International Journal of Applied Engineering Research ISSN 0973-4562 Volume 10, Number 14 (2015) pp 34256-34361

Copy move forgery detection using fusion of zernike and dct

[1] Gelareh Majid, [2] Ghazali Sulong
UTM-IRDA Digital Media Centre (MaGIC-X),Faculty of Computing,Universiti Teknologi Malaysia,
UTM Skudai 81310,Johor, Malaysia
[1]glareh.majid@gmail.com [2]ghazali@utmspace.edu.my

Abstract- *Image forgery is a kind of manipulation to conceal important and useful information. Between wide ranges of tampering techniques, copy-move forgery which includes copied area from another part of same image, is one of the frequently used techniques. Adding different type of attack such as noise and rotation are often involved to assimilate tampered image to original one. Thus, an improved technique is required to be developed for efficient and robust duplicated-block detection. The aim of this study is to improve detection accuracy under different kind of post-processing like noise and rotation. In order to achieve this goal, a detection method of copy-move forgery using the combination of discrete cosine transform (DCT) and Zernike moments for localization of duplicated regions is proposed. Since the magnitude of Zernike moments is algebraically invariant against rotation and DCT is insensitive to additive noise, the proposed method is therefore introduced by exploiting these advantages. Firstly, image is divided into blocks of 16x16 pixels. Secondly, for each block, both Zernike moments and also DCT coefficients are computed and sorted lexicographically. Thirdly, for each type of feature (Zernike moments and DCT Coefficients), each pair of blocks is compared to find a possible matching according to a predetermined threshold value. The proposed method is evaluated on ten forged images of MICC-F220 standard dataset. Simulation results demonstrated that precision rate of proposed method under rotation and noise attack was above 75% beside, because of upward trend of True Positive, recall rate of proposed method exceeded 90%.*

Keywords- Copy-move; Image Integrity; Discrete Cosine Transform Coefficients Quantization; Region Duplication Detection; Zernike moments.

1. Introduction

High resolution capturing devices, advanced photo editing software tools and certainly powerful computers made digital images' manipulations to become really easy. While the application of pictures is growing as historical records and supporting evidences in different fields, the authenticity of these photographs became an important task [2]. Copy-move forgery is the most popular image forgery manipulation in which a part of a photo is duplicated and pasted on a different part of same photo to cover an important object. Various methods have been proposed in the field to detect the Copy-move forgery but some algorithms are weak to locate the copy-move region after copying manipulations, such as noise, rotation or combination of these operations [12].

Accuracy of true cases and false cases is a problem that often faced with Copy-Move Forgery Detection (CMFD), because the performances of methods are given in term of true positive and false positive. As a result for improving performance of Copy-Move Forgery Detection (CMFD), a method should be found that has great efficiency in recognizing post processing attacks on image. Hence, it is an important issue to improve an algorithm by increasing true positive against amounts of false positives for forgery detection.

The focus of this paper is to detect the transformation of copy-pasted areas by increasing the true positives' rate and robust detection method against some common pro-processes. The propose method is based on DCT and Zernike. The experimental results and feature matching demonstrate that proposed feature has precise results in the case of adding a combination of noise and rotation on manipulated image.

The paper is organized as follows: section 2 gives related work. In section 3, provides proposed technique methodology explanation. Section 4 discusses results of the methodology. Section 5 overall conclusions are drawn and recommendations for future works are also given.

1.2. Related Work

1.2.1. Discrete Cosine Transform (DCT)

Fridrich [6] proposed the very first method for copy-move forgery detection. In their method, coefficients of small blocks for sorted gradual discrete cosine transform (DCT) were used to check the similarity of the adjusted blocks [11]. Its drawback is that it only indicates the matched points and not the regions [6].

Huang [8] improved discrete cosine transform DCT-based methods that were used to detect CMFD. With DCT technique, the digital images are divided into fixed-size blocks that overlapped with each other. This method is able to detect duplication even if images were compressed, blurred or stabilized by white Gaussian noise. However the improved DCT- based method does not deal with geometrical transformation of the tampered image [8].

