775-4785, 2015.
[24]. Ansari, M.D. and Ghrera, S.P. andWajid, M. "An Approach for Identication of Copy- Move Image Forgery based on Projection Profiling, *Pertanika Journal of Science & Technology*, Vol 25, No.2 pp.507-518,2017.
[25]. Michael Zimba, Sun Xingming, "DWT-PCA (EVD) Based Copy-move Image Forgery Detection" *International Journal of Digital Content Technology and its Applications*, Vol.5(1), pp.251-258, 2011
[26]. Wang, X., Zhang, X., Li, Z., & Wang, S."A DWT-DCT based passive forensics method for copy-move attacks" *Third International Conference on Multimedia Information Networking and Security*, pp.304-308, 2011.
[27]. Hu, J., Zhang, H., Gao, Q. and Huang, H., "An improved lexicographical sort algorithm of copy-move forgery detection" *Second International Conference on Networking and Distributed Computing (ICNDC)*, pp. 23-27, 2011.
[28]. Huang, Yanping, Wei Lu, Wei Sun, and Dongyang Long. Improved DCT-based detection of copy-move forgery in images. *Forensic science international*, vol. 206(1),pp. 178-184, 2011.
[29]. Ansari, M.D., Mishra, A.R. & Ansari, F.T. "New Divergence and Entropy Measuresfor Intuitionistic Fuzzy Sets on Edge Detection" *Int. J. Fuzzy Syst*.(2017).doi:10.1007/s40815-017-0348-4
[30]. Ansari, M. D., Mishra, A. R., Ansari, F. T., & Chawla, M. "On edge detectionbased on new intuitionistic fuzzy divergence and entropy measures" *Fourth IEEE International Conference on Parallel, Distributed and Grid Computing (PDGC)*, pp. 689-693, 2016.

Mohd Dilshad Ansari is pursuing his Ph.D. in Image Processing at Jaypee University of Information Technology, Waknaghat, Solan, HP, India. He received his M.Tech in Computer Science and Engineering in 2011 and B.Tech in Information Technology from Uttar Pradesh Technical University, Lucknow, UP in 2009. He has published more than 20 papers in International Journals and conferences. He is the Member of various technical/professional societies such as IEEE, UACEE and IACSIT. He has been appointed as Editorial/Reviewer Board and Technical Programme Committee member in various reputed Journals/Conferences. His research interest includes image forensics and image processing.

Satya Prakash Ghrera is Professor and HoD of Department of Computer Science and Engineering at Jaypee University of Information Technology, Waknaghat, Solan (HP), India. His research interests include image processing and image security.