Angular Radial Transform based Copy-Move Forgery Detection

Manpreet Kaur[1] Dr. Amandeep Kaur[2]
[2]Associate Professor
[1,2]Department of Computer Engineering
[1,2]School of Engineering and Technology, Central University of Punjab, Bathinda India

Abstract— Digital images are most common and the convenient way of storing and transmitting the visual information. Copy move forgery is most common form local processing among other techniques. This paper proposes a dense field copy move detection technique based on Angular Radial Transform of small image blocks. We exploit rotation invariance properties to reliably unveil duplicated regions after arbitrary rotations. Experiments indicate high robustness against rotation JPEG compression, blurring, smooth and textured images.

Key words: CMF: Copy Move Forgery, ART: Angular Radial Transform

I. INTRODUCTION

Digital images play very significant role in the storing and transferring the visual information i.e. animations or gifs. With the advancement in digital photography there is rapid increase in the use of images for representation of information. According to Mary Meeker's (a former Morgan Stanley internet analyst) annual Internet Trends report states that all internet-connected citizens share over 1.8 billion photos each day through multi-platform services such as Snapchat, Instagram. From the earlier days, an image has commonly been accepted as an evidence of occurrence of the illustrated scene. Images are widely used in various kind of applications in the area of military, news, medical diagnosis and media for multipurpose. In today's digital world due to the development in technology of digital image, for example, cameras, mobile apps, software, and computers and the wide spread via the internet, digital image can be considered a major source of information. At the same time, with the wide and easy availability of advanced image editing tools (e.g. Adobe Photoshop, Gimp), modifying a digital photo, with little or no obvious signs of tampering, has become also very easy and widespread. Photo editing is widely used for enhancing the quality of digital image (such as contrast enhancement, coloring, noise removal or smoothening etc.). Example of image forgery is shown in Fig 1.

Fig. 1: Photo shopped image [1] of North Korea's missile launch from submarine

Digital forensics is the field which deals with the authenticity and trustworthiness of the image or video. Forgery is the process of making, adapting, or imitating objects, statistics, or documents with the intent to deceive for the sake of altering the public perception, or to earn profit by selling the forged item. Studio replicas, and reproductions are not the forgeries, though they may later become forgeries through knowing and willful misrepresentations. Adding, deleting, resizing, rotating content of an image are standard methods to forge any image forgery. This poses a significant social hitch of the extent of trust that may be placed within the credibleness of digital content.

Digital image forgery can be classified as Image Retouching, Copy-Move forgery, and Image splice relying upon the kind of techniques used to produce the tampered images. Image retouching is a common technique employed in the media industry. Image retouching manipulate features of the image by adjusting colors, contrast, white balance (i.e. gradational retouching), sharpness, noise and removing elements or visible flaws on skin or materials. Image splicing is techniques in which fragments from different images are used to create forged image which further undergo operations like smoothening, compression to make tempering visually undetectable. Copy-move forgery (or cloning) parts of the image are copied and pasted in another region, with some geometrical transformations on part, of the same image to conceal or emphasize image details.

II. LITERATURE REVIEW

Within the last decade, researchers in digital image forensics have developed techniques can be classified as active and passive, to restore some of the lost trustworthiness of digital images. In Active approach some information should be kept at source facet like Digital Watermark Digital signature. In case of Passive approach any foresaid information regarding the image is not available. The key assumption of passive approach is that images exhibits artifacts, e.g. due to re-sampling, smoothing, compression, sharpening, contrast enhancement and quantization.

Copy Move Forgery Image forgery detection methods [11] can be classified as: Key Point-Based methods and dense field methods. Key-point based methods works on the comparatively lesser set of pixels, some methods are used to extract local features from the image and generate keypoint descriptors to represent the features. In case of dense field image apportioned into overlapping blocks corresponding features are computed. Dense field methods are slow as compared to key point methods but have higher accuracy. In key point methods interest points (key points) are computed using algorithm like SIFT [3], Harris corner detection, LBP [9] or SURF. In case of dense field methods invariant features like Zernike moments [2], Fourier Miller Transform [1], Polar sine and cosine transforms based on a log-polar sampling.