Ghorbani [7] combined DCT and DWT (Discrete Wavelet Transform), in ordered to propose an enhanced algorithm for cloning forgery detection. This combination improved the accuracy of detecting tampered region. Though, in the experiments, it was shown that this technique is able to detect mentioned image tampering on condition that copied areas have not been scaled or rotated and have been pasted as long as possible from their original place in the image [7].

1.2.2. Zernike Moments (ZMs)

ZMs have been used widely as a powerful feature extractor in pattern-recognition systems with satisfactory results. Teague [13] introduced ZMs based on the theory of orthogonal polynomials in image analysis and constructed useful moments. Hence, the ZMs magnitude is a rotation invariant [5]. Ryu [11] calculates the size of Zernike moments (ZMs) where the vectors were lexicographically sorted in order. Then, they have investigated the neighboring vectors' similarity. It was supported by experimental results that the method is suitable for localizing and identifying tampered areas even when the area is intentionally manipulated. Although despite the ZMs has well performance in detecting rotation, it faces some errors to detect noise attacks [11]. However in case of rotated forgery detection, the Zernike moment feature reflected a good performance, this method is not able to handle detected results' false contents which reduce the algorithm's accuracy [14].

3. The Proposed Algorithm

Increasing the accuracy in CMFD against some common attacks such as rotation and noise addition is important. This paper aims to find a novel method to improve accuracy rate of CMFD algorithms in order to have better detection after adding noise and rotation in CMFD. The method combines DCT- and Zernike-based algorithms as illustrated in Figure 1.

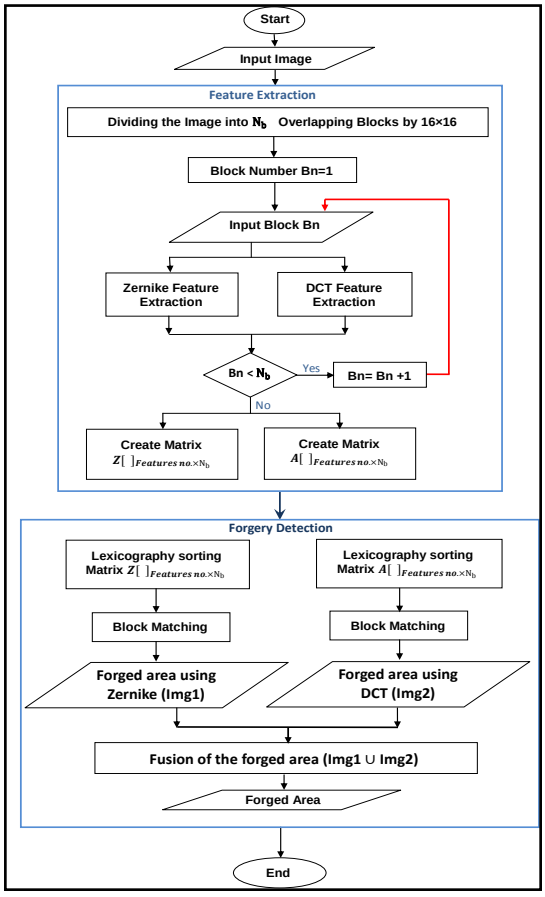

Fig 1. The general procedure of the Proposed Method

4. Research Method

4.1. Feature Extraction

Assume a picture contains M×N pixels. A square which contains L×L pixels starts to slide horizontally from the upper left corner to bottom right corner. The total number of overlapping blocks will be (M-L+1)(N-L+1) [8]. After dividing suspected image into overlapped sub-blocks, each block is considered as Bij where i and j indicate coordinate of first point of each block [11]. Every sub-block is represented by Zernike moment and DCT coefficient.

