Comparison of specific segmentation methods used for copy move detection

Eman Abdulazeem Ahmed[1,2], Malek Alzaqebah[1,2], Sana Jawarneh[3], Jehad Saad Alqurni[4], Fahad A. Alghamdi[5], Hayat Alfagham[5], Lubna Mahmoud Abdel Jawad[6], Usama A. Badawi[5], Mutasem K. Alsmadi[5], Ibrahim Almarashdeh[5]

[1]Department of Mathematics, College of Science, Imam Abdulrahman Bin Faisal University, Dammam, Saudi Arabia
[2]Basic and Applied Scientific Research Center, Imam Abdulrahman Bin Faisal University, Dammam, Saudi Arabia
[3]Computer Science Department, Applied College Dammam, Imam Abdulrahman Bin Faisal University, Dammam, Saudi Arabia
[4]Department of Educational Technology, College of Education, Imam Abdulrahman Bin Faisal University, Dammam, Saudi Arabia
[5]Department of Management of Information Systems, College of Applied Studies and Community Service, Imam Abdulrahman Bin Faisal University, Dammam, Saudi Arabia
[6]College of Healthcare Management and Economics, Gulf Medical University, Ajman, United Arab Emirates

Article Info

Article history:

Received Nov 12, 2021
Revised Oct 11, 2022
Accepted Nov 3, 2022

Keywords:

Copy move detection
Density-based spatial clustering of applications with noise
Image segmentation
K-means
Super pixel segmentation

ABSTRACT

In this digital age, the widespread use of digital images and the availability of image editors have made the credibility of images controversial. To confirm the credibility of digital images many image forgery detection types are arises, copy-move forgery is consisting of transforming any image by duplicating a part of the image, to add or hide existing objects. Several methods have been proposed in the literature to detect copy-move forgery, these methods use the key point-based and block-based to find the duplicated areas. However, the key point-based and block-based have a drawback of the ability to handle the smooth region. In addition, image segmentation plays a vital role in changing the representation of the image in a meaningful form for analysis. Hence, we execute a comparison study for segmentation based on two clustering algorithms (i.e., k-means and super pixel segmentation with density-based spatial clustering of applications with noise (DBSCAN)), the paper compares methods in term of the accuracy of detecting the forgery regions of digital images. K-means shows better performance compared with DBSCAN and with other techniques in the literature.

Corresponding Author:

Eman Abdulazeem Ahmed
Basic and Applied Scientific Research Center, Imam Abdulrahman Bin Faisal University
P.O. Box 1982, 31441, Dammam, Saudi Arabia
Email: eabdulazeem@iau.edu.sa

1. INTRODUCTION

These days, the manipulation of digital images became very easy by using image editing software. The headway of this software in a short time arrives at a good level to manipulate the images without decreasing the quality of images or leaving any traces to know that. This is disturbing as images where it is now presented as evidence and historical records in different domains, like in forensic investigation, journalistic photography, law implementation, and medical photos. In the scientific area, this manipulation gives negative effects also whereas Farid [1] declared that twenty percent of the accepted articles in the Journal of cell biology have unsuitable image manipulation. Hence, image forge and discovery have garnered essential interest and attention as manipulated images can be applied to deviate their concepts with bad intent. It is important on the internet and social networks to be sure the images are real without any forge, so a lot of research has been working in the copy-move forgery detection (CMFD) field. The CMFD methods can be either key point-based techniques or block-based methods.

In the method of block-based CMFD [2], [3], any image split into size overlapping blocks, then identical blocks seek, later discovered the feature extraction method. The search area reduction procedure is the major variation between these techniques [4]. In the block-based methods, the number of blocks is very huge, so it is costly and the computing load of the feature extraction method and the preprocessing method for removing some blocks from assessment are considered significant [5]. In key points-based CMFD techniques firstly the key points are discovered [6]. Then, similar areas just depending on key points searched, and finally found. Clearly, the key points are less than overall overlapped blocks, so key points-based techniques are quicker than block-based techniques. In this work detecting the copy-move forgery is executed with the help of two methods of clustering, namely; k-means and the simple linear iterative clustering (SLIC) with the density-based spatial clustering of applications with noise (DBSCAN) methods. Detecting and searching for identical parts or blocks in fake images are the essential idea in CMFD algorithms. The robustness, accuracy, and speed of this discovery are various measurements used to evaluate the effectiveness of the algorithms. The related works in this section focus on the methods that improve the CMFD.

A feature vector is presented by Kushol *et al.* [7], as an array of objects of features and color view. Prasad and Ramkumar [8] showed the passive CMFD by combining the speeded up robust features (SURF), histogram of oriented gradients (HOG) and scale invariant feature transform (SIFT) features. Al-Hammadi and Emmanuel [9] proposed the speeded-up robust features (SURE) similar to the latter, but they aim to enhance key points detection by performing more steps before obtaining the SURF, which applies a single image super-resolution (SISR) method.