Patch Match [6] is a fast randomized algorithm which finds dense approximate nearest neighbor matches between image patches. Patch Match generalized [7] and

extended by including the ability to search across scales and rotation angles, going beyond mere translations, and to match patches based on arbitrary descriptors and distances, rather than just the Euclidean norm of original patches used in the basic version. In [4] modification in basic Patch Match is introduced which take into account zero order predictors for offset magnitude. In [1] the algorithm in [4] is further modified with addition of first order predictors for offset values.

For post processing Random Sample Consensus (RANSAC) algorithm, SATS, Dense Linear fitting approaches are used in [2], [7] and [1] respectively. Image segmentation technique has been exploited for removal false matches in [8] and [10].

A. Generalization of CMF Algorithm

The basic pipeline for copy move forgery detection is shown in figure 2. Algorithm can be generalized as following:

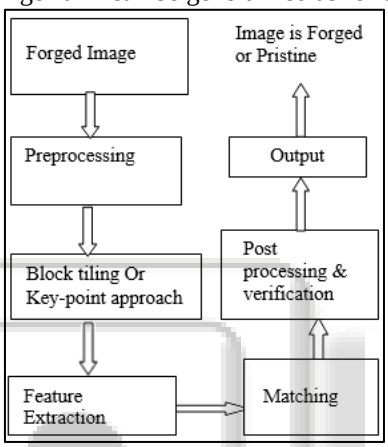

Fig. 2: Copy-move forgery detection algorithm pipeline.

– Suppose an image of size M × N, the duplicated regions detection can computed as follows:

1) Preprocessing

Convert the image to grayscale when applicable (exceptions: features of require all color channels for the feature calculation).

2) Block-based (Dense Field) Procedure

– Tile the image in Bi overlapping blocks of size b × b; Where, $0 \le I < ((M - b + 1) \bullet (N - b + 1))$
– Compute a feature vector fi for every block Bi

a) Key point-based procedure:

– Scan the image for key points (i.e. high entropy)
– Compute for every key point a feature vector fi.

3) Feature Extraction

Feature vectors computed for each block or key point as compact and discrete representation of region and these are used to inspect similarities in matching procedure.

4) Matching

It can be performed on the basis of exhaustive search, nearest neighbor approach and random search has been used in various literatures. Let Fij be a matched pair consisting of features fi and fj, where i, j denote feature indices, and $i \neq j$. Let c(fi) denote the image coordinates of the block or key-point from which fi was extracted. Then, vij denotes the translational difference ("shift vector") between positions c(fi) and c(fj). Minimum distance resembles similar patterns. For matching purpose approximate nearest neighbor based Patch Match, exhaustive search. Remove pairs Fij where $|Distij|_2 < \tau$ (threshold), Where, $Dist_i$ denotes the any distance norm such as Euclidean norm.

5) Clustering of the remaining matches that adhere to a joint pattern.

– For block-based methods: Let H(A) be the number of pairs satisfying the same affine transformation A. Remove all matched pairs where $H(A) < \tau 2$.
– For key point-based methods: Apply similar methods based on affine transformation, autocorrelation based clustering as in block based methods.

6) If an image contains connected regions of more than τ3 connected pixels, it is denoted as tampered. It is quite common to set the thresholds τ2 and τ3 to the same value.

III. FEATURE EXTRACTION

A. Angular Radial Transform

The ART coefficients of order n and repetition m for a continuous image function $f(x,y)$ in a unit disk are given by:

$$F_{nm} = \iint_{x^2+y^2 \le 1} f(\rho,\theta) V^*_{nm}(\rho,\theta) \rho d\rho d\theta \quad (1)$$

