SIViP (2017) 11:785–792
DOI 10.1007/s11760-016-1023-1

ORIGINAL PAPER

A new Zernike moments based technique for camera identification and forgery detection

O. M. Fahmy[1]

Received: 15 April 2016 / Revised: 22 October 2016 / Accepted: 11 November 2016 / Published online: 29 November 2016

Abstract In multimedia forensics, it is important to identify those images that were captured by a specific camera from a given set of N data images as well as detecting the tampered region in these images if forged. This paper presents a new technique based on Zernike moments feature extraction for blindly classifying correlated PRNU images as well as locating the tampered regions in image under investigation. The proposed clustering algorithm is based on estimating the Zernike moments and applying a hierarchical clustering for classification. The forgery detection algorithm is based on picking up the peak *Euclidean* distance between the Zernike moments vector of blocks of the scaled-down forged image and its corresponding ones in the capturing camera PRNU. As Zernike moments are scale and rotational invariant, its feature when computed using scaled-down PRNU images lead to considerable computation time saving. Simulation examples are given to verify the effectiveness of the proposed techniques when compared to other state-of-the-art techniques even in case of very weakly correlated PRNU.

Keywords Camera identification · Forgery detection · Camera fingerprint · Zernike moments

1 Introduction

There is an increasing demand for a series of reliable digital forensic techniques for using in security and privacy applications. This is due to the ease of manipulating digital images. Investigating the sources cameras and detecting the tampered regions in forged images are the most important forensic tasks. This goal is achieved using the Photo Response Non-Uniformity (PRNU) [1–3] as it uniquely identifies images captured by this camera and can be used to identify the forged regions in those images.

The paper objectives are concerned with image clustering and forgery detection. Image clustering can be defined as: given a group of data images captured by a set of unknown cameras, it is required to assign each source image to its mother camera. In forgery detection case, the goal is to find the tampered region, if found, in the image under investigation. Many techniques were proposed for image classifications. These techniques depend on setting a certain threshold to decide whether an image belongs to a specific cluster or not [4–7]. Another clustering algorithm based on hierarchical clustering that does not require a predefined number of clusters was proposed in [8,9]. Different classification systems based on Multi-Class Spectral Clustering MCSC and its improved version using the Normalized Cuts were proposed in [10,11]. However, in view of no prior knowledge about the images, all these clustering techniques suffer from poor performance and requiring a stopping criterion to limit the number of clusters. Recently, a Hu's moments-based clustering algorithm was proposed [12,13]. Although it overcomes most of previous drawbacks, it is computationally expensive and suffers from poor performance in case of weakly correlated images.

Part I of this paper addresses the proposed clustering technique. It is based on incorporating hierarchical clustering with Zernike moments in the clustering algorithm [21–23]. Simulation results of several examples have indicated that this technique significantly reduce the computation time needed beside overcoming most of the shortcomings of other proposed clustering techniques.

✉ O. M. Fahmy
omar.fahmy@fue.edu.eg;
omarfarouk_mamdouh@hotmail.com

[1] Electrical Engineering Department, Future University in Egypt, Cairo, Egypt

Part II is concerned with forgery detection. In this respect, many forgery detection techniques were proposed [14–19]. The basic idea of forgery detection is to check whether or not the PRNU of a certain region matches its corresponding region in the camera PRNU. In [14], the decision threshold c_{min} is based on incorporating Bayesian estimation with Neyman–Pearson criterion. Quite recently [17], the estimation of the decision threshold has been improved through modeling the pixel's spatial dependencies using Markov Random Field (MRF), together with employing non-local means denoizing. Some techniques suggested using adaptive block sizes [18]. Recently, a Natural Preserving Transform [20] forgery detection technique was proposed [19] to detect forgeries in weakly correlated images. The main drawbacks of these approaches, apart from excessive computation time, are that they are all of the second-order-based techniques and, therefore, failed to locate forgeries when the PRNUs are very weakly correlated with its mother camera.

In this paper, the proposed forgery detection algorithm is based on identifying the peak *Euclidean* distances between the Zernike moments of blocks of the forged image and its corresponding ones in the camera PRNU. Simulation results have shown that the proposed algorithm is capable of detecting forgeries copy-paste, copy-move and spliced forged images.

The paper is organized as follows: Sect. 2 briefly describes the theory of Zernike moments. In Sect. 3, the proposed Zernike-based clustering algorithm is described. Section 4 describes the proposed Zernike-based forgery detection scheme. Simulation results for the proposed techniques are given in Sect. 5. Section 6 concludes the paper. In this paper, capital letters will denote matrices, e.g., K while bold letters denote vectors, e.g., x and small italic letters for variables.

