Copy-Move Forgery Detection Using Zernike and Pseudo Zernike Moments

Khaled Mahmoud and Arwa Abu-AlRukab
Computer Science Department, Zarqa University, Jordan

Abstract: *Despite the fact that images are a primary source of information, the rapid growing of tools that used to amendment images makes the reliability of the digital images in risk. Copy-Move forgery is one important method to forge an image; where part of the image is copied and pasted in another part of the same image. Regarding the related literature in this topic, many methods were developed to detect Copy-Move forgery; each method has its own strengths and weaknesses. In this paper, the capability and the efficiency of using Pseudo-Zernike Moment (PZM) and Zernike Moments (ZM) in detecting this type of forgery are tested. For evaluating the performance of these methods, comprehensive and authentic dataset is used for testing purposes. The results showed that both methods (PZM-based and ZM-based) are robust against blurring, noise adding, color reduction, brightness change, and contrast adjustments that may affect the image with an acceptable false match. However, rotated and scaled copied region still give weak results. Moreover, the PZM-based method is slightly faster and more accurate than ZM-based method.*

Keywords: *Digital forensics, copy-move forgery, moments, ZM, PZM.*

Received May 9, 2016; accepted June 29, 2016

1. Introduction

Digital image forensics is a research field that aims to validate the authenticity of images by recovering information about their history. It exploits digital image processing principles and analysis tools to recover information about the history of an image. There are many types of digital image forensics such as: format-based, camera-based, pixel-based, printer forensic, …., etc. [21]

Many methods are used to forge images (i.e., creating fake images). They can be categorized into three major groups: Images retouching (enhances or reduces certain feature of an image), image splicing (combine two or more images), and copy-move forgery (region duplication forgery) [18]. Digital image forgery detection methods are classified into two principle approaches; the active approach and the passive approach. With active approach, the signature (watermark) that was embedded in the image is extracted and then used to detect any changes in the image. On the other hand, the passive (blind) approach checks the authenticity of images from an unknown and uncontrolled source [8]. This approach studies inconsistencies in natural image statistics.

Copy-move forgery is one important type of image forgeries. In this type, part of the image is copied and pasted in another part of the same image. Most of the algorithms that were designed to detect this type of forgery compose of a sequence of steps: Dividing the image into overlapped blocks, extracting certain features from each block, comparing features. Finally, blocks that have similar features will be marked as forged parts.

On the other hand, criminals-in order to foil the detection process-change the copied region before pasting them in the new place. These modifications increase the camouflage and the complexity of detecting process. For example, the copied region can be slightly rotated or scaled before pasting them. Moreover, additive noise, blurring and JPEG compression are other types of modifications that may affect the image. Thus the desired algorithm should be robust against any possible modifications.

Regarding the related literature in this topic, all researchers try to develop a robust method against a wide range of possible modification. Actually, rotation and scaling still need more concerns.

In this study, the capability and the efficiency of using Pseudo-Zernike Moment (PZM) and Zernike Moments (ZM) in detecting copy-move forgery were tested. In order to do that, a ZM-based method that was suggested by [23] is implemented and improved. Next, a new method based on PZM is developed and implemented. PZM method is tested against many images with different modification. Finally, a comparison between the two methods is conducted.

For evaluating the performance of detection methods, comprehensive and authentic dataset is used for testing purposes. The strength of both methods are tested against rotation, scaling, blurring, noise adding, color reduction, brightness change, and contrast adjustments that may affect the image blocks.

The outline of this paper is as follows: In section 2, a review of some available relevant literature is given. In section 3, the mathematical background of the image moments is given. Section 4 describes the developed algorithm. Results and comparisons are

given in the section 5 and finally the conclusions are presented in last section.

2. Copy-Move Forgery Detection Methods: General Overview

A very rich literature in the field of copy-move detection focuses mainly on the robustness of the detection method against different modifications, as well as the speed of the method. For this reason, methods are classified according to the selected feature used to check the duplication. However, most of them follow the same pipeline Figure 1.

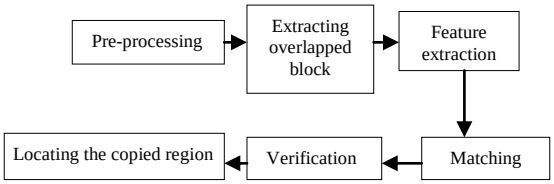


Figure 1. Copy-move detection method pipeline.