4.1.1. Zernike Feature Extraction

Zernike moments are based on a set of complex polynomials which is the calculation of the image function on the orthogonal basis functions. Three steps should apply to each Bij, firstly the center of block should be taken as the origin of the unit circle then pixel coordinates should be computed in the range of unit circle, finally Pixels within this range are used for normalizing image and the rest pixels of block are vanished. In the next step, ZM's with n degree and m moments are computed from each block by calculating A_{nm} from equation (1), where ρ and θ represent the polar coordinates over the unit circle and R is Radial polynomials of ρ .

$$A_{nm} = \frac{n+1}{\pi} \sum_{\rho} \sum_{\theta} f(\rho,\theta) R_{nm}(\rho) \exp(-jm\theta) \qquad (1)$$

After obtaining Anm for each block, set of results are vectorized in form of Vij (Figure 2) which i and j refer to coordination of first point of each block, then vectors of features are placed in matrix Z[ ]. Figure 3, illustrated Zernike moments feature extraction process.

$$V_{ij} = \left(|A_{0,0}| \ |A_{1,1}| \dots |A_{\bar{n},\bar{n}-2}| \ |A_{\bar{n},\bar{n}}| \right) \quad \text{for} \quad N_{moments} = \sum_{i=0}^{nMax} \left(\left\lfloor \frac{i}{2} \right\rfloor + 1 \right)$$

$$Z = \begin{bmatrix} V_{00} \\ \vdots \\ V_{(M-L)(N-L)} \end{bmatrix}$$

Fig 2. Constructing Matrix Z

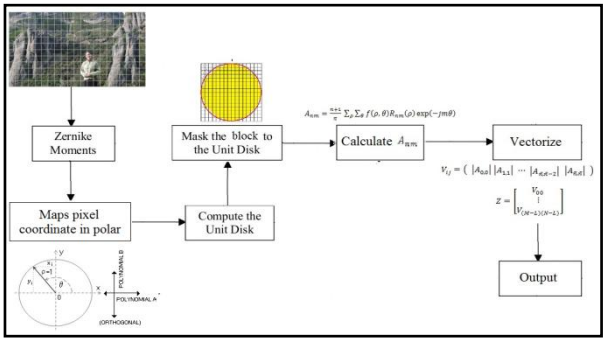

Fig 3. Steps of Zernike Moments Feature Extraction

4.1.2. DCT Feature Extraction

In this step, for each L×L block, DCT is used then a vector of feature is created with dimension of L×L. By using nature of DCT, most energy of transformed coefficients concentrates on the lower frequency coefficients (LFC). The higher frequency coefficients (HFC) are less important. Therefore, HFC can be truncated by saving a part of row vector components. Because of zigzag ordering, the DCT coefficients changed to a row vector and make truncating easy. To make faster sorting and matching process, the dimension is reduced [8].The Discrete Cosine Transform tried to decorrelate the image data. After this procedure each transform coefficient encoded independently without losing compression efficiency. The 2-D (2 dimensional) basis functions are produced by multiplying the horizontally oriented and vertically oriented set of the 1-D basis functions [9]. Thus the 2-D DCT is a direct extension of the 1-D (1 dimensional) case. The most common DCT definition of a 2-D sequence of length N shows in equation (2) which ∝ (u) and α (v) component for u and v equal to zero is the square root of 1/N and otherwise is the square root of 2/N. DCT coefficient feature extraction process depicted below (Figure 4).

$$f(x,y) = \sum_{u=0}^{N-1}\sum_{v=0}^{N-1} \propto(u) \propto(v)\, C(u,v) \times \cos\left[\frac{\pi(2x+1)u}{2N}\right] \cos\left[\frac{\pi(2y+1)v}{2N}\right]$$

$$x,y = \{0,1,2,\dots,N-1\} \qquad (2)$$

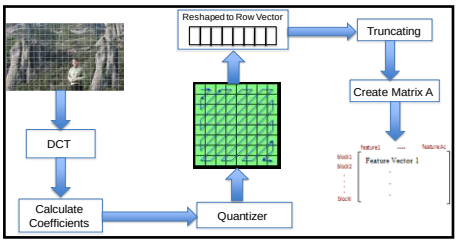

Fig 4. Steps of DCT Coefficient Feature Extraction

4.2.Forgery Detection

This step includes detecting similar blocks and then shows the copy-move region in suspected image. First lexicographically sorting should be used to reduce detecting time then blocks that have same representations are detected. The lexicographical order arranges feature vectors and inserts them into a matrix, where the rows and columns of the matrix correspond to the blocks and the features respectively. Lexicographical order arranges same feature vectors in the consecutive rows of the matrix. As a result consecutive rows could be forged blocks [6, 10]. One problem during matching process is similar blocks is flat region which have same characteristics. To deal with this problem, one important factor related to feature set is threshold values that are modified manually to best fit to the benchmark dataset. In order to avoid matching neighbor blocks, two factors should be considered [4]:

i. Minimum Euclidean distance - distance between two matched blocks
ii. Minimum number of correspondences - the minimum number of pairs that are connected together in a same distance.

4.2.1. Forgery decision in DCT

The DCT extracts block's features and inserts them into matrix A [ ]. Each features represent by F_{AC}^{i} where Ac indicates the feature number and i refers to coordination (x, y) of starting point of block. The lexicographical order arranges feature vectors and creates Matrix $\hat{A}$ (Figure 5). The same feature vectors' rows represent in consecutive rows which correspond to same blocks in the image.

$$\hat{A} = \begin{bmatrix} \vdots & & \\ F_1^i & F_2^i & \cdots \\ F_1^k & F_2^k & \cdots \\ \vdots & & \end{bmatrix}$$ Same Blocks

Fig 1. Sorted matrix of A[ ]

For making forgery decision in DCT, two type of threshold should be calculated. Firstly, the distance between two matching block should not be more than Minimum Euclidean distance (τ1) [3]. The distance D(dx, dy) between the two matching blocks number of i and k that have the similar feature vectors and with coordination of (x_i, y_i) and (x_k, y_k) that indicate the starting point of blocks, is calculated by using equation (3).

$$if \begin{cases} d_x(i,k) = x_i - x_k > \tau_1 \\ d_y(i,k) = y_i - y_k > \tau_1 \end{cases} then \text{ blocks are forged} \qquad (3)$$

The forgery decision can be made if there are more than a certain number of connected blocks within a same distance. Following this, a distance vector D (dx,dy) is produced and its value is set to zero. For every similar feature values in same distance between two rows, the value of D is incremented by one. If summation of D is more than τ2 (Minimum number of correspondences) and if these blocks are connected to each other then the image is marked as forged image [3].

4.2.2. Forgery decision in Zernike

Before the matching procedure, the magnitude of ZM's is calculated to form matrix Z[ ] which includes a set of vectorized moments Vij . Each moment represents by $A^{i,j}{}_{n,m}$ that i and j are first point of block and n and m are Zernike moment's order and repetition respectively. If $A^{i,j}{}_{n,m}$ represent by Z_n^{ρ} , in the way that ρ and n correspond to first point of block coordination and number of Zernike moments in above matrix, the lexicographicaly sorted set is shown below (Figure 6).

$$\hat{Z} = \begin{bmatrix} \vdots & & & & \\ \hat{z}_1^{\rho}, \hat{z}_2^{\rho}, & \dots & , \hat{z}_{Nmoment-1}^{\rho}, \hat{z}_{Nmoment}^{\rho} & \leftarrow V_{ij} \\ \hat{z}_1^{\rho+1}, \hat{z}_2^{\rho+1}, & \dots & , \hat{z}_{Nmoment-1}^{\rho+1}, \hat{z}_{Nmoment}^{\rho+1} & \leftarrow V_{kj} \\ \vdots & & & & \end{bmatrix}$$ Same Blocks

Fig 2. Sorted matrix of Z [ ]

For making forgery decision in Zernike moments for near duplicated entries the Euclidean distance is calculated by equation (4) which D and D1 are Euclidean distance and

threshold value. If D< D1, then the pair of blocks candidate as duplicated region evaluated [11].

$$D = \sqrt{\sum_{q=1}^{N_{moments}} \left(Z_q^{\rho} - z_q^{\rho+1}\right)^2}$$

$$\begin{cases} if & D \le D1 \quad pair\ blocks\ are\ forged \\ if & D > D1 \quad not\ forged \end{cases} \quad (4)$$

