Detection of Copy-Rotate-Move forgery using Wavelet Decomposition and Zernike moments

Abhishek Kashyap, Megha Agarwal, Hariom Gupta
Department of Electronics and Communication Engineering, Jaypee Institute of Information Technology, Noida-201304, Uttar Pradesh, India.
Email: abhishek.kashyap@jiit.ac.in, megha.agarwal@jiit.ac.in, hariom.gupta@jiit.ac.in

Abstract

To determine whether a particular image is authentic or not is a principal problem in digital image forensics. Many techniques have been proposed to detect clues of intended manipulation in the literature. Copy-move forgery is one of the most commonly used techniques, in which a part of the image is copy and paste it into another part of the same image. In this paper, we propose an efficient and robust algorithm (CMFD-Zernike) for detection of copy-rotate-move forgery using wavelet decomposition and Zernike moments that localizes duplicated regions using Zernike moments. Since the magnitude of Zernike moments is algebraically invariant against rotation, the proposed method can detect a forged region even though copied region is rotated. Our scheme is also resilient to the intentional distortions such as additive white Gaussian noise, JPEG compression, and Scaling. Experimental results demonstrate that the proposed algorithm is appropriate to identify the forged region by copy-rotate-move forgery.

Index Terms: Copy-rotate-move; Wavelet decomposition; Zernike moments; PCA.

1. Introduction

Images play critical role in everybody’s life in our society, which are broadly used as a medium of communication, insurance processing, surveillance systems, intelligence services, forensic investigations, political battles and medical imaging. Today normal client has used to alter the digital photograph through high-resolution digital cameras and computer graphics software. There are two approaches for detection of digital image forgery such as active approach and passive approach [1]. In the Active approach, we insert certain authentic information inside an image at the time of capturing or after capturing, and after that it will be disseminated to the public and In the Passive Approach method, we will never insert any information for authentication purpose, rather it works purely by analyzing binary information of digital image. There are several methods to make forged images, such as removing, replacement, copy-move, copy-create and computer generated media [2]. Copy-move is the most common techniques to make manipulated images. There are some algorithms in the literature to detect copy-move forgery [3]. All of these algorithms can only detect copy-move forgery without any rotation and scaling operation done before pasting. In practice, image seems more natural by performing the operation like scaling and rotation. Such modifications change pixel values, so that the detection algorithms are not efficient for the detection of copy-move image forgery. One approach is applying Fourier-Mellin transform to the blocks [4]. This method performs well when the degree of rotation is small. In other approach, each block is represented by log-polar coordinates [5]. Since the method depends on the pixel values, it is sensitive to the change of the pixel values. To solve such problems, there are some algorithms that extract interest points on the whole image by scale invariant feature transform (SIFT). These algorithms extract special feature points in the given image which are invariants against changes as scaling or rotation. Use of these special feature points instead of pixel blocks makes these algorithms less sensitive against noise or JPEG compression [6]. After extracting SIFT feature, the transform between copied areas are estimated. All
parts of image are compared using their transform. We make a map using these similarities, which shows the probable regions with high likelihood to be duplicated from other regions [18]. As mentioned before these methods cannot detect rotated flat copied regions. This problem can be solved by using Zernike moments. In this paper, we propose an improved framework to deal with that problem of image forgery confinement with the assistance of wavelet decomposition and Zernike moments. Our experimental outcomes demonstrate that the proposed CMFD-Zernike scheme outperforms most prior arts, especially the block-based ones regarding detection rate.

The rest of the paper is organized as follows. A review of image forgery detection is presented in section I. In Section II we present formulation of problem. In section III we propose design of our approach based on wavelet decomposition and Zernike moments of an image for forgery detection. In section IV we provide the computer simulation results. In section V we present conclusions and scope of the future work.

2. Formation of problem

This section investigates problem in parameter setting after a brief description of the block based structure.