This pipeline consist of the following steps [8]:

1. *Preprocessing*: This step is used to improve the computational time by preparing the image for the next step. The most popular operations in this step are: Scale the image down before going on the remaining steps and converting color images into gray scale images. Converting image to gray scale makes its simple to enhance and interprets.
2. *Extracting Overlapped Blocks*: The image is divided into (squared or circular) overlapping blocks. Input image with resolution M×N is divided into (M–B+1)×(N–B+1) squared blocks, where each block is of B×B size.
3. *Feature Extraction*: Here, the representative features of each block are computed. Robustness of these features against different post-processing operations gives better chance in detecting the duplicated areas. Some examples are given in Table 1.
4. *Matching*: The aim of this step is to find the duplicated blocks based on their features descriptor that has been extracted in the previous step. These features are sorted and the high similarity between two features is interpreted as a hint for a duplicated region. Lexicographically sorting [12], and K-D tree [18], the most common sorting methods that were used [5].
5. *Verification*: This step is performed in order to reduce superior matches. This done by grouping matches that jointly follow a same transformation pattern. For example matches that belong to a copied region are expected to be spatially close to each other in both source and target blocks. Furthermore, matches that originate from the same copy-move action should exhibit similar amounts of translation, scaling and rotation.
6. *Locating the copied region:* By coloring or highlighting them.

Many methods were developed for copy-move forgery detection. Table 1 show some methods classified according to the selected feature that were used to represent the image.

Table 1. Copy-move forgery detection method classification.

Class	Feature used
1. Key-point based method.	SIFT [4] and SURF [24].
2. Block-based methods.	
a. Frequency domain-based.	DCT [6, 10, 13], FMT [5], DWT [14].
b. Dimensionality reduction-based.	SVD[27], and PCA[20].
c. Moment-based.	Hu [17] and Zernike[22, 23].
3. Segment-based approaches: the image is segmented using a multi-scale segmentation algorithm.	The image is segmented using a multi-scale segmentation algorithm [15, 19]

According to [8] the most precise copy-move detection results can be achieved using ZM This led us to study the capability and the efficiency of using ZM and PZM in detecting copy-move forgery. Next, a moment overview will be discussed.

3. Moments

The representation of any image is one of the most important points in any image processing application. Some images are represented in spatial domain, others in frequency domain like Discrete Cosine Transformation (DCT). Moreover, moments could be used to represent images. Moments are a way to reduce the image down to be a set of numbers. It is a global description of an image rather than local (i.e., global properties of the image are used rather than local properties) [9, 16].

Depending on the polynomial basis function that may be used, moments are divided into: Geometric moments, complex moments, and orthogonal moments. ZM and PZM are types of orthogonal moments.

3.1. Zernike Moment

ZM can be defined as a set of complete complex orthogonal basis functions that are defined over a unit disk. They were named after optical physicist Frits Zernike, the winner of the 1953 Nobel Prize in Physics. The distinguishing feature of ZM is the invariance of its magnitude with respect to rotation [7].

Zernike Computation: The complex ZM of order *n* with repetition *m* for an image function *f(x, y)* is given in Equation 1 [16].

$$A_{nm} = \frac{n+1}{\pi} \int\int_{x^2+y^2 \le 1} f(x,y)\, R_{nm}(\rho) e^{-im\theta}\, dx\, dy \qquad (1)$$

$$R_{nm}(\rho) = \sum_{\alpha=0}^{\frac{n-|m|}{2}} -1^{\alpha} \frac{(n-\alpha)!}{\alpha!\left(\frac{n+|m|}{2}-\alpha\right)!\left(\frac{n-|m|}{2}-\alpha\right)!} \rho^{n-2\alpha} \qquad (2)$$

Where,

- $n \in z^+$
- $n - |m|\ is\ even$
- $|m| \leq n$
- n = 0, 1 2 ....., m= -p, ...,p
- $R_{nm}(\rho)$: is the radial part of the Zernike basis polynomial
- $e^{-im\theta}$:is the angular part of the Zernike basis polynomial
- (ρ, θ): is the corresponding polar coordinate for *(x, y)*
- $\rho \leq 1$

Similarly, ZM for digital function (image) is given in Equation 3.

$$A_{nm} = \frac{n+1}{\pi} \sum \sum_{x^2+y^2 \leq 1} f(x,y) V^*_{nm}(\rho, \theta) \quad (3)$$

Since, the area of or thogonality is a unit disk Ω= {(x, y)| x^2+y^2≤ 1}, the image f must be scaled down such that it is fully contained in Ω. Those pixels falling outside the unit circle are not used in the computation [11].