Where the function $V^*_{nm}(\rho,\theta)$ is the complex conjugate of the ART basis function $V_{nm}(\rho,\theta)$ of order n and m that are separable along the angular and radial directions, that is:

$$V_{nm}(\rho,\theta) = A_m(\theta) R_n(\rho) \quad (2)$$

To achieve rotation invariance, an exponential function is used for the angular basis function. The radial basis function is defined by a cosine function:

$$F'_{nm} = \frac{1}{2\pi} \int_0^{2\pi} \int_0^1 f(\rho,\theta_1) R_n(\rho) e^{jm(\theta_1+\alpha)} \rho d\rho d\theta$$

$$A_m(\theta) = \frac{1}{2\pi} e^{jm\theta} \quad (3)$$

$$R_n(\rho) = \begin{cases} 1, n = 0 \\ 2\cos(\pi n r), n > 0 \end{cases} \quad (4)$$

Where, ρ is the Radial component, $\rho = \sqrt{x^2 + y^2}$ Θ = Azimuthal component i.e. $\theta = \arctan(\frac{y}{x})$,

f(ρ ,θ) = Image intensity function in polar coordinates, n is a non-negative integer, m is an integer $j = \sqrt{-1}$.

B. Rotation Invariance of Angular Radial Transform

This section proves algebraic invariance of Angular Radial transform against rotation. Consider a rotation of the image through angle α. If the rotated image is denoted by f', the relationship between the original and rotated image in the same polar coordinate is as given as following:

$$f'(\rho, \theta) = f(\rho, \theta - \alpha) \quad (5)$$

Substituting equation 2 and 3 in equation 1:

$$F_{nm} = \frac{1}{2\pi} \int_0^{2\pi} \int_0^1 f(\rho,\theta) R_n(\rho) e^{jm\theta} \rho d\rho d\theta$$

$$F_{nm} = \int_0^{2\pi} \int_0^1 f(\rho,\theta) R_n(\rho) \frac{1}{2\pi} e^{jm\theta} \rho d\rho d\theta \quad (6)$$

Therefore, the Angular radial transform of the rotated image in the same coordinate is:

$$F'_{nm} = \frac{1}{2\pi} \int_0^{2\pi} \int_0^1 f(\rho,\theta-\alpha) R_n(\rho) e^{jm\theta} \rho d\rho d\theta$$

By a change of variable $\theta_1=\theta-\alpha$,

$$F'_{nm} = [\frac{1}{2\pi}\int_0^{2\pi}\int_0^1 f(\rho,\theta_1)R_n(\rho)e^{jm\theta_1}\rho d\rho d\theta_1]e^{jm\alpha}$$

$$F'_{nm} = [F_{nm}]e^{jm\alpha} \quad (7)$$

Equation (7) represents that each angular transform acquires a phase shift on rotation. Thus, $|F_{nm}|$ the magnitude of the transform can be used as rotation invariant feature. Therefore, the magnitude of the angular radial transform is computed to uniquely describe the each block regardless of rotation.

IV. PROPOSED METHOD

A. *Image Set*

For experimental purposes Benchmark dataset and Grip dataset is used. Benchmark dataset consists of forged images with JPEG compression, Gaussian noise, JPEG artifacts, rotated copies, scaled copies, combined effects, copies that were pasted multiple times. Grip dataset has 80 forged images with copy-move forgeries (in different contexts like texture smooth, rough or structured) and associated ground-truth.

1) Step1: Take an image and tile it in overlapping blocks with the assumption that size of the block will be smaller than the size of patch used for tempering. Image is apportioned into 16*16 and 32*32 blocks for experimental usage.
2) Step 2: Compute the ART feature descriptor for each block using n order and m repetitions. ART feature is computed using order n is set to 5 with five repetitions. Description of these features and their invariant properties are already discussed in Section IV. Feature descriptor for each block will be used as input to next step of algorithm.
3) Step 3: Matching: Every feature descriptor by searching its approximate nearest neighbor. Let Fij be a matched pair consisting of features fi and fj, where i, j denote feature indices, and $i \neq j$. The Chi Square distance is used compute the similarity of features. As per spatial property of image nearest pixels resemble with each other. Therefore, offset is used to search the similar patches at distant. Offset initialized at random as:

$$\delta(s) = U(s) - s \quad (8)$$

Where, U(s) is a bi-dimensional random variable, uniform over the image support Ω. The value $\delta(s) = 0$ is explicitly discarded, as it corresponds to a trivial and useless solution. Regular offset field specified for nearest-neighbor search over images using zero order predictors and first order predictors.