Copy-rotate-move forgery detection approaches under the block-based structure may be divided into pre-processing, block tiling, feature extraction, matching, filtering and post-processing as shown in Fig. 1. Pre-processing is used to prepare an image for detection such as converting a RGB image into a grayscale image with standard color space conversion. Block based method is used to subdivided the image in rectangular regions, a feature vector is computed for every such regions. They can be graphed in to singular values of reduced rank. Feature extraction is used to assemble descriptor, i.e. feature vector, it is used for each key point in view of its association with the surrounding pixels. Matching is to determine matched key-points based on feature vector. The regions around the matched key points are probably duplicated regions. Filtering is to eliminate mismatch key points and post-processing is to delete duplicated regions or estimate geometric transformation parameters and so on, when necessary. It depends upon different detection approaches.

3. Design of our approach

The objective of our approach, CMFD-Zernike is to automatically detect copy-rotate-move forgery for each test image. The flow chart of CMFD-Zernike is shown in the Fig. 2. It incorporates elemental detection, which is derived from the block based structure. The initial step is to recognize the input and the output of the block-based framework. The output is just the number of matched blocks. Which is utilized to evaluate whether the outcome is good or not. An evaluation criterion is formed for better outcome, which is basically based on the number of matched blocks.

The proposed elemental detection of digital image forgery method involves the following steps: Wavelet decomposition of the input image; 2) Tiling the image with overlapping grid or block; 3) Zernike moment invariants representation of each overlapping blocks; 4) Principal component analysis; 5) Block similarity analysis; 6) Duplicated regions map creation. In the remaining section, a new image forgery detection algorithm is developed by the means above. To encourage the portrayal, we begin with a \((M\times N)\) dimensional forged image.
3.1 Wavelet decomposition

This method begins with the computation of wavelet transform of the input image, after computing wavelet transform we have low-high bands, high-low bands and high-high bands of the image at different scales, then we have further processed the coarse part of the image for forgery detection.

we have used Harr wavelet, \( \psi(x) \), which is orthogonal to the scaling function and it is defined [21] – [23] as-

\[
\psi(z) = \sum_{m=-\infty}^{\infty} (-1)^m a_{N-1-m} \sqrt{2} \phi(2z - m) \tag{1}
\]

The two dimensional wavelet decomposition function \( f(x; y) \) is defined as [23],

\[
f(z,y) = \sum_{j=-\infty}^{\infty} \sum_{k=-\infty}^{\infty} \sum_{l=-\infty}^{\infty} w_{j,k,l} \psi_j,k(x) \psi_l,j(y) \tag{2}
\]

3.2 Tiling the image with overlapping grid or block

The wavelet decomposed image is being tiled [7] by the block of \((R\times R)\) pixels. This block is horizontally slide by one pixel rightwards starting with the upper left corner and ending with the bottom right corner as shown in Fig. 3. Here the size of the duplicated regions are assumed to be larger than block size and the total number of overlapping blocks are \((M-R+1)\times(N-R+1)\) for an image size of \((M\times N)\) pixels.
3.3 Zernike moment invariants representation of each overlapping blocks

In this step, we have found out Zernike moment of each overlapping blocks. Moments and invariant functions of moments have been extensively used for invariant feature extraction in a wide range of pattern recognition, digital watermark applications and etc [10]- [11]. As moments of image region have the better characteristics to resist the rotation, they have become the main approach to detect the copy-move images. In all kinds of moments of images, Zernike moments have shown to be superior to the others in terms of their insensitivity to image noise, easier to calculate high order moments, and better ability to depict the structural properties [11]- [13]. In this section, how to extract the Zernike moments will be depicted. The Zernike moments [14] of order n with repetition m for a continuous image function f(x, y) that vanishes outside the unit circle are

\[
A_{nm} = \frac{n + 1}{\pi} \int_{x^2 + y^2 \leq 1} f(x, y) V_{nm}^*(\rho, \theta) d\rho d\theta, \quad (3)
\]

where n a nonnegative integer and m an integer such that (n-m) is nonnegative and even. The complex-valued functions \( V_{nm}(x, y) \) are defined by