2 Zernike moments theory

The most important task in the proposed classification design and forgery detection systems is feature extraction from the image under investigation. It is well known that images are uniquely identified from its 2-D moments. There are various kinds of moments, such as geometric moments and orthogonal moments [21–23]. In this paper, orthogonal Zernike moments were used due to its unique features of being rotational or scaling down invariant. This means that the features of a large image are the same as the feature of its scaled-down one when computed by Zernike moments. The orthogonal Zernike polynomial $V_{r,s}(x, y)$ decomposes a 2-D function $f(x, y)$ as

$$f(x, y) = \sum_{r} \sum_{s=-r}^{r} A_{r,s} V_{r,s}(x, y)$$

where $V_{r,s}(x, y)$ is given by

$$\begin{aligned} V_{r,s}(x, y) &= V_{r,s}(\rho \cos\theta, \rho \sin\theta) \\ &= R_{r,s}(\rho) e^{js\theta}, \quad r - |s| = \text{even} \end{aligned}$$

$R_{r,s}(\rho)$ is known as the radial polynomial and is given by

$$R_{r,s}(\rho) = \sum_{k=0}^{\frac{r-|S|}{2}} (-1)^k \frac{(r-k)!}{k!\left(\frac{r+|s|}{2} - k\right)!\left(\frac{r-|s|}{2} - k\right)!} \rho^{r-2k} \quad (1)$$

where ρ is the vector from the origin to the (x, y) point, while θ is its angle with the x-axis $(0 \leq \theta \leq 2\pi)$. The Zernike polynomials constitute a set of polynomials, orthogonal on the unit disk $\sqrt{x^2 + y^2} \leq 1$, i.e.,

$$\iint_{\sqrt{x^2+y^2} \leq 1} V_{r,s}(x, y) \Big(V_{p,q}(x, y) \Big)^* dxdy = \frac{\pi}{r+1} \delta_{rp} \delta_{sq}$$

where the asterisk * denotes the complex conjugate $A_{r,s}$ is known as the Zernike moment of order r and repetition s $(r - |s| = even, |s| \leq r)$. It is given by

$$\begin{aligned} A_{r,s} &= \frac{r+1}{\pi} \iint_{x^2+y^2 \leq 1} f(x, y) \Big(V_{r,s}(\rho, \theta) \Big)^* dxdy \\ &= \frac{r+1}{\pi} \int_0^{2\pi} \int_0^1 f(\rho, \theta) R^*_{r,s}(\rho, \theta) e^{-js\theta} \rho d\rho d\theta \quad (2) \end{aligned}$$

Due to the condition $r - |s| = even$ and $|s| \leq r$, the number of Zernike moments for an order r is $\frac{(r+1)(r+2)}{2}$ elements. However, as $A^*_{r,s} = A_{r,-s}$, we only need to compute the Zernike moments for $s \geq 0$. If $f(x, y)$ is rotated by an angle θ_0, i.e., $f'(\rho, \theta) = f(\rho, \theta - \theta_0)$. Then the rotated Zernike moment $A^{rot}_{r,s}$ is

$$\begin{aligned} A^{rot}_{r,s} &= \frac{r+1}{\pi} \int_0^{2\pi} \int_0^1 f'(\rho, \theta) R^*_{r,s}(\rho, \theta) e^{-js\theta} \rho d\rho d\theta \\ &= \frac{r+1}{\pi} \int_0^{2\pi} \int_0^1 f(\rho, \theta + \theta_0) R^*_{r,s}(\rho, \theta) e^{-js\theta} \rho d\rho d\theta \\ &= A_{r,s} e^{-js\theta_0} \quad (3) \end{aligned}$$

Equation (3) indicates that the magnitude of the Zernike moments of a rotated function remains invariant. Similarly, one can easily show that in case of scaling down function, its Zernike moments still invariant. At this point, it is worth mentioning that if $f(x, y)$ is an $N \times L$ digital image, then the double integration in Eq. (2) is replaced by a double summation, i.e.,

$$\begin{aligned} A_{r,s} =& \frac{r+1}{\pi} \sum_{j=0}^{L-1} \sum_{i=0}^{N-1} f(x_i, y_j) V^*_{r,s}(x_i, y_j) \Delta x_i \Delta y_j \\ & \text{subject to } x_i^2 + y_j^2 \leq 1 \quad (4) \end{aligned}$$

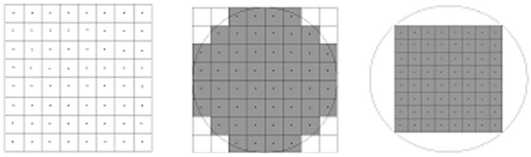

Fig. 1 **a** 8×8 image. **b** Image included unit circle. **c** Unit circle includes image

The (x_i, y_j) is the (i, j) pixel when mapped into the unit disk by a mapping transform. If the center of a pixel fall inside the border of unit disk $x^2 + y^2 \leq 1$, this pixel will be used in computing Eq. (4), otherwise it is discarded. This leads to a geometric error as not all pixels in the $N \times L$ image are included in the unit disk [21,22]. This geometric error can be eliminated by including the whole image inside the unit disk [21,22]. Figure 1 illustrates these concepts. Similarly, one can easily show that in case of scaling down function, its Zernike moments still invariant.