All offsets smaller than a given threshold are excluded as search is made for the matches relatively far apart from the target, a condition applied implicitly in further developments. The main idea of matching algorithm is to quickly propagate such good offsets, updating iteratively the whole field. In the generic iteration, there are two phases: propagation and random search.

In propagation phase image is raster scanned from top to down and left to right for each pixel s and current offset is updated as:

$$\delta(s) = min_{\emptyset \in P(s)}(D(s),D(s+\emptyset)) \quad (9)$$

Where, $P(s) = \{ \delta(s), \delta(s^{0r}), \delta(s^{0c}), \delta(s^{0d}), \delta(s^{0a}), \delta(s^{1r}), \delta(s^{1c}), \delta(s^{1d}), \delta(s^{1a}) \}$, and zero and first order predictors are:

$$\delta^{0x}(s) = \delta(s^x)$$

$$\delta^{1x}(s) = 2\delta(s^x) - \delta(s^{xx}); \text{ and } x \in \{r,c,d,a\};$$

Here, where s^{xx} is the pixel preceding s^x along direction x in the scanning order, and the diagonal and anti-diagonal directions, d and a, respectively, obtaining eventually the enlarged set of predicted offsets. As a result of this modification, whenever a correct offset field is found over a couple of neighboring pixels it will quickly propagate to the rest of the interested region within two iterations.

4) Step 4: Post processing :we follow the method mentioned in [1] based on dense linear fitting, which comprises the median filtering on circular window ρ_m to remove outliers as minimum mean square error are sensitive to outlier then computation of fitting error (minimum mean square error$\varepsilon^2(s)$) w. r. t. least-squares linear model over a circular neighborhood of radius ρ_n followed by setting threshold based on fitting error $\varepsilon^2(s)$ is selected at level $T\varepsilon$ to keep the complexity limited and remove couples of regions closer than T_d pixels and smaller than T_s pixels and mirroring of detected regions. Finally, morphological dilation with a circular structuring element of radius to obtain mask.

$$\rho_D = \rho_m + \rho_n$$

The values of thresholds are taken as described in [1].

V. RESULTS & DISCUSSIONS

In this section, we present the results of our proposed copy-move move forgery detection technique and examples for copy-move forgeries subjected to many image processing operations. The results are provided both at pixel level and image level. F-Measure is computed for performance measure. F-measure is defined as:

$$F - Measure = \frac{2TP}{2TP + FN + FP} \quad (10)$$

Where, TP is the number of detected forged images, FN is number of undetected forged images and FP is the number of wrongly detected genuine images. Similar definitions are used over pixel level. At image level is the ability to correctly recognize an image is forged or not, while pixel level measures the localization accuracy.

Proposed technique is tested on images from benchmark and grip database. Benchmark dataset consists of 48 true color lossless images and forged images sets by various image processing operations i.e. rotation, scaling, compression, noise and combined effects.

Sr. no.	Type of copy move forgery operations	F-Measure
1	Jpeg Compreesion	0.96
2	Rot	0.97
3	RotExtra	0.92
4	rotExtra2	0.87
6	Cmb_easy	0.97
7	Cmb_extra	0.93
8	Cmb_extra2	0.83

Table 1: F-Measure of Proposed Technique

Examples from Benchmark dataset having multiple copy paste forgeries and extra rotation is illustrated following:

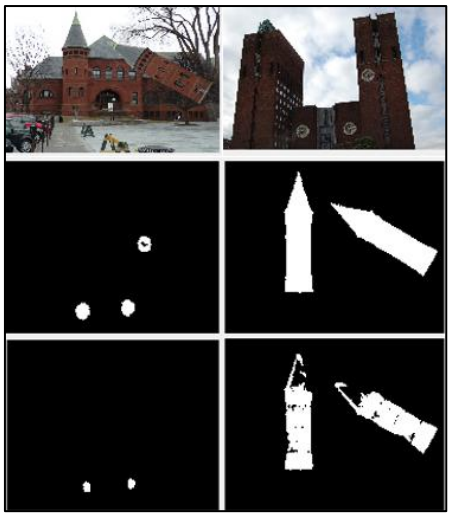

Fig. 3: Forgery detection results with ART and Zernike features. From top: forged image, output by ART features, output by Zernike features[2].