\[
V_{nm}(x, y) = V_{nm}(\rho, \theta) = R_{nm}(\rho) \exp(jm\theta), \quad (4)
\]

where \( \rho \) and \( \theta \) represent polar coordinates over the unit disk and \( R_{nm} \) are polynomials of \( \rho \) (Zernike polynomials) given by

\[
R_{nm}(\rho) = \sum_{s=0}^{(n-|m|)/2} \frac{(-1)^s [(n-s)!][n^2-s^2]}{s! \left( \frac{n+|m|}{2} - s \right)! \left( \frac{n-|m|}{2} - s \right)!} \rho^{n-2s}, \quad (5)
\]

Note that \( R_{nm}(\rho) = R_{nm}(\rho) \). These polynomials are orthogonal and satisfy

\[
\int_{x^2 + y^2 \leq 1} \left[ V_{nm}^*(x, y) \right] \times V_{pq}(x, y) d\rho d\theta = \frac{\pi}{n+1} \delta_{np} \delta_{mq},
\]

where \( \delta_{ab} = \begin{cases} 1, & a = b \\ 0, & otherwise \end{cases} \quad (6) \)

For a digital image, the integrals are replaced by summations. To compute the Zernike moments of a given block, the center of the block is taken as the origin and pixel coordinates are mapped to the range of the unit circle. Those pixels falling outside the unit circle are not used in the computation. Note that \( A_{nm} = A_{nm} \).

\( \text{Fig. 3.} \) Pixel block scan and array dimensions for the matching algorithm. [20]
Consider a rotation of the image through angle $\alpha$. If the rotated image is denoted by $f'$, the relationship between the original and rotated image in the same polar coordinate is

$$f'(\rho, \theta) = f(\rho, \theta - \alpha). \quad (7)$$

From equation 3 and 4, we can construct

$$A_{nm} = \frac{n + 1}{\pi} \int_0^{2\pi} \int_0^1 f(\rho, \theta)V_{nm}(\rho, \theta)\rho d\rho d\theta \quad (8)$$

$$A_{nm} = \frac{n + 1}{\pi} \int_0^{2\pi} \int_0^1 f(\rho, \theta)R_{nm}(\rho)\exp(-jm\theta)\rho d\rho d\theta \quad (9)$$

Therefore, the Zernike moment of the rotated image in the same coordinate is

$$A'_{nm} = \frac{n + 1}{\pi} \int_0^{2\pi} \int_0^1 f(\rho, \theta - \alpha)R_{nm}(\rho)\exp(-jm\theta)\rho d\rho d\theta \quad (10)$$

By a change of variable $0_1 = 0 - \alpha$,

$$A'_{nm} = \frac{n + 1}{\pi} \int_0^{2\pi} \int_0^1 f(\rho, \theta_1)R_{nm}(\rho)\exp(-jm(\theta_1 + \alpha))\rho d\rho d\theta_1 \quad (11)$$

$$A'_{nm} = \frac{n + 1}{\pi} \int_0^{2\pi} \int_0^1 f(\rho, \theta_1)R_{nm}(\rho)\exp(-jm\theta_1)\rho d\rho d\theta_1 \times \exp(-jm\alpha) \quad (12)$$

$$A'_{nm} = A_{nm} \exp(-jm\alpha). \quad (13)$$

Equation 13 shows that each Zernike moment acquires a phase shift on rotation. Thus $|A_{nm}|$, the magnitude of the Zernike moment, can be used as a rotation invariant feature of the image. Therefore we calculate the magnitude of the Zernike moments to uniquely describe each block regardless of the rotation.