3 The proposed Zernike clustering technique

In this section, a clustering technique based on incorporating hierarchical clustering with Zernike moments is proposed. The hierarchical has an important feature that it does not require a predefined number of clusters. On the other hand, the higher order moment features of Zernike moments yield more information about the image than the correlation-based second-order techniques. The *Silhouette* coefficient are used in the hierarchy process.

The proposed clustering algorithm starts by an initialization step that:

1. Estimate the image PRNU K_I, for each image I_j for an N image dataset as described in [1–3].
2. Each K_I is resized using a decimation factor L.
3. Estimate the Zernike moments $A_{r,s}^{j}$, $j = 1, \ldots, N$ for each decimated K_I as described in Sect. 2.

The clustering process now proceeds as follows:

(a) Compute the $N \times N$ distance matrix $Dist = [d_{i,j}]$, $i, j = 1, \ldots, N$

$$d_{i,j} = ||A_{r,s}^{i} - A_{r,s}^{j}||$$

(b) The first cluster **CL(1)** is constructed by picking up the pair of PRNU images (m, n) that have smallest $Dist$. The centroid of this cluster has an average center $K_{\mathbf{CL(1)}} = \frac{K_m + K_n}{2}$ where K_m, K_n are the PRNU of images (m, n). The Zernike moments vector $A_{r,s}^{\mathbf{CL(1)}}$ is computed for $K_{\mathbf{CL(1)}}$.

(c) The distance matrix $Dist$ is updated between a new PRNU image j and cluster **CL(1)** according to:

$$d_{\mathbf{CL(1)},j} = ||A_{r,s}^{\mathbf{CL(1)}} - A_{r,s}^{j}|| \tag{5}$$

where **CL(1)** is the cluster that contains images $m\&n$.

(d) The *Silhouette* coefficient is computed for each PRNU image j using the updated matrix $Dist$. Note that the *Silhouette* coefficient is defined as [8]

$$sil_j = coh_j - sep_j \tag{6}$$

- coh_j is for cohesion (i.e., the average *Euclidean* distance of a new PRNU image *j* and all the other PRNUs in $L(1)$).
- sep_j for separation (i.e., the average *Euclidean* distance of the PRNU *j* and all the other PRNUs in other clusters).

The image j that has the most negative (in amplitude) sil_j, which means it has minimum distance with $L(1)$, is joined to cluster $L(1)$.

These steps are repeated until the cohesion of the PRNU image j with cluster $L(1)$ is very small. In this paper, the results of more than 800 simulations suggest that the cutting threshold is $coh_j < 0.1coh_1$ where coh_1 is the cohesion of first joined image to this cluster and the first cluster $L(1)$ is constructed. The new clusters $L(q), q = 2, \ldots, p$ were formed by repeating computation for the remaining PRNUs until the cohesion coefficient of every cluster is very small negative.

4 The proposed Zernike forgery detection technique

The proposed forgery detection scheme is based on detecting dissimilarity between the Zernike moments of blocks of the forged image K_f and its corresponding camera PRNU K_c. The dissimilarity is measured by the *Euclidean* distance. The forgery detection technique is summarized as follows:

Initialization Step In this step, the forged image PRNU K_f as well as the mother camera PRNU K_c are estimated as described in [1–3]. In order to speed up computations, resize K_f and K_c using a decimation factor L. Decompose each of decimated K_f and K_c into $P \times P$ non-overlapping blocks. Denote these blocks by $BL_f(i), BL_c(i), i = 1, 2, \ldots, N$, respectively. N is the total number of these blocks. Extract the features of each $BL_f(i)$, $BL_c(i)$ through estimating their $A_{r,s}$ order Zernike moments vector $A_{r,s}^{f}(i) \& A_{r,s}^{c}(i)$, respectively, i.e., $BL_c(i) = \sum_r \sum_{s=-r}^{r} A_{r,s}^{c}(i) V_{r,s} \& BL_f(i) = \sum_r \sum_{s=-r}^{r} A_{r,s}^{f}(i) V_{r,s}$ where $V_{r,s}$ is the orthogonal radial polynomial given in Eq. (1). This results in $d(i) =$

$||BL_c(i) - BL_f(i)|| = ||A^c_{r,s}(i) - A^f_{r,s}(i)||$. The detection process is carried out as follows:

1. Construct $N \times 1$ vector D. Its elements represent the *Euclidean* distances $d(i) = ||A^c_{r,s}(i) - A^f_{r,s}(i)||$. Plot the graph that represent $d(i)$ against the block numbers. If the image under investigation is tampered, then there will be abrupt change in the distance distribution. The minimum threshold T that determines whether a block is genuine or tampered is estimated at the pedestal of this curve.
2. Construct a binary image B_I that represents tampered blocks whose $d(i) \geq T$ through setting these blocks to 1, while zeroing all other blocks.
3. Morphological labeling techniques are applied to B_I to determine the number of its connected components N_c [13]. If the number of the connected components of B_I is $N_c = 0$, this means that the image is genuine, otherwise it is tampered. In this case, determine the centroids of each of these components. Retain only components that are in the neighborhood of each other, i.e., that lie within P pixels of each other.
4. If desired to get a localized tampered region, morphological filling and dilation techniques can be applied to yield the final binary image B_{mrph}.