Note that: The set of Zernike polynomials contains (n+1)*(n+2)/2linearly independent polynomials if the given maximum degree is n [16].

3.2. Pseudo Zernike Moments

PZM were derived from ZM by releasing the condition" n-|m| is even". However, the set of PZ polynomials has properties analogous to those of Zernike polynomials. The radial part of the Pseudo Zernike basis polynomial R_{nm}(ρ) is then rewritten as it shown in Equation 4:

$$Rnm(\rho) = \sum_{\alpha=0}^{n-|m|} -1^{\alpha} \frac{(2n+1-\alpha)!}{\alpha!(n+|m|+1-\alpha)!(n-|m|-\alpha)!} \rho^{n-\alpha} \quad (4)$$

Where,

- n= 0, 1, 2...∞
- m: is a positive and negative integers subject only to $|m| \leq n$

PZM of order n with repetition m for an image function $f(x, y)$ are defined in Equation 5 [16].

$$B_{nm} = \frac{n+1}{\pi} \sum \sum_{x^2+y^2 \leq 1} f(x,y) R_{nm}(\rho)\, e^{-im\theta} \quad (5)$$

The set of PZ polynomials contains $(n+1)^2$ linearly independent polynomials if the given maximum degree is n [16]. As a result, the set of PZM contains approximately twice as many as ZM. Due to this, the reconstructed image with PZM will catch more details than the conventional ZM of the same order. As mentioned in [16], PZMs are less sensitive to image noise than the conventional ZM. Moreover, their or thogonality property of the polynomials helps in achieving a near zero value of redundancy. So that moments of different orders correspond to independent characteristics of the image [7].

PZM enjoys better performance over the traditional ZM, but they have not been extensively used as feature descriptors due to the high computational complexity of PZ polynomial [3].

3.3. Fast Computation of Zernike Moment and Pseudo-Zernike Moment

The direct computation of ZM and PZM takes a huge amount of arithmetic operations (especially for factorial and exponential part of the equations) and consequently a long time is needed to calculate the moments [2]. In the following subsections, two methods used to accelerate the computation of both ZM and PZM are explained briefly.

3.3.1. Fast Computation of Zernike Moment

There are three main methods which are normally used in ZM calculation: Prata, Kintner and q-recursive. The Prata's method which was developed by Singh and Walia [25] is selected here to be used in order to reduce the time needed to detect the duplicated regions in ZM based method.

Prata method: Prata's algorithm uses polynomials of lower order ($R_{p-1,\ q-1}(r)$, $R_{p-2,q}(r)$) to derive a polynomial of higher order $R_{p,q}(r)$. This calculations given in Equation 6.

$$R_{p,q}(r) = \frac{2pr}{p+q} R_{p-1,q-1}(r) - \frac{p-q}{p+q} R_{p-2,q}(r) \quad (6)$$

Where,

$$R_{pp}(r) = r^p, R_{p,-p}(r) = r^p, R_{p,-q}(r) = R_{p,q}(r) \quad (7)$$

According to the above formulas, the Zernike polynomial can be calculated by the following steps:

1. Compute $R_{pp}(r)$, where p = 0, 1, 2, ...P_{max}.
2. Compute $R_{p,0}(r)$ using the direct equation (Equation 2), where P = 1, 2, ...P_{max}
3. Compute the remaining values $R_{pq}(r)$, where $p \neq q$ and $q \neq 0$

3.3.2. Fast Computation of Pseudo-Zernike Moment

A method that is appeared in [3] is selected to be implemented in order to reduce the time needed to detect the duplicated regions in our proposed method (PZM-based method). Al-Rawi addresses a two-stage p-recursive algorithm where a couple of recurrence relations are specifically derived for PZ radial polynomials and their coefficients for fast computation of PZM. The first stage is shown in Equation 8 and the second stage is shown in Equation 9:

$$R_{pq}(r) = (L_1 r + L_2) R_{p-1,q}(r) + L_3 R_{p-2,q}(r) \quad (8)$$

$$R_{p,p-1}(r) = (2n+1) R_{pp}(r) - 2n R_{p-1,p-1}(r) \quad (9)$$

Where

$$L_1 = \frac{(2p+1)(2p)}{(p+q+1)(p-q)}$$
$$L_2 = -2p + \frac{(p+q)(p-q-1)}{(2p-1)} L_1$$
$$L_3 = (2p-1)(p-1) - \frac{(p+q-1)(p-q-2)}{2} L_1 + 2(n-1)L_2$$