### 3.4 Principal component transformation

In this step we have lessened the dimensionality of Zernike moment invariants of each overlapping blocks, and these blocks are conveying the information related to the course part of wavelet decomposed image. We have diminished the dimensionality using Principal Component Analysis (PCA). Let us consider $\vec{X}$ vector:

$$\vec{X} = (x_1, x_2, x_3, x_4, \ldots x_{m_0}, \ldots x_m) \quad (14)$$

Consider only $m_0$ in $m$, neglect $(m-m_0)$. We do not know where maximum information occurs. So we transform $\vec{X}$ of $m$ dimensional to another space.

$$\vec{T} \cdot \vec{X} = \vec{X}_{new} \quad (15)$$
We have designed T matrix, by which we got $X_{new}$. This vector permits us to chop off the values which are having very low variance, and then we can easily chop off. The above mentioned step is known as Principal Component Transform (PCT) [19].

Projection of random vector $\tilde{X}$ onto unit vector $\bar{q}$.

$$a_i = \tilde{X}^T \cdot \bar{q}_i = \bar{q}_i^T \cdot \tilde{X}$$

where $a_i$ is projection and $\bar{q}_i$ orthogonal basis.

$$\tilde{X} = \sum_{i=1}^{m} a_i \cdot \bar{q}_i$$

$$E[a_i a_j] = \lambda_i \delta_{ij}; \ \delta_{ij} = \begin{cases} 1, & i = j \\ 0, & i \neq j \end{cases}$$

If these equations are satisfy then equation (21) is likewise satisfy, then we have taken Eigen values in decreasing order. After reduction of the dimensionality, we can also reconstruct the coarse part of the wavelet decomposed image using dimension diminished vector.

### 3.5 Block similarity analysis

In this step, the similarity between the sub-blocks is obtained by calculating Euclidean distance. If we found any sub-block has lesser Euclidean distance, at that point, we can say they are similar. This is not a sufficient but a necessary condition. Additionally, we need to check their neighborhood sub-blocks for finding similarity. If their neighborhood is additionally comparable, by then there is a high probability that they are duplicated and they ought to be marked.

The similarity measure $S(B_a, B_b)$ [9] between two sub-blocks $B_a$ and $B_b$ is defined as:

$$S(B_a, B_b) = \frac{1}{1 + \rho(B_a, B_b)}$$

(9)

Where $\rho$ is Euclidean distance between two sub-blocks, $a = 1, 2... (M-R+1) \times (N-R+1)$ and $b = 1, 2... (M-R+1) \times (N-R+1)$.

$$\rho(B_a, B_b) = \left( \sum_{d=1}^{n} (B_a[d] - B_b[d])^2 \right)^{1/2}$$

(10)

If $S(B_a, B_b) > T$, at that point we have further investigated the neighboring blocks of $B_a$ and $B_b$. Threshold (T) is the minimum required similarity and it played a very vital role to obtain the degree of reliability between sub-blocks a and b, which is utilized to make a decision for digital image forgery. We have picked 16 neighboring sub-blocks r with a most extreme separation of 4 pixels from the analyzed sub-block for investigating the neighborhood blocks.
Where $x_r \in 2 (-4, -3, 3, 4)$ and $y_r \in 2 (-4, -3, 3, 4)$ respectively; the corresponding detection results are reported in the fourth column based on MICC-F2000 database.

3.6 Duplicated regions map creation

Duplicated regions map is formed by the multiplication of each element of $I (x, y)$ by its respective element in $Q (x, y)$. 

$$S(b\_block(i + x_r, s + y_r), b\_block(i + x_r, s + y_r)) \geq T \quad (11)$$

$$\sqrt{(a - b)^2 + (s - t)^2} \leq D \quad (12)$$

We have obtained the optimum size of forged area using equation (11) and (12). If the similarity between sub-blocks is more prominent than the threshold T but the separation between them is not as much as the threshold D, then these sub-blocks will not be further analyzed and will not be assigned as a copied region. Threshold D is utilized to decide the minimum separation between the duplicated regions and it plays a vital role to provide more precise outcomes for digital image forgery detection.