In case of Grip dataset which consists of smooth, structured, rough and textured images. The performance of proposed algorithm is shown following in examples:

Fig. 4: Three forged images from Grip database with different levels of activity and there pixel level F-Meaure. From top:smooth, textured, mixed.

A. Comparison with state of art

As described in Section 3, the image ART features enables us to make full use of their advantages. Compared with other forgery detection methods that use Circular Harmonic Transforms [1] features, the forgery detection results can be improved with the proposed method. Performance of proposed algorithm with testing dataset Grip is given below:

Sr. No.	Technique	F-Measure
1	Amerini 2013	67.72
2	Cozzolino 2015(Zernike)	92.04
3	Proposed Method	94.93

Table 2: F-Measure for Grip Dataset

Computation time of features are less as compare to other feature extractions in [1], as in case of computation of Zernike moments[2] radial functions composite of factorial computation which is simple cosine function in case of ART. Therefore feature computation cost of ART is comparatively less.

Sr. No.	Technique	F-Measure
1	Amerini 2013	67.72
2	Cozzolino 2015(Zernike)	93.04
3	Cozzolino 2015(Zernike-Polar)	94.95
4	Cozzolino 2015(FMT)	89.13
5	Proposed Method	95.91

Table 3: F-Measure for Benchmark Dataset

Experimental results are quite satisfactory, as they show the proposed technique to provide state-of-the-art detection performance, with significant improvements in terms of localization accuracy and speed. The comparative performance measure of existing and proposed technique I represented in Figure 5. The proposed method outperforms for texture, smooth, structured images. Amerini's technique is a keypoint based technique makes the use SIFT feature performs well where dense field method fails i.e. in case of scaled forgeries. ART feature are robust for detection of geometric distortion.

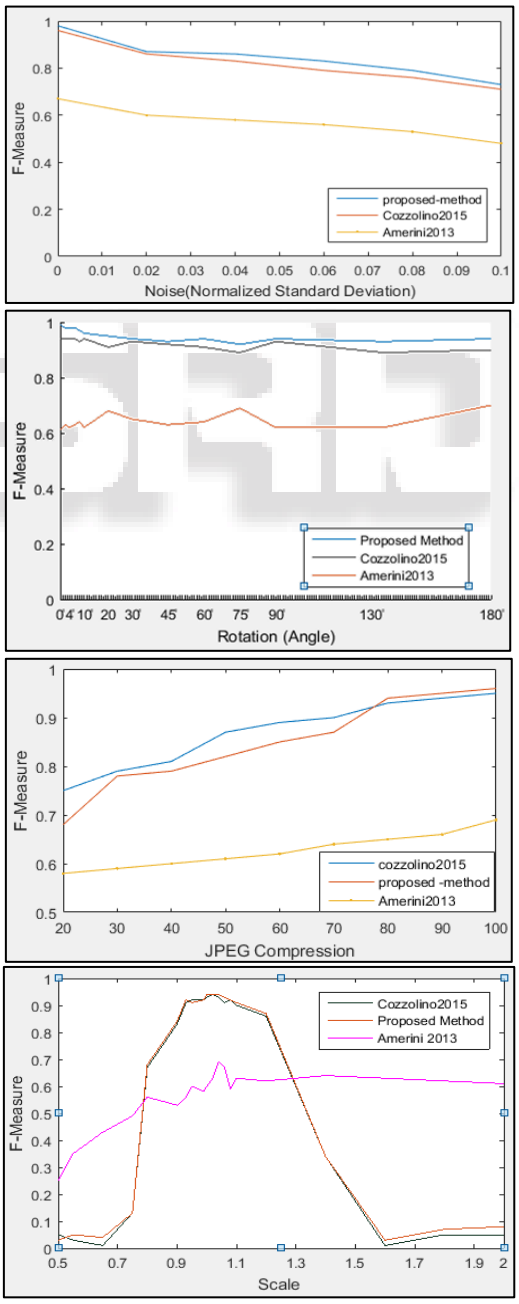

Fig. 5: F-Measure of measure curves for the proposed and reference techniques.