According to the above equations, PZ polynomial can be calculated by the following steps:

1. Compute $R_{pp}(r)=r^p$, where $p = 0, 1, 2,.....P_{max}$
2. Compute $R_{p, p-1}(r)$, where $p = 1, 2,.....P_{max}$
3. Compute the remaining values $R_{pq}(r)$, where p-q≥2

4. PZM-based Copy-Move Detection Method

In this section, a proposed PZM-based method is explained in detail as well as ZM-based method that was developed by Ryu *at el*. [23] is introduced. These two methods will be used to exploits the ability of PZM and ZM as a feature descriptor in order to detect copy-move forgery.

4.1. PZM-based Method

The main steps related to PZM-based method are as follows:

1. The RGB color image is converted into gray-scale image and resized (scale down) to be 512*512 as a preprocessing step. This is because gray-scale image is simple to enhance and interprets. Moreover, the resizing of the image will reduce the execution time for each image.
2. The image with size N×N is partitioned into overlapping blocks of size B×B, assuming that the pre-defined size of a block is smaller than the tampered region. The number of blocks (N of B) equal (N–B+1)×(N–B+1).
3. B_{nm} Vector is calculated (using Equation 5) for each block. The vectorB_{nm} are stored in a 2-D array (PZ) of size (N of B *number of moments), where number of moment sequal $(n+1)^2$.
   Note that:
   - In order to calculate B_{nm}; only the order n is given to the function. This function generates all moments of order 0 up to n with all available repetition m, where $|m|\leq n$.
   - P-recursive method which was explained in section 3.3 is used here in order to accelerate the process of computing B_{nm} for each block.
4. PZ is lexicographically sorted in $\hat{Z}$, so that blocks with similar features become close to each other.
5. For every two adjacent blocks in the sorted array $\hat{Z}$ calculate the Euclidian distance (E_{Dist}) and the Physical distance (Ph_{Dist}) between them. The adjacent block in the sorted array could be the next block in the array or the q^{th} next. Let's say that the index of the two vectors are p and $p+q$, then the two vectors can be represented as:
   $\hat{Z}_p = (\hat{z}_1^p, \hat{z}_2^p, \cdots, \hat{z}_{Nmoment-1}^p, \hat{z}_{Nmoment}^p)$
   $\hat{Z}_{p+q} = (\hat{z}_1^{p+q}, \hat{z}_2^{p+q}, \cdots, \hat{z}_{Nmoment-1}^{p+q}, \hat{z}_{Nmoment}^{p+q})$
   E_{Dist} can be calculated using Equation 10.

$$E_{Dist} = \sqrt{\sum_{r=1}^{Nmoment} (\hat{z}_r^p - \hat{z}_r^{p+q})^2} \quad (10)$$

   and Ph_{Dist} can be calculated using Equation 11.

$$Ph_{Dist} = \max(|x_1 - x_2|, |y_1 - y_2|) \quad (11)$$

   Where (x_1, y_1), (x_2, y_2) are the coordinates of the top left corner of the two blocks.
6. Now, if the tested pair satisfies the following two conditions, then they are candidate to be a copy-move case (i.e., duplicated parts). These two conditions are:

a. E_{Dist} is smaller than a pre-defined threshold D_1 ($E_{Dist}<D_1$).
b. Due to the fact that the neighboring blocks might result in relatively similar PZM, then Ph_{Dist} should be greater than a pre-defined threshold D_2 ($Ph_{Dist}>D_2$). Here, D_2 is related to block size (B).

7. For all candidates blocks resulted from the previous step update the shift vector. The shift vector maintain a counter for each (row, column) shift. This counter represents number of duplicated regions that have the same shift. The shift between two blocks is equal to (x_1-x_2, y_1-y_2), where (x_1, y_1), (x_2, y_2) are the coordinates of the top left corner of the two blocks.
8. Finally, all candidate blocks (step 6) that their shift gain a counter greater than a predefined threshold (C) are marked as a copied region. This can be done by coloring them with a same color.

Thresholds Used: The following thresholds were used in this method: Block size (B), order of moment (n), EDist ($D1$), physical distance ($D2$), and minimum shift counter (C).

4.2. Zernike Moment-based Method

This method which was developed by [4] is implemented with some modifications. Actually, Ryu *et al*. [23] doesn't mention in his paper weather he uses shift vector nor any accelerated method to calculate the ZM. Here, and in order to do the comparisons two main modifications are implemented:

1. Prata method is used to accelerate the process of computing ZM for each block.
2. The idea of shift vector is added in order to get more accurate results.