5 Experimental results

To check the performance of the proposed techniques, the following simulation experiments have been carried out.

5.1 Clustering algorithm

In this case, the proposed clustering algorithm is compared with three other state-of-the-art methods [4,11,12]. Three simulation examples have been carried out. These examples have been performed over random images drawn from 2 databases namely *Dresden Image database* and *Image Manipulation dataset* [25,26].

Example 1 This example considers 300 images randomly chosen from *Dresden Image database* [24] and captured by 5 cameras. The cameras are, *Nikon D70* (6 MP) and 2 another different *Nikon D70S* (6 MP) cameras, *Canon Ixus70* (7.1 MP), and *Kodak M1063* (10.3 MP). First, the Maximum Likelihood Estimate (MLE) technique of [1,2] is used for extracting the PRNU of each image. Each PRNU is decimated by ($L = 4$). Their features were extracted using 10th order Zernike moments ($r = 10$) as described in Sect. 2. The clustering algorithm starts by assigning images using the proposed clustering approach of Sect. 3. Table 1 compares the proposed clustering technique with the Hu's moments-based technique of [12], the MCSC using Normalized Cuts technique in [11] and the classical clustering technique in [4]. The comparison for each camera *j* is shown in terms of *TPR* and *FPR* [11] (the ideal case $TPR = 100\%$ & $FPR = 0\%$) where

$$\text{TPR}(j) = \frac{\text{No. of images correctly assigned to a cluster j}}{\text{No. of images actually belong to this cluster j}}$$

$$\text{FPR}(j) = \frac{\text{No.of images erroneously assigned to a cluster j}}{\text{No.of images actually belong to other clusters}}$$

Table 1 TPR% values and FPR% values of Example 1

	MCSC technique		Classical technique		Hu's moments technique		Proposed technique	
	TPR	FPR	TPR	FPR	TPR	FPR	TPR	FPR
Camera 1	90	2.8	60	6	96	1.2	100	0.2
Camera 2	88.5	2.6	64.5	9	95.8	1.3	98.7	0.4
Camera 3	92.5	1.9	72.5	5.9	100	0.3	100	0
Camera 4	91.5	2.5	78	9	98	0.42	100	0
Camera 5	87.5	3.1	75	11	96	0.92	97.6	0.5

Table 2 TPR% values and FPR% values of Example 2

	MCSC technique		Classical technique		Hu's moments technique		Proposed technique	
	TPR	FPR	TPR	FPR	TPR	FPR	TPR	FPR
Camera 1	90	1.25	70	6.2	94	0.75	100	0
Camera 2	88.6	4	73.3	12.5	96.6	0.9	99	0.5
Camera 3	91	3	77	7.5	96	0.5	98	0.2
Camera 4	94	1.8	71.4	4.65	100	0.7	100	0
Camera 5	91.2	2.1	68.7	4.5	98	1.1	100	0

Table 3 TPR% values and FPR% values of Example 3

	MCSC technique		Classical technique		Hu's moments technique		Proposed technique	
	TPR	FPR	TPR	FPR	TPR	FPR	TPR	FPR
Camera 1	83.3	5.6	66.6	16.7	91.6	2.7	100	0
Camera 2	84.2	10.3	58	24	94.7	3.4	100	0
Camera 3	88.2	6.5	59	19.3	94.1	3.2	100	0