Finally, we got an outcome in the form of a matrix $Q$, which will be the same size of the coarse part of the input image. An element of this matrix is set to one if the block at this position is copied otherwise set to zero.
4. Experiments and results

4.1 Metrics

The critical measures are the number of successfully recognized forged images ($T_p$), the number of images that have been falsely recognized as forged ($F_p$) and the erroneously missed forged images ($F_N$) at the image level. From these, we have computed the measures precision ($p$) and recall ($r$). They are characterized as:

$$p = \frac{T_p}{T_p + F_p}, \quad \text{and} \quad r = \frac{T_p}{T_p + F_N} \quad (14)$$

Precision demonstrates the likelihood that a distinguished forgery is a genuinely forged, while recall demonstrates the likelihood that the forged image is recognized. The recall is also known as true positive rate. For a reasonable comparison with all the outcomes obtained from the tested images, localization performance of the forged image is evaluated with the $F_1$-score, which is characterized as:

$$F_1 = 2 \cdot \frac{\text{Precision} \cdot \text{Recall}}{\text{Precision} + \text{Recall}} = \frac{2T_p}{2T_p + F_N + F_p} \quad (15)$$

4.2 Results

In this section we have discussed about the outcomes for the algorithm depicted in section III. We have analyzed different images for detection of copy-move forgery from the MICC-F2000 [24] database. This database is created by 2000 images, in which 700 are tampered and 1300 original images. When we process these images to the proposed algorithm for the detection of copy-move forgery, we have got the possible signs of the tempering. Some examples of original images, tempered images, and their detection results are shown in Fig. 4. Table I shows precision, recall and $F_1$-score for proposed and distinctive existing strategies based on MICC-F2000 and average precision, recall and $F_1$-score of our proposed method are 95.87, 92.59 and 94.20 respectively. We test the robustness of CMFD-Zernike against various attacks, which include plain copy-move, Gaussian noise, JPEG compression, scaling and rotation type of forgery. The duplicated regions will be translated as follows:

- Plain copy-move: Duplicate region is moved to the target location without any additional modification.
- Add Gaussian Noise: The images intensities are normalized between 0 and 1 and add zero mean Gaussian noise with standard deviations of 0.02, 0.04, 0.06, 0.08 and 0.10 to the duplicate regions.
- JPEG compression: It is common global disturbance. The quality factor varied between 100 and 20 in steps of 10 degree.
- Scaling: The duplicate regions are rescaled by 40%, 60%, 80%, 100%, 120%, 140%, 160% and 200%.
- Rotation: The duplicated regions are rotated between 2 to 10 degree in steps of 2 degree, and larger rotation angles of 20, 40, 60, 80 and 180 degree.

Fig. 5 shows the comparison between proposed CMFD-Zernike and existing methods, when adding Gaussian noise. Precision and recall of proposed method have better results and its values would be reduced, when we include zero mean Gaussian noise with standard deviations of 0.02, 0.04, 0.06, 0.08 and 0.10 to the duplicated regions. Fig. 6 shows the comparison between proposed CMFD-Zernike and existing methods, when JPEG compression performed. For plain copy-move forgery, our proposed method has better precision and recall values than the existing methods and its values have reduced, when quality factor fluctuated between 100 and 20 in the steps of 10 degrees. Fig. 7 demonstrates the
comparison between proposed CMFD-Zernike and existing methods, when scaling performed. For plain copy-move forgery, precision and recall have highest values but its values reduced to lower values, when duplicate regions have rescaled by the factor of 40%, 60%, 80%, 120%, 140%, 160% and 200%. Fig. 8 demonstrates the comparison between proposed CMFD-Zernike and existing methods, when rotation performed. For plain copy-move forgery, precision and recall have highest values but its values reduced to lower values, when duplicate regions have rotated between 2 to 10 degree in steps of 2 degree, and larger rotation angles of 20, 40, 60, 80 and 180 degree.