If amount of D greater than threshold D1 then consecutive blocks in Matrix $\hat{Z}$ is not forged, otherwise they might be forged. Since neighboring blocks has same feature vectors the spatial distance between blocks with consecutive moment vectors should be evaluated [11]. The distance between two consecutive blocks with coordination of (i, j) and (k, l) is calculated by equation (5), where D and D2 are spatial distance and threshold value.

$$D = \sqrt{(i-k)^2 + (j-l)^2}$$

$$\begin{cases} \text{if} & D \le D2 \quad blocks\ are\ neighbore \\ \text{if} & D > D2 \quad blocks\ are\ forged \end{cases} \quad (5)$$

4.3. Image Integrity

Each image can be defined as a matrix which values of pixels form the matrix elements. Overlapped block is a matrix which is subset of image's matrix. Thus, pixels of forged blocks can be marked in original image that they are detected after lexicography order. In the block matching phase, detected forged area from matrix ZL[ ] and AL[ ] are found separately then the algorithm convert forged blocks to zero amounts and inserted into matrix Img1[ ] and Img2[ ] respectively. Each element of these matrixes indicates one overlap block. By merging Img1 [ ] and Img2 [ ] all forged blocks which are detected by DCT and Zernike moments insert into output image with zero amount. As a result, in the matrix of output image, there are some detected blocks that refer to those areas which DCT can recognize but Zernike cannot or inverse. Also there are some blocks that are considered as a forged area by both of methods.

5. Experimental Setup

In the experiments of proposed method, five standard JPG images with size of 800×532 have been chosen from the MICC-F200 Dataset [1]. To verify the robustness of proposed method two types of CMF attacks applied on selected images, which were Gaussian noise and Rotation. Gaussian noise of 0.4 was added on the tampered images and the duplicated region was rotated by 40 degree. The input images used are 10 forged images from 5 original images which they have noise or rotation attacks. In experimental results, DCT feature included 64 DCT coefficient with the block size 16×16 was employed as feature extraction method. Furthermore the number of Zernike moments equal with 9 moments that was obtained from Zernike with order 4 with the block size 16×16, selected as feature extraction method. Furthermore lexicography sorting was used for block matching. The detection accuracy performance of proposed algorithm is evaluated by utilizing precision and recall.

5.1. Performance Metrics And Result Analysis

To evaluate the performance of the method in copy-move forgery, appropriate measures are required. In this study, two famous performance measurements of information retrieval field include Precision and Recall values is adopted for ten selected copy-move forgery images from standard dataset of MICC-F220. The Precision is a measure for calculating the chance of region detection that is recognized correctly. However, the ratio of Recall calculates probability of a forged region which is detected correctly [11]. The Precision and recall in percentage terms is computed as below equation (6) and equation (7).

$$\text{Precision} = \frac{(\text{Forged Region} \cap \text{Detected Region})}{\text{Detected Region}} \times 100[\%] \quad (6)$$

$$\text{Recall} = \frac{(\text{Forged Region} \cap \text{Detected Region})}{\text{Forged Region}} \times 100[\%] \quad (7)$$

Table (1), summarizes accuracy precision and recall performance evaluation of the proposed algorithm versus Zernike and DCT method on five original images from a standard dataset. In this table, it can be seen that the proposed algorithm outperforms and has a clear advantage over Zernike and DCT algorithm as it perfectly detected forged blocks (Recall) and contains many truly detected forged blocks (Precision) in result images. Here, the proposed method obtained higher performance level than DCT in precision which is about 76% against 66%. However, Zernike and proposed method have the approximately similar values. They are amounted for about 73% and 76%, respectively. The proposed method reached performance levels in detecting duplicated blocks with an average of more than 90% in recall while the average of recall in the previous algorithms were significantly less than and equal to 47% in DCT and 65% in ZM's. The proposed method generates high true positive duplicated blocks.