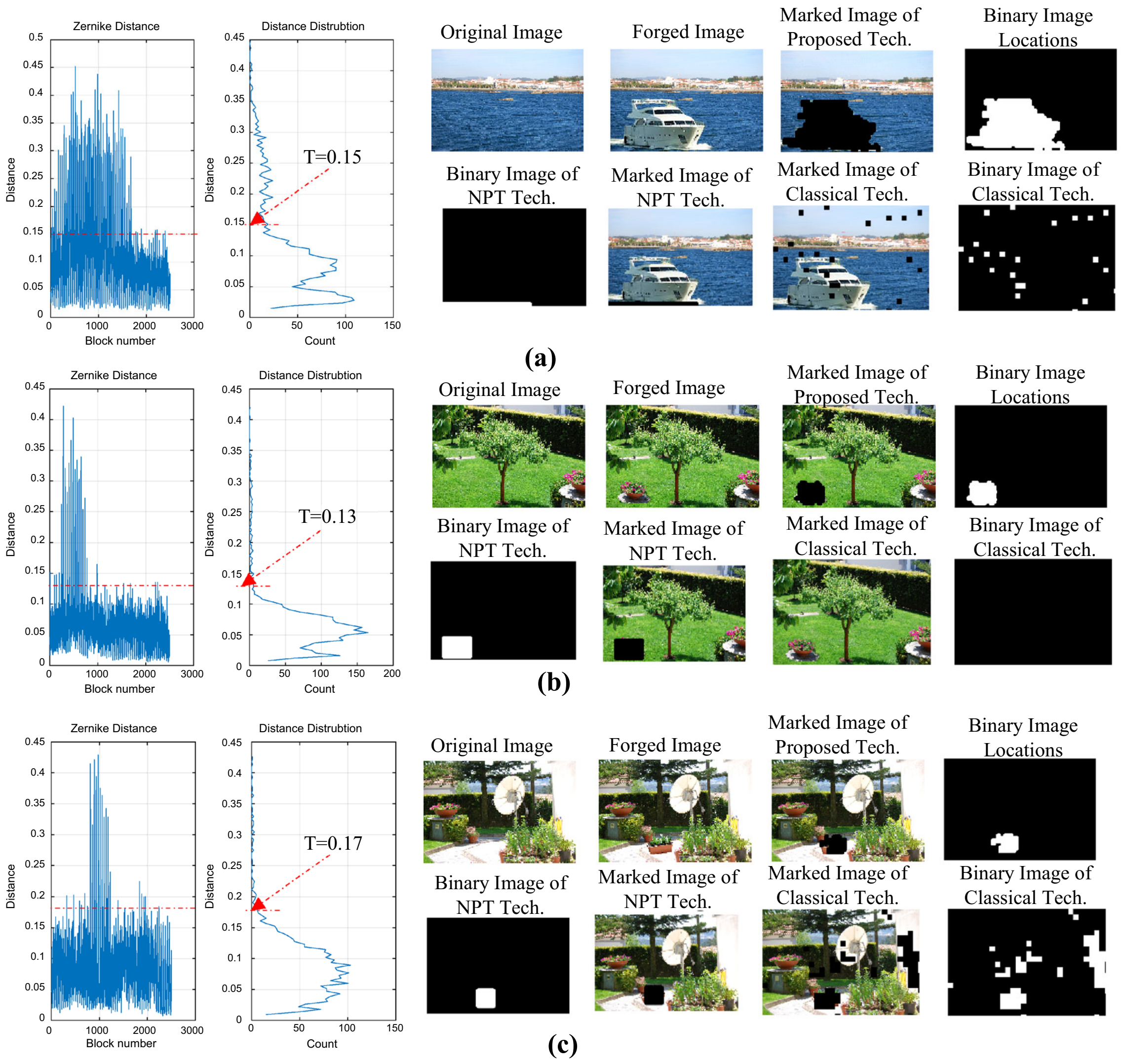

Fig. 2 *Distance* distribution curve of Zernike moments (*left*), original, forged, the binary forged location B_{mrph} of the proposed technique as well as the marked images of NPT and Classical techniques. The threshold T used in the proposed technique is **a** $T = 0.15$, **b** $T = 0.13$, **c** $T = 0.17$

These results indicate that the proposed technique manages to accurately classify unknown images to their mother cameras. The proposed technique takes an execution time 11 s against 8.5 s of the MCSC technique, 10 s of Hu's moments technique and 25 s for the classical technique. The computations have been run on LENOVO-G510 laptop PC, equipped with an Intel Core i5-4200M 64 bit CPU @2.50 Ghz, RAM 8GB.

Example 2 In this example, another set consisting of 500 images randomly drawn from *Dresden Image data base* were carried out. The images were captured by 5 different cameras. The cameras are, Nikon D60 (10.2 MP), Nikon D200S (10.2 MP) cameras, Samsung NV15 (10 MP), Kodak M1063 (10.3 MP) and Panasonic FZ50 (10.1 MP). Table 2 compares the performance of the proposed clustering technique with other