A mirror-reflection invariant feature transform (MIFT) is proposed by Agarwal and Mane [10] as an alternative to SIFT. Where the flipped images are produced by mirror reflection of the main images. Wenchang *et al.* [11] have the same idea of [8], [9] where they applied the SURF attributes, to solve the number of key points problems, Wenchang *et al.* [11] enhance the key point detection by using the particle swarm optimization (PSO). Moradi-Gharghani and Nasri [12] and Fadl and Semary [13] used the discrete cosine transform (DCT) for forgery detection where Fadl and Semary proposed a dynamic threshold to avoid any big plane area in the images. Applying this threshold, the number of chosen blocks reduced, and the pace of the technique was improved. An idea of dividing blocks into parts by fast k-means clustering technique was used in [13] to decrease the computational load. In [14], [15] extracted all features from the blocks by the discrete wavelet transform. Mahmood *et al.* [14] applied the stationary wavelet transform and Dixit and Naskar [15] applied undecimated dyadic wavelet transform. Where the latter used Canberra distance and the earlier used the Euclidean distance for distance measurement. Zhao *et al*. [16] added the PSO algorithm to the CMFD process to assess the identical area in the image and is not forged. Isaac and Wilscy [17] presented Harris corner detection for the key point CMFD technique to the discovery region of interest (ROI) and removed the unwanted blocks. The work presented by [18] utilizes the deep learning procedure for CMFD, where no traditional feature extrication method used. A survey by [19] listed several articles about CMFD.

Yang and Huang [20] split the image into blocks as the essential feature for the detection and then move all the blocks to a specific vector for the comparison step. The dimension of characteristics and number of blocks are the most important factor influencing the computation complexity. By using a fewer cumulative offset, they enhance the earlier methods for block matching. Their experimental results demonstrate that this technique can detect the forgery area successfully even while the forged image is saved in a losing format like JPEG.

Tejas *et al.* [21] propose different algorithms where it identifies a distinctive approach of using Hu's immutable moments and discrete cosine transformations (DCT) to achieve the required resize invariant and intensity invariant CMFD methods respectively. Because of failing in most techniques when the copied image is resized or added with specific concentration before pasting due to desynchronization of pixels in the search process. In the paper of Al-Qershi and Khoo [22], a new matching technique is presented, this technique reduces the computational time and improved the accuracy, by clustering the image to blocks and working only on the identical blocks in each cluster.

All of the above mentioned methods have some drawbacks. The computational cost is the main challenge in CMFD. Specifically, in high quality images, where the key point-based methods attempt to decrease the computational time, however, the precision is generally less than the block-based methods.

2. RELATED WORK

Too far, a number of CMFD strategies have been presented to efficiently solve the problem of region duplication. In this regard, the research aims to improve the representation of image areas in order to detect duplicated regions more precisely. Fridrich *et al.* [23] introduced the copy-move forgery detection approach employing DCT on small overlapping blocks for the first time in. DCT coefficients are used to create the feature vectors. After lexicographically sorting the feature vectors, the similarity between blocks is examined. Principal component analysis (PCA) is used to represent picture blocks in [24] where the authors employed nearly half of the number of features used by [23] by utilizing one of PCA's features. It improves the effectiveness of this approach, but it fails to identify copy-move forgery when rotated.

Li *et al.* [25] proposes a sorted neighborhood method based on the discreet wavelet transform (DWT). To get the feature vector, the image is split into four sub bands and the singular value decomposition (SVD) is used to the low frequency components. The method is only resistant to JPEG compression up to quality level 70. Mahdian and Saic in [26] introduces a strategy for extracting block features and *k-d* tree matching based on blur moment invariants up to 7th order.

For detecting image forgeries, Bayram *et al.* [2] suggests using the scaling and rotation invariant Fourier-Mellin transform (FMT) on the image blocks in conjunction with bloom filters. Huang *et al.* in [27] proposes an enhanced DCT-based approach for forgery detection by incorporating a sub setting mechanism to minimize the dimension of the feature vector. Zhao and Guo propose a method for identifying image forgeries based on DCT and SVD in [28]. The technique has been found to be resistant to compression, noise, and blurring, but it fails when pictures are rotated even slightly. Lynch *et al.* [29] proposed a direct block comparison based efficient expanding block approaching. Li *et al.* [30] performs circular block extraction and obtains features using rotation invariant uniform local binary patterns (LBP). Blurring, additive noise, compression, flipping, and rotation do not affect the approach. This method, however, was unable to detect fabricated sections rotated at arbitrary angles.

For detecting comparable regions in the photos, the scientists used a new robust collection of keypoint-based features termed MIFT in [31]. Li *et al.* [6] used the polar harmonic transform (PHT) to extract feature vectors from circular blocks in order to identify image frauds. In the block matching stage, the authors in [32] presents an adaptive similarity threshold-based technique. Thresholds proportional to the blocks standard deviations are used to detect fabricated sections.