Ryu *et al*. [23] method is similar to PZM method except:

1. A_{nm} of particular degree n are calculated for each block- using Equation 3.
2. The number of moments calculated for each block is calculated using the following Equation:

$$Nmoments = \sum_{i=0}^{n} \left(\left\lfloor \frac{i}{2} \right\rfloor + 1 \right) \quad (12)$$

3. Physical distance between two blocks is calculated using the following Equation:

$$Ph\_Dist = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2} \quad (13)$$

Where (x_1, y_1), (x_2, y_2) are the coordinates of the top left corner of the two blocks.

PZM-based method and ZM-based method were implemented using Mat lab 7.10.0 (R2010a) in 64-bit, 2GB RAM, and core i5-2540M CPU @ 260 GHz. In the next section, the experimental setup and results will be shown.

5. Experimental Results and Comparisons

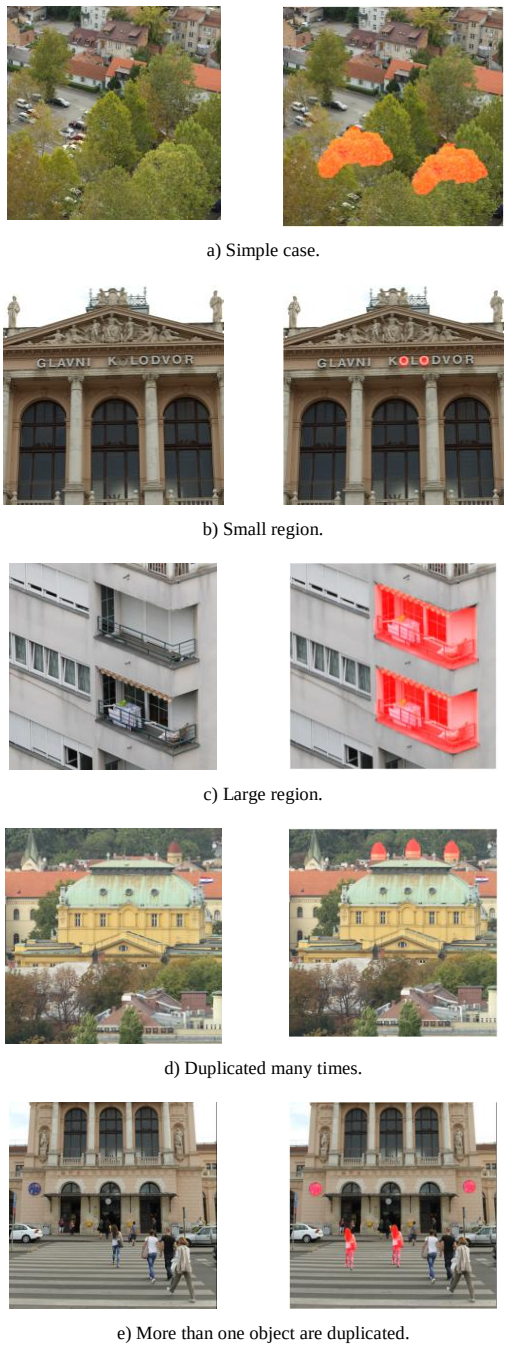
The main dataset that has been used in this experimental part is COMOFOD database [26], which consists of 260 forged images in two categories (small 512×512, and large 3000×2000). Images are grouped in 5 groups according to the applied manipulation: translation, rotation, scaling, combination and distortion. Different types of post processing methods, such as JPEG compression, blurring, noise adding, and color reduction ..., are applied to some forged images. Also, two other datasets are exist: CMFD [8], and MICC-F220 [4].

5.1. Testing Pseudo-Zernike Moment-based Method

The following are some experiments that have been used to test PZM-based method [1]:

1. *Normal Copy-Move Forgery:* In this experiment 50 forged images without any modifications (i.e., no modification is applied on the copied region) were selected. All forged regions have been detected with a high degree of accuracy. Figure 2-a is an example of forged image where a tree branch from the original image is pasted in the same image to hide some cars (orange parts indicate that these parts are duplicated). Moreover, PZM-based method is able to detect -with a high accuracy- the forged regions even if they were:

- Too small, like the image in Figure 2-b,
- Too large, like the image in Figure 2-c,
- Duplicated many times as in Figure 2-d,
- More than one different region copied and pasted in the same image), see Figure 2-e.



a) Simple case.

b) Small region.

c) Large region.

d) Duplicated many times.

e) More than one object are duplicated.