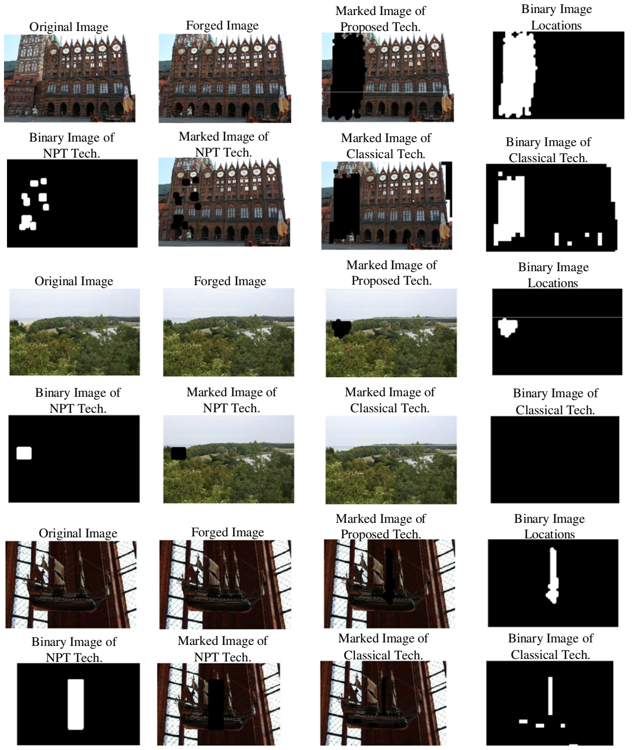
Original Image
Forged Image
Marked Image of Proposed Tech.
Binary Image Locations
Binary Image of NPT Tech.
Marked Image of NPT Tech.
Marked Image of Classical Tech.
Binary Image of Classical Tech.
Original Image
Forged Image
Marked Image of Proposed Tech.
Binary Image Locations
Binary Image of NPT Tech.
Marked Image of NPT Tech.
Marked Image of Classical Tech.
Binary Image of Classical Tech.
Original Image
Forged Image
Marked Image of Proposed Tech.
Binary Image Locations
Binary Image of NPT Tech.
Marked Image of NPT Tech.
Marked Image of Classical Tech.
Binary Image of Classical Tech.

Fig. 3 Comparison between proposed, the NPT technique in [19] and the classical technique [14] for images captured by Canon camera from dataset [26]

published techniques. The proposed technique takes an execution time 18 s against 14.8 s of the MCSC technique, 16 s of Hu's moments technique and 40 s for the classical technique.

Example 3 In this example, another set consisting of 48 images randomly drawn from *Image Manipulation data* [25,26] set were carried out. The images were captured by 3 different cameras namely Nikon, Canon, Panasonic. Table 3 compares the performance of the proposed clustering technique with other techniques. The proposed technique takes an execution time 2 s against 0.78 s of the MCSC technique, 1.2 s of Hu's moments technique and 11 s for the classical technique. All these results indicate the superiority of the proposed Zernike-based clustering technique over other state-of-the-art techniques. Although the proposed technique has slightly larger computation time than MCSC technique and Hu's moments technique, it manages to accurate classify of images whereas other techniques fail.

5.2 Forgery detection algorithm

The performance of the proposed forgery detection scheme is applied using images drawn from *Dresden Image database* as well as *Image Manipulation dataset*. Forging has been carried out using either copy-paste, copy-move or splicing forging techniques. In the first simulation, three 2592 × 3872 natural images captured by the same camera from *Dresden Image database*. These images were manually forged by Photoshop software. The normalized correlation between forged fingerprint K_f & the camera PRNU K_c of these image were 0.0015, 0.1779, 0.2032, respectively. Initially, both of K_f & K_c were decimated by $L = 4$. Next, the decimated K_f & K_c were decomposed into 16×16 non-overlapping blocks. Fifth-order Zernike moments were computed for each of these blocks. The threshold level T was estimated as described in Sect. 4 step 1. Figure 2a–c show the original, forged images, the distance distribution graph of its Zernike moments and the binary forged location B_{mrph} of the proposed technique. These figures also include their comparison with the NPT forgery detection scheme in [19] and the classical forgery detection technique [14]. In all cases, the forged regions are masked in black. The proposed technique took about 25.2 s to detect forgery, while the NPT forgery detection as well as the classical technique of [14] took about 35.2 and 65 s, respectively, and even so they failed to detect forgery, as Fig. 2a shows.

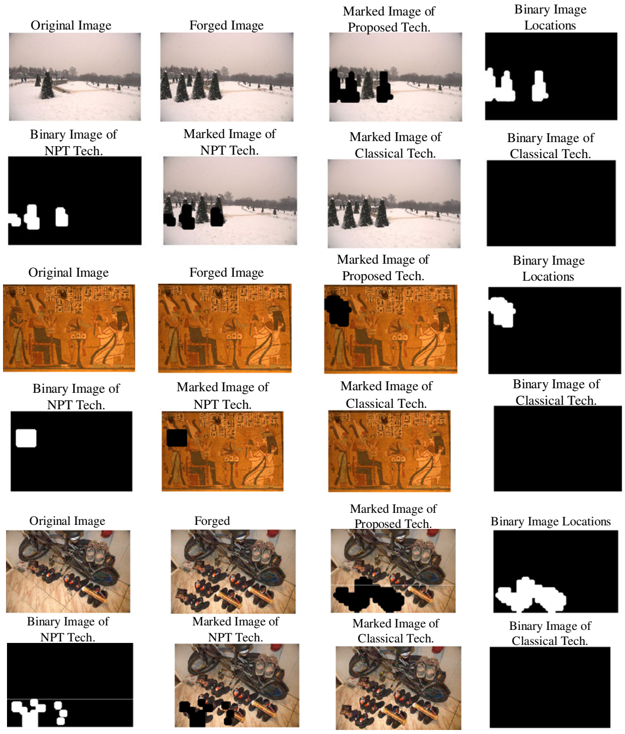
Original Image
Forged Image
Marked Image of Proposed Tech.
Binary Image Locations
Binary Image of NPT Tech.
Marked Image of NPT Tech.
Marked Image of Classical Tech.
Binary Image of Classical Tech.
Original Image
Forged Image
Marked Image of Proposed Tech.
Binary Image Locations
Binary Image of NPT Tech.
Marked Image of NPT Tech.
Marked Image of Classical Tech.
Binary Image of Classical Tech.
Original Image
Forged
Marked Image of Proposed Tech.
Binary Image Locations
Binary Image of NPT Tech.
Marked Image of NPT Tech.
Marked Image of Classical Tech.
Binary Image of Classical Tech.