VI. CONCLUSION

As described in Section 3, the image ART features enable us to make full use of their advantages. Compared with other forgery detection methods that use Circular Harmonic Transforms [1] features, the forgery detection results can be improved with the proposed method. The proposed technique performs better in case of rotation and noise present in the image. It outperforms in case of combined forgery attacks present in cmbextra, cmbextra2 and multiple copy paste forgeries present in benchmark dataset. But there is need to work for scaled forgeries. In literature review we have found the techniques for scaled forgeries detection but they does not perform well in case of rotation. Therefore, we suggest that the fusion features which are rotation invariant with those which are scale invariant (and outperforms for scaled forgeries) may provide better results.

REFERENCES

[1] Cozzolino, Davide, Giovanni Poggi, and Luisa Verdoliva (2015), "Efficient dense-field copy–move forgery detection." IEEE Transactions on Information Forensics and Security 10.11.pp. 2284-2297.
[2] Ryu, Seung-Jin, et al. (2013), "Rotation invariant localization of duplicated image regions based on Zernike moments." IEEE Transactions on Information Forensics and Security 8.8, pp. 1355-1370.
[3] D'Amiano, L., et al.(2013) "Video forgery detection and localization based on 3D patchmatch." Multimedia & Expo Workshops (ICMEW), 2015 IEEE International Conference on. IEEE.
[4] D. Cozzolino, G. Poggi, and L. Verdoliva, (2014), "Copy-Move forgery detection based on PatchMatch," in IEEE International Conference on Image Processing (ICIP), Oct. 2014, pp. 5312–5316.
[5] C. Barnes, E. Shechtman, A. Finkelstein, and D. Goldman (2009), "Patchmatch: A randomized correspondence algorithm for structural image editing," ACM Transactions on Graphics, vol. 28, no. 3, pp. 24:1–24:11,
[6] C. Barnes, E. Shechtman, D. Goldman, and A. Finkelstein (2010), "The generalizedpatchmatch correspondence algorithm," in European Conference on Computer Vision (ECCV), vol. 6313. Springer Berlin Heidelberg, pp. 29–43.
[7] V. Christlein, C. Riess, and E. Angelopoulou (Dec. 2010), "On rotation invariance in copy-move forgery detection," in IEEE International Workshop on Information Forensics and Security.
[8] Li, J., Li, X., Bin, Y., Sun, X., 2015. Segmentation-based image copy-move forgery detection scheme. IEEE Trans. Inf. Forensics Secur. 10 (3), 507–518.
[9] Li, L., Li, S., Zhu, H., Chu, S.-C., Roddick, J.F., Pan, J.-S., 2013. An efficient scheme for detecting copy-move forged images by local binary patterns. J. Inf. Hiding Multimed. Signal Process. 4, 46–56.
[10] Pun, C.-M., Yuan, X.-C., Bi, X.L., 2015. Image forgery detection using adaptive oversegmentation and feature points matching. IEEE Trans. Inf. Forensics Secur. 10 (8), 1705–1716.
[11] Kaur, A., & Singh, C. (2012). Cephalometric x-ray registration using angular radial transform. In IJCA Proc. Int. Conf. Recent Advances Future Trends Inf. Technol. (pp. 18-22).
[12] Singh, C. (2012). An effective image retrieval using the fusion of global and local transforms based features. Optics & Laser Technology, 44(7), 2249-2259.
[13] Anuja Dixit and R. K. Gupta," Copy-Move Image Forgery Detection a Review," I.J. Image, Graphics and Signal Processing, 2016, 6, 29-40 Published Online June 2016 in MECS, DOI: 10.5815/ijigsp.2016.06.04