Figure 2. Normal copy-move forgery experiment. Left images are the original images. Right images are the forged images after being detected.

2. *Post-Processing Methods:* In this experiment five different types of post-processing methods were applied on images in COMOFOD database. These methods are noise adding, image blurring, brightness change, color reduction and contrast adjustments. The parameters used for each image are shown below each one.

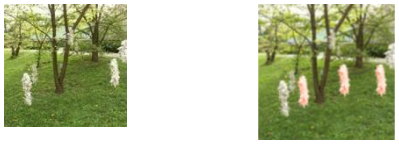
- *Color Reduction:* In this experiment 60 forged images were used. These images are affected by color reduction to 32, 64 or 128 per each color channel. The results show that the entire tampered region is detected with high accuracy. One example is shown in Figure 3-a.

- *Additive Noise*: In this experiment 30 forged images were used. These images are affected by additive Gaussian white noise with zero mean ($\mu=0$) and different values of variance (σ^2 = [0.009, 0.005, 0.0005]). The results was good except some false match in some cases (the orange color cover some area around the forged object). Figure 3-b is an example.
- *Contrast Adjustments*: In this experiment the intensity values of 30 forged images were mapped to a new interval bounded with lower and upper bound such as: [(0.01, 0.95), (0.01, 0.9), (0.01, 0.8)]. Figure 3-c shows a one example for accurate result.
- *Blurring*: In this experiment 30 forged images were used. These images are obtained by convolving the image with 3×3, 5×5 or 7×7 averaging filters. The results show that the entire tampered region is detected with a high accurately. Figure 3-d is an example.
- *Brightness Change*: Changing the brightness of the image was obtained by mapping the intensity values of the original image that were between lower and upper bound (like [(0.01, 0.95), (0.01, 0.9), (0.01, 0.8)]) to interval [0, 1]. Intensity values below lower bound and above upper bound were saturated to minimal and maximal value [26]. Results of 60 images that were used show that the entire tampered region is detected with high accuracy. One example is shown in Figure 3-e.

a) Color reduction by 128 per each color channel.

b) Additive guassian noise (μ =0, σ^2= 0.0005).

c) Contrast adjustments with interval=(0.01, 0.8).



d) Blurring by convoloving the image with [3x3] average filter.

e) Brightness change with interval=[0.01, 0.8].

Figure 3. Detecting forgeries under different set of modifications. Left images are the original images. Right images are the forged images being detected.

3. *Rotation and Scaling:* In this part, the algorithm is examined against rotation-a copied region is rotated and translated to a new location; and scaling-a copied region is scaled and translated to a new location.

- *Rotation:* In this experiment 30 forged images were used. The copied region is affected by rotation with different angles. Results were not perfect but they are acceptable as shown in Figure 4-b.
- *Scaling:* In this experiment 30 forged images were used. The copied region is affected by scaling with different scaling ratio. Results were not acceptable perfectly as shown in Figure 4-c.

a) Original Image.

b) Rotation by 4 degrees.

c) Scaling down to 70% of the original.

Figure 4. Detecting forgeries under rotation and scaling. Left images are the forged images. Right images are the forged images after being detected.

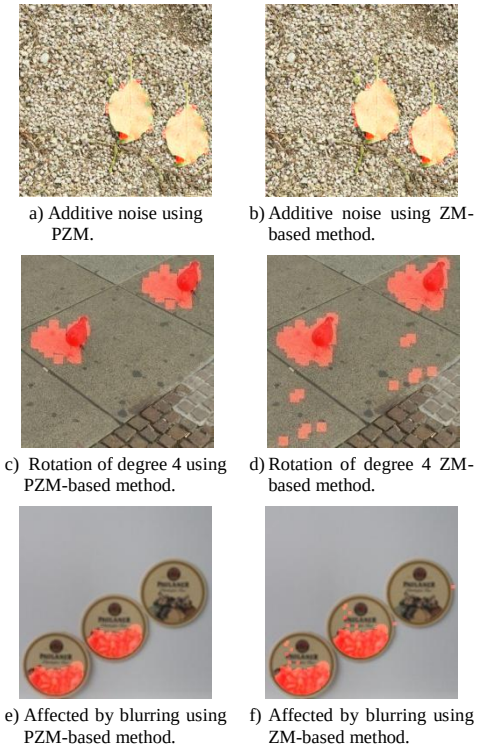
5.2. Comparisons Between Pseudo-Zernike Moment-based Method and ZM-based Method