Fig. 4 Comparison between proposed, the NPT technique in [19] and the classical technique [14] for images captured by Nikon camera from dataset [26]

In the second simulation, the proposed algorithm is applied for detecting forgeries for 9 images randomly drawn from *Image Manipulation Database*. These images were captured by Canon, Nikon and Panasonic cameras, with typical size 3000 × 2400 pixels. The tampered areas covering about 6% of each image, on average. Figures 3, 4 and 5 show the performance of the proposed technique when compared with

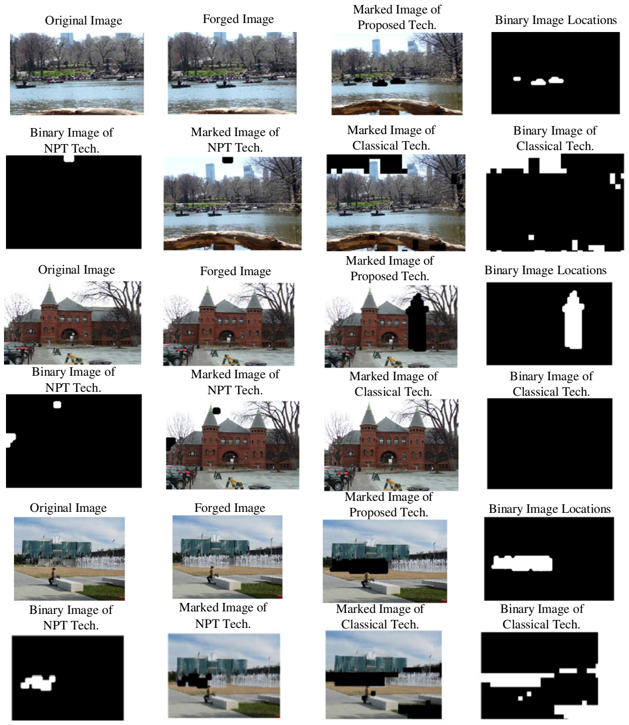
Original Image
Forged Image
Marked Image of Proposed Tech.
Binary Image Locations
Binary Image of NPT Tech.
Marked Image of NPT Tech.
Marked Image of Classical Tech.
Binary Image of Classical Tech.
Original Image
Forged Image
Marked Image of Proposed Tech.
Binary Image Locations
Binary Image of NPT Tech.
Marked Image of NPT Tech.
Marked Image of Classical Tech.
Binary Image of Classical Tech.
Original Image
Forged Image
Marked Image of Proposed Tech.
Binary Image Locations
Binary Image of NPT Tech.
Marked Image of NPT Tech.
Marked Image of Classical Tech.
Binary Image of Classical Tech.

Fig. 5 Comparison between proposed, the NPT technique in [19] and the classical technique [14] for images captured by Panasonic camera from dataset [26]

Table 4 F-measure and Av. computation time

	F-measure (%)	Av. Comp. Time (s)
Proposed Zernike	97	29
Hu's moments	92	37
Classical	80	68

other techniques [14,19]. In order to assess the algorithm performance, we use the *F-measure* [16], defined as

$$F = \frac{2TP}{2TP + FN + FP} \tag{7}$$

TP is number of detected forged images, FN is number of undetected forged images and FP is number of wrongly detected genuine images. The following table compares the *F-measure* and average computation time of the proposed technique, with the classical forgery detection and NPT forgery detection techniques. Table 4 illustrates these results.

6 Conclusion

This paper proposes an efficient clustering technique for grouping a set of images belonging to its capturing camera. The main feature of this technique is the ability of classifying images with very low correlation values. When applied for forgery detection process, the proposed Zernike-based technique is very fast and has superior performance when compared with other state-of-the-art techniques. Besides, it has the ability of checking whether the image under investigation is genuine or forged.

Acknowledgements Omar M. Fahmy acknowledges the support from Prof. M. F. Fahmy, Professor of Electrical Engineering Dept., Faculty of Engineering, Assiut University, Egypt.