Table 1. Experiment result of Precision-Recall Performance

Method	Recall	Precision
DCT Coefficient	47.64506	66.44532
Zernike Moments	65.79305	73.50485
Proposed Method	90.92761	76.49520

Line-charts of Figure 7 and Figure 8, includes recall and precision rates of each tampered image which used proposed algorithm and two other ones as a detection methods.

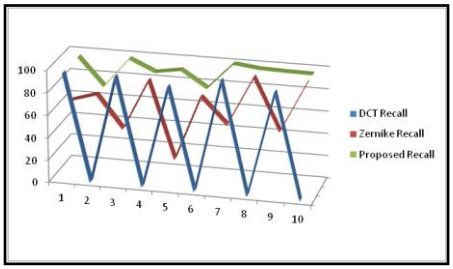

Fig 7. Comparison Recall rate of ten tempered photos with two other detection methods (Odd numbers have noise additional and even numbers have rotation attack)

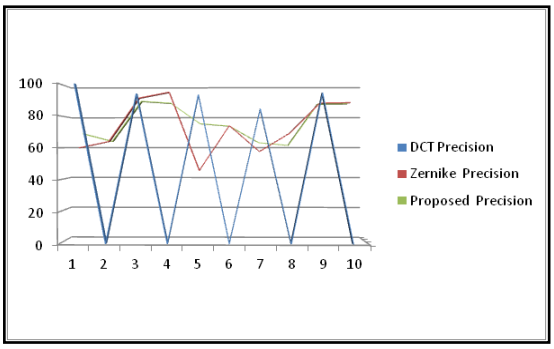

Fig 8. Comparison Precision rate of ten tempered photos with two other detection methods (Odd numbers have noise additional and even numbers have rotation attack)

The line chart of Figure 7, which belongs to recall rate shows that DCT failed in five photos because of it is not sensibility to rotation. Whereas, ZM's has a dramatic fluctuation and in some photos it hit the lowest point of 19%. In contrast, recall rate of the proposed method is superior to either DCT or ZM's. Its diagram never fell under 70% and in most of the cases it is just under 100%. Meanwhile, the precision rate of the proposed method in Figure 8, is close to ZM's but if the proposed method and ZM's are used to detect copy-move forgery under noise attack, the precision rate of proposed method will be higher than ZM's. Also, it is need to be pointed that the proposed method is invariant to rotation in contrast to DCT which failed in such cases. From the experimental results, it is clear that proposed method can detect the images with noise and rotation better than previous methods.

5.2. Visual Result

Five original images with same size were selected from dataset of [1]. Since they manipulated by rotating or Gaussian noise artifacts, ten input images were used. Images 1, 3, 5, 7 and 9 have noise additional without rotation. The recall and precision rate of them were shown in form of line-chart in Figure 7 and Figure 8. The images 2, 4, 6, 8 and 10 have 40 degree rotation without noise additional.

Results of some output images are shown in Figure 9, 10, 11 and12. In image 5 (Figure 9) which is called Gun with only Gaussian noise attack, recall rate of proposed method (Figure 7) had a marked differentiate with ZM's diagram and it also transcended a little higher than DCT. Precision rate of proposed method (Figure 8) was 30% more than ZM's as well. Though, precision rate of proposed method fell behind DCT about 10%. In image 6 (Figure 10) which has only rotation attack both recall and precision rates of proposed method were as same as ZM's. However DC was unsuccessful in this test.

Fig 9. Forgery detection of Gun image with noise attack

Fig 10. Forgery detection of Park image with rotation attack

Image 3 (Figure 11) is called Park with Gaussian noise attack, ZM's had the lowest rate of recall while proposed method had relative increase in compare to DCT (Figure 7). The precision rate of three methods was close to each other and diagram of proposed method was slightly lower than others (Figure 8). In image 4 (Figure 12) with only rotation attack, proposed method and ZM's had similar trend in recall while Zernike's precision surged for just 5% in compare to propose method and DCT was failed in both measurement values.