30 forged images were used in the comparison phase. Each image is tested using ZM-based method and PZM-based method. It is noted that:

1. ZM-based method and PZM based method are very good in detection copy-move forgery for images that are not affected by any modification, but for images that affected by rotation, scaling, blurring … etc., PZM gives better results in less time.
2. In most cases PZM-based method need less time to detect the forged parts comparing to ZM-based method. Figures 5-a and 5-b is an example of image that a affected by additive noise, average filter [3×3], and scaling 96%. PZM-based method can detect the forged parts using moment of order (n=1) in 126 second, while ZM-based method can detect

the forged parts using moment order (n=2) in 144 second.

3. For images that affected by rotation, PZM-based method gives more accurate results than ZM-based method. Figures 5-c and5-d is an example of image that a affected by rotation of degree 4.
4. For images that affected by blurring, PZM-based method gives more accurate results, than ZM-based method. Figures 5-e and 5-f is an example of image that a affected by blurring.



a) Additive noise using PZM. b) Additive noise using ZM-based method.

c) Rotation of degree 4 using PZM-based method. d) Rotation of degree 4 ZM-based method.

e) Affected by blurring using PZM-based method. f) Affected by blurring using ZM-based method.

Figure 5. Images after detecting copy-move for gery using PZM-based method (left) and ZM-based method (right).

6. Conclusions

In this study, copy-move forgery detection method based on PZM is developed. The p-recursive algorithm was used to calculate PZM, in order to reduce the time. Then, PZM-based method is compared with ZM-based method that was mentioned in [23] after doing some improvements.

More than 200 images were used to evaluate the proposed method, these images selected mainly from COMOFOD [26]. The tested images cover all cases that may occur; duplicating an object more than one time, duplicating more than one object, and make some modifications in the copied objects like scaling, rotation, adding noise, or blurring,… etc.

The results showed that PZM-based method can detect all forged images without any pre/post processing with accurate results, all forged images with more than one copied object. It is robust against contrast adjustments and color reduction, and against - but with little false match- brightness change, noise adding, and image blurring. Finally, its ability to detect rotated and scaled parts is weak and there was some false match.

The results of the comparisons between PZM- based method and ZM- based method showed that PZM-based method is better in detecting the duplicated areas that affected by additive noise, rotation, scaling and need less time. PZM-based method can detect the duplicated areas in less time comparing with ZM based method.

Acknowledgment

This research is funded by the deanship of scientific research at Zarqa University/Jordan.

References

[1] Abu-AlRukab A., *A Robust Method for Copy-Move Forgery Detection*, The Zarqa University, 2016.

[2] Al-Rawi M. and Yang J., "Practical Fast Computation of Zernike Moments," *Journal of Computer Science and Technology*, vol. 17, no. 2, p. 181-188, 2002.

[3] Al-Rawi M., "Fast Computation of Pseudo Zernike Moments," *Journal of Real-Time Image Processing*, vol. 5, no. 1, pp. 3-10, 2010.

[4] Amerini I., Ballan L., Caldelli R., Del Bimbo A., and Serra G., "A SIFT-Based Forensic Method for Copy-Move Attack Detection and Transformation Recovery," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 1099-1110, 2011.

[5] Bayram S., Sencar H., and Memon N., "An Efficient And Robust Method For Detecting Copy-Move Forgery," *in Proceeding of IEEE International Conference on Acoustics, Speech and Signal Processing*, Taipei, pp. 1053-1056, 2009.

[6] Cao Y., Gao T., Fan L., and Yang Q., "A Robust Detection Algorithm for Copy-Move Forgery in Digital Images," *Forensic Science International*, vol. 214, no. 1-3, pp. 33-43, 2012.

[7] Chong C., Raveendran P., and Mukundan R., "Translation Invariants of Zernike Moments," *Pattern Recognition*, vol. 36, no. 8, pp. 1765-1773, 2003.

[8] Christlein V., Riess C., Jordan J., Riess C., and Angelopoulou E., "An Evaluation of Popular Copy-Move Forgery Detection Approaches," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 6, pp. 1841-1854, 2012.

[9] Flusser J., Suk T., and Zitová B., *Moments and Moment Invariants in Pattern Recognition*, Wiley Publishing, 2009.