The approach based on the HOG is proposed in [33] for detecting copy-move forged areas. The multiscale Weber's law descriptor (multi-WLD) and multiscale local binary pattern (LBP) features are retrieved from chrominance components in [34] for image splicing and copy-move forgery detection. The authors used SVM to determine if a picture was genuine or fake. By merging the enhanced pulse coupled neural network (PCNN) with self-selected sub-images, Zhou *et al.* in [35] were the first who present an image copy-move forgery passive detection approach. Zhu *et al.* [36] created a Gaussian scale space for each scale space, retrieved the oriented FAST key points and ORB features in each scale space, utilized hamming distance to compare features, and then used random sample consensus (RANSAC) to remove mismatches.

Prakash *et al.* [37] extracted image feature points and blended them into mixed image features using accelerated KAZE (AKAZE) and SIFT, then used g2NN to match features and find forged sections. To achieve accurate matches, Paul *et al.* [38] employed (SURF) to extract important spots from the picture, followed by k-nearest neighbor (kNN) training and mapping. To detect counterfeit areas, Chen *et al.* [39] devised a system that employed SIFT, moment-invariant computation, and region growth strategies.

3. RESEARCH METHOD

K-means are proposed here for detecting the copy-move forgery. K-means is able to segment the image to k-clusters [40]–[50], the main challenge of this method is the performance of k-means is very sensitive to the K (number of clusters) while determining the ideal k is very difficult. However, the density-based methods do not require determining the number of clusters, such as DBSCAN. DBSCAN algorithm generates the segmentation by processing the super pixels to find clusters of superpixels. Where the superpixels are generated by the SLIC; the simple linear iterative clustering. In the proposed method several steps have been performed, which can be concluded in the following Figure 1, followed by the explanation for the used algorithm.

Step 1: Image preprocessing, which includes applying adjustment on the input image. This method works on grayscale images and generates new values to be mapped with the intensity values to enhance the image to the next step. This operation increases the contrast of the input image.

Step 2: Image segmentation, in this step, the image blocks was grouped into clusters and analyze each cluster separately. Image segmentation used as a pre-step to the feature's extraction step, and it can be considered as a searcher tool that discovers sudden cutout in the pixel values, which indicate edges that find the similarities in the image. A number of clustering methods were used in literature for image segmentation [51], in this work two methods are implemented, the first one is SLIC followed by DBSCAN which used to classify and extract the objects from the image then some morphological cleanup operations are executed after applying the clustering to remove very big and very small regions (objects) the second is the k-means clustering algorithm, also a specific threshold is used to merge the remained objects according to the Euclidean distance between each two object's centroids (if this distance is less than this threshold so, merge these two objects and repeat this till all centroid’s of remained objects are separated with more than this threshold). The threshold value is based on the nature and size of images in the used dataset. The following sections give a brief description of the basics of SLIC-DBSCAN and k-means. Step 2 executed by two different techniques. The first includes implementing super pixels generation (SLIC) followed by applying DBSCAN and the second executed using k-means method. SLIC is a clustering algorithm used in this work to find the color similarity and proximity to generates super pixels. Steps for the SLIC algorithm can be found in [52]. DBSCAN algorithm is used to integrate the spatial connectivity and color similarity with each other in the segmentation process. K-means needs a parameter K to be determined but DBSCAN does not require stating this parameter. DBSCAN finds areas of high density that are separated from one another by regions of low density. DBSCAN needs two parameters to form a cluster, the first one is epsilon which is a threshold for a neighborhood search query and the second one is minimum points (MINPTS) which is a positive integer used as a threshold to determine whether a point is a core point. DBSCAN is based on some rules and definitions most of them stated in [53], [54]. K-means is type of clustering is categorized as an unsupervised learning algorithm that able to use the background of an image for segmentation. K-means uses the given value k to find the K-centroids to cluster the data to K parts. The (1) shows the objective function for the k-means clustering which designed to minimize the total squared distances between K-centroids and all points.

$$J = \sum_{j=1}^{k} \sum_{i=1}^{n} \left\| x_i^{(j)} - C_j \right\|^2 \qquad (1)$$

Where the number of clusters is k, each cluster j has centroid denoted as (C_j), n is the number of data points, and $\left\| x_i^{(j)} - C_j \right\|^2$ describes the distance function. Details of k-means procedures are available at [55].

Step 3: Features extraction, which executed by measuring the properties of each region in the image, these properties include; the area which describes the real number of pixels in the region, the major axis length in pixels which describes the length of the major axis of the ellipse that has the same normalized second central moments as the region, returned as a scalar, bounding box which refers to position and size of the smallest box containing the region, centroid which describes the center of mass of the region, eccentricity is the ratio of the distance between the foci of the ellipse and its major axis length, minor axis length which refers to the length (in pixels) of the minor axis of the ellipse that has the same normalized second central moments as the region and the orientation which refers to the angle between the x-axis and the major axis of the ellipse that has the same second-moments as the region. All these features were measured for all continuous objects in the image to execute the matching depending on the nearest values and the greatest matching number in these features.

Step 4: Detecting copy move regions, in this step, both the original and the copied parts are