Fig 11. Forgery detection of Park image with noise attack

Fig 12. Forgery detection of Park image with rotation attack

6. Conclusion

In this paper we have presented a novel algorithm of copy-move forgery detection utilizing combination of Zernike features and DCT. First, algorithm extracted features of all the blocks from the original image. To extract feature vectors of overlapping blocks, the magnitude of Zernike moments and DCT coefficient were calculated. Afterward, lexicographically-based algorithm was used to sort the blocks' features and to form a matrix for each method. Finally, features were compared with each other to detect duplicated blocks. Then merging all forged blocks which were detected by DCT and Zernike moments, inserted into output image with zero amount. The algorithm's output included the map image and the input image together. The suspected regions were measured by Precision and Recall. Finally, according to statistics, this new algorithm showed its robustness against the attack mentioned above. So it could be confirmed that the proposed method has successfully increased both recall and precision rates. In general, this study has achieved the higher performance level than pervious methods that was about 76% in precision and about 91% in recall. The future work might include, but not limited to continuing to examine the proposed method under the various rotation degrees combined with noise.

Correspondence to:

Gelareh Majid
Glareh.majid@gmail.com

References

[1] Amerini, I., Ballan, L., Caldelli, R., Del Bimbo, A., & Serra, G. 2011. A SIFT-based forensic method for copy–move attack detection and transformation recovery. *Information Forensics and Security, IEEE Transactions on*, *6*(3), 1099-1110.

[2] Amsberry, C. 1989. Alterations of photos raise host of legal, ethical issues. *The Wall Street Journal*, *1*, 26-89.

[3] Bayram, S., Sencar, H. T., & Memon, N. 2008, September. A survey of copy-move forgery detection techniques. In *IEEE Western New York Image Processing Workshop* (pp. 538-542

[4] Christlein, V., Riess, C., Jordan, J., & Angelopoulou, E. 2012. An evaluation of popular copy-move forgery detection approaches. *Information Forensics and Security, IEEE Transactions on*, *7*(6), 1841-1854.

[5] Farokhi, S., Shamsuddin, S. M., Flusser, J., Sheikh, U. U., Khansari, M., & Jafari-Khouzani, K. 2013. Rotation and noise invariant near-infrared face recognition by means of Zernike moments and spectral regression discriminant analysis. *Journal of Electronic Imaging*, *22*(1), 013030-013030.

[6] Fridrich, A. J., Soukal, B. D., & Lukáš, A. J. 2003. Detection of copy-move forgery in digital images. In *in Proceedings of Digital Forensic Research Workshop*.

[7] Ghorbani, M., Firouzmand, M., & Faraahi, A. 2011, June. DWT-DCT (QCD) based copy-move image forgery detection. In *Systems, Signals and Image Processing (IWSSIP), 2011 18th International Conference on* (pp. 1-4). IEEE.

[8] Huang, Y., Lu, W., Sun, W., & Long, D. 2011. Improved DCT-based detection of copy-move forgery in images. *Forensic science international*, *206*(1), 178-184.

[9] Pennebaker, W. B., & Mitchell, J. L. 1993. *JPEG: Still image data compression standard*. Springer.

[10] Popescu, A. C., & Farid, H. 2005. Exposing digital forgeries in color filter array interpolated images. *Signal Processing, IEEE Transactions on*, *53*(10), 3948-3959..

[11] Ryu, S. J., Lee, M. J., & Lee, H. K. 2010, January. Detection of copy-rotate-move forgery using Zernike moments. In *Information Hiding* (pp. 51-65). Springer Berlin Heidelberg.

[12] Shivakumar, B. L., & Santhosh Baboo, S. 2011. Detection of Region Duplication Forgery in Digital Images Using SURF. *International Journal of Computer Science Issues (IJCSI)*, *8*(4).

[13] Teague, M. R. 1980. Image analysis via the general theory of moments*. *JOSA*, *70*(8), 920-930.

[14] Yang, J., Ran, P., Xiao, D., & Tan, J. 2013. Digital Image Forgery Forensics by Using Undecimated Dyadic Wavelet Transform and Zernike Moments⋆. *Journal of Computational Information Systems*, *9*(16), 6399-6408.