[10] Gupta A., Saxena N., and Vasistha S., "Detecting Copy Move Forgery using DCT," *International Journal of Scientific and Research Publications*,

vol. 3, no. 5, pp. 3-6, 2013.
[11] Hosny K., "Fast Computation of Accurate Pseudo Zernike Moments for Binary and Gray-Level Images," *The International Arab Journal of Information Technology*, vol. 11, no. 3, pp. 243-249, 2014.
[12] Hu J., Zhang H., Gao Q., and Huang H., "An Improved Lexicographical Sort Algorithm of Copy-Move Forgery Detection," *in Proceeding of 2nd International Conference on Networking and Distributed Computing*, Beijing, pp. 23-27, 2011.
[13] Kumar S., Desai J., and Mukherjee S., "Copy Move Forgery Detection in Contrast Variant Environment using Binary DCT Vectors," *International Journal of Image, Graphics and Signal Processing*, vol. 7, no. 6, pp. 38-44, 2015.
[14] Li G., Wu Q., Tu D., and Sun S., "A Sorted Neighborhood Approach for Detecting Duplicated Regions in Image Forgeries Based on DWT and SVD," *in Proceeding of IEEE International Conference on Multimedia and Expo*, Beijing, pp. 1750-1753, 2007.
[15] Li J., Li X., Yang B., and Sun X., "Segmentation-Based Image Copy-Move Forgery Detection Scheme," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 3, pp. 507-518, 2015 .
[16] Liao S., *Image Analysis by Moments*, The University of Manitoba, 1993.
[17] Liu G., Wang J., Lian S., and Wang Z., "A Passive Image Authentication Scheme for Detecting Region-Duplication Forgery with Rotatio," *Journal of Network and Computer Applications*, vol. 34, no. 5, pp. 1557-1565, 2011.
[18] Mahdian B. and Saic S., "Detection of Copy-Move Forgery Using a Method Based on Blur Moment Invariants," *Forensic Science International*, vol. 171, no. 2-3, pp. 180-189, 2007.
[19] Muhammad N., Hussain M., Muhamad G., and Bebis G., "A Non-Intrusive Method for Copy-Move Forgery Detection," *in Proceeding of 7th International Symposium*, Nevada, pp. 516-525, 2011.
[20] Popescu A. and Farid H., "Exposing Digital Forgeries by Detecting Duplicated Image Regions," Technical Report Department of Computer Science, 2004.
[21] Redi J., Taktak W., and Dugelay J., "Digital Image Forensics: A Booklet for Beginners," *Multimedia Tools and Applications*, vol. 51, no. 1, pp. 133-162, 2011.
[22] Ryu S., Kirchner M., Lee M., and Lee H., "Rotation Invariant Localization of Duplicated Image Regions Based on Zernike Moments," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 8, pp. 1355-1370, 2013.
[23] Ryu S., Lee M., and Lee H., "Detection of Copy-Rotate-Move Forgery Using Zernike Moments," *Information Hiding*, vol. 6387, pp. 51-65, 2010.
[24] Shivakumar B. and Santhosh-Baboo S., "Detection of Region Duplication Forgery in Digital Images Using SURF," *International Journal of Computer Science*, vol. 8, no. 4, pp. 199-205, 2011.
[25] Singh C. and Walia E., "Fast and numerically stable methods for the computation of Zernike moments," *Pattern Recognition*, vol. 43, no. 7, pp. 2497-2506, 2010.
[26] Tralic D., Zupancic I., Grgic S., and Grgic M., "CoMoFoD New Database for Copy-Move Forgery Detection," *in Proceeding of 55th International Symposium ELMAR*, Zadar, pp. 49-54, 2013.
[27] Zhang T. and Wang R., "Copy-move Forgery Detection Based on SVD in Digital Image," *in Proceeding of the 2nd International Congress on Image and Signal Processing*, Tianjin, pp. 1-5, 2009.

Khaled Mahmoud received a BSc in Computer Science from Jordan University in 1992, MSc in Computer Science (Artificial Intelligence) from Jordan University in 1998 and a PhD in Print Security and Digital Watermarking from Loughborough University (uk) in 2004. This was followed by academic appointments at Zarqa University (Assistance Professor in computer Science). His areas of interest include Information Security, Digital watermarking, Image processing, AI and Arabic Language processing.

Arwa Abu Al-Rukab received the BA degree in computer science from the Jordan University of science and technology, Jordan in 2008. She received MSc degree of computer science from Zarqa University , Jordan, in 2016. Currently, she worked at Colleges of Computing and Information Society. Her research interests are in Image Processing and Machine learning.