References

1. Fridrich, J.: Digital image forensics. IEEE Signal Process. Mag. **26**, 26–37 (2009)
2. Farid, H.: A survey of image forgery detection. IEEE Signal Process. Mag. **2**(26), 16–25 (2009)
3. Li, C.-T.: Source camera identification using enhanced sensor pattern noise. IEEE Trans. Inf. Forensics Secur. **5**(2), 280–287 (2010)
4. Bloy, G.J.: Blind camera fingerprinting and image clustering. IEEE Trans. Pattern Anal. Mach. Intell. **30**(3), 532–535 (2008)
5. Liu, B.B., Hu, Y., Lee, H.: Source Camera Identification from Significant Noise Residual Regions. In: 17th IEEE ICIP, pp. 26–29 (2010)
6. Li, C.-T.: Unsupervised classification of digital images enhanced sensor pattern noise. In: IEEE International Symposium on Circuits and Systems (ISCAS 10), (2010)
7. Parsi, A., Ghanbari Sorkhi, A., Zahedi, M.: Improving the unsupervised LBG clustering algorithm performance in image segmentation using principal component analysis. SIVP **10**(2), 301–309 (2016)
8. Caldelli, R., Amerini, I., Picchioni, F., Innocenti, M.: Fast Image Clustering of Unknown Source Images. In: IEEE International workshop on Information Forensics and Security (WIFS), pp. 12–15 (2010)
9. Shahbaba, M., Beheshti, S.: Signature test as statistical testing in clustering. SIViP **10**(7), 1343–1351 (2016)
10. Liu, B.B., Lee, H.K., Hu, Y., Choi, C.H.: On Classification of Source Cameras: a graph Based Approach. In: IEEE International workshop on Information Forensics and Security (WIFS), pp. 1–5, 12–15 (2010)
11. Amerini, I., Caldelli, R., Crescenzi, P., Del Mastio, A., Marino, A.: Blind image clustering based on the normalized cuts criterion for camera identification. Image Commun. **29**, 1–13 (2014)
12. Fahmy, O.M.: An Efficient Clustering Technique for Cameras Identification using Sensor Pattern Noise. In: IEEE International Conference on Systems, Signals and Image Processing (IWSSIP), pp. 10–12 (2015)
13. Solomon, C., Breckon, T.: Fundaments of Digital Image Processing. Wiley-Black Well, ISBN 9780470689776 (2011)
14. Chen, M., Fridrich, J., Goljan, M., Lukas, J.: Determining image origin and integrity using sensor noise. IEEE Trans. Inf. Forensics Secur. **3**(1), 74–90 (2008)
15. Amerini, I., Ballan, L., Caldelli, R., Del Bimbo, A., Serra, G.: A SIFT-based forensic method for copy and move attack detection and transformation recovery. IEEE Trans. Inf. Forensics Secur. **6**(3), 1099–1110 (2011)
16. Cozzolino, D., Poggi, G., Verdoliva, L.: Efficient dense-field copy-move forgery detection. IEEE Trans. Inf. Forensics Secur. **10**, 2284–2297 (2015)
17. Chierchia, G., Poggi, G., Sansone, C., Verdoliva, L.: A Bayesian-MRF approach for PRNU-based image forgery detection. IEEE Trans. Inf. Forensics Secur. **9**(4), 554–567 (2014)

18. Kohale, T., Chede, D., Lakhe, P.R.: Forgery detection technique based on block and feature based method. Int. J. Adv. Res. Comput. Commun. Eng. **3**(6), 7334–7335 (2014)
19. Fahmy, M.F., Fahmy, O.M.: A Natural Preserving Transform Based Forgery Detection Scheme. In: IEEE International Symposium on Signal Processing and Information Technology (ISSPIT), pp. 7–10 (2015)
20. Day, D.D., Ahmed, A.M.: A Modified Natural Preserving Transform for data hiding and Image Watermarking. In: Proceedings of JCIS 7th Joint Conf. of IASTED Int. Conf. on Signal and Image Processing, pp. 44-48 (2003)
21. Fahmy, M.F., Abd Raheem, G., Thabet, M.A.: A Zernike Moment Based Rotational Invariant Watermarking Scheme. In: IEEE National Radio Science Conference (NRSC), pp. 16–18 (2013)
22. Liao, S.X., Pawlak, M.: Image Analysis with Zernike Moments Descriptors. In: IEEE Electrical and Computer Engineering, 1997. Engineering Innovation: Voyage of Discovery, vol. 2, pp. 700–703 (1998)
23. Tran, T.T., Pham, V.T., Shyu, K.K.: Zernike moment and local distribution fitting fuzzy energy-based active contours for image segmentation. SIVP **8**(1), 11–25 (2014)
24. *Dresden Image database*, (http://forensics.inf.tu-dresden.de/ddimgdb/)
25. Christlein, V., Riess, C., Jordan, J., Riess, C., Angelopoulou, E.: An evaluation of popular copy-move forgery detection approaches. IEEE Trans. Inf. Forensics Secur. **7**(6), 1841–1854 (2012)
26. *Image Manipulation Data set*, (http://www5.cs.fau.de/)