From Table I and Fig. 4-8, it has been observed that the results of our proposed algorithm are superior to the existing methods such as Bravo [15], Wang [16], Blur-moment [7], SIFT [6], SURF [17] and Wavelet Dec. [8]. Finally, we can say that our proposed method performs better with the database, where block based methods have worse results.
Fig. 7. Comparison between proposed CMFD-Zernike and existing algorithms, when scaling operation performed

Table I

<table>
<thead>
<tr>
<th>Methods</th>
<th>Precision (%)</th>
<th>Recall (%)</th>
<th>F1 (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bravo [15]</td>
<td>89.57</td>
<td>91.10</td>
<td>90.33</td>
</tr>
<tr>
<td>Wang [16]</td>
<td>90.46</td>
<td>92.30</td>
<td>91.37</td>
</tr>
<tr>
<td>Blur-moment [7]</td>
<td>89.43</td>
<td>87.21</td>
<td>88.31</td>
</tr>
<tr>
<td>SIFT [6]</td>
<td>88.37</td>
<td>79.17</td>
<td>83.52</td>
</tr>
<tr>
<td>SURF [17]</td>
<td>91.49</td>
<td>89.42</td>
<td>90.44</td>
</tr>
<tr>
<td>Wavelet Dec. [8]</td>
<td>92.13</td>
<td>90.65</td>
<td>91.38</td>
</tr>
<tr>
<td>Proposed CMFD-Zernike</td>
<td>95.87</td>
<td>92.59</td>
<td>94.20</td>
</tr>
</tbody>
</table>
5. Conclusion and scope for future work

In this paper, we propose a novel approach CMFD-Zernike, to detect copy-move forgery in digital images. Comparing with existing work, this paper makes three contributions. (i) It puts forward the concept of applying the Zernike moment to copy-move forgery detection. (ii) It integrates the Zernike moment into the block-based framework to perform copy-move forgery detection. The experimental results demonstrate the high ability of the proposed algorithm to detect copy move forgery in the given image even with the presence of noise, rotation, blur or contrast changes in the copied areas. In this paper we considered Harr basis, but the system performance can be compared with other basis like deubechey’s basis and DCT can also be utilized. Although CMFD-Zernike is applicable to most of the copy-rotate-move forged images, but we observe that the Block based framework methods cannot find reliably matched blocks in uniform texture regions or when the duplicate regions are too small.

References


**Authors Biography**

**Abhishek Kashyap** was born in Kanpur (U.P), India. I did my B.Tech in Electronics & Communication Engineering. I completed my M.Tech in the specialization of Communication Engineering from Indian Institute of Technology (IIT) Delhi, India in the year 2013. Currently I am working as assistant Professor at JIIT Noida, In the Department of Electronics and Communication Engineering.

**Dr. Megha Agrawal** received her B. Tech. degree from I. E. T. M. J. P. Rohilkhand University, Bareilly, Uttar Pradesh, and M. Tech. and Ph.D. degree from Indian Institute of Technology Roorkee. Her major fields of interest are Image Classification, Object Tracking, Medical Imaging, and Face Recognition. She is working as assistant Professor at JIIT Noida, In the Department of Electronics and Communication Engineering.

**Prof. Hariom Gupta** was born in Agra, India. He obtained his B.E. in Electrical Engineering from the Government Engineering College, Jabalpur securing 1st position in Jabalpur University. He received his ME in Systems Engineering and Operations Research and Ph.D. from Indian Institute of Technology, Roorkee in 1975 and 1980, respectively. Before joining JIIT as Director Noida-sector 128 he was working as Professor in the Department of Electrical Engineering and Dean Faculty Affairs, at Indian Institute of Technology, Roorkee, India. Worked as Head, Department of Electrical Engineering from 2002 to 2005, Dean Academic (UGS) 2005-06, Dean Academic (PGS &R) 2007-08, Dean Academic Research 2008-2009 and Dean Academic Studies 2010. He visited McMaster University, Hamilton, Canada, from 1981 to 1983 as a post-doctorate fellow. Dr. Gupta has also visited Iraq, Italy, Spain, USA, Singapore and Oman on various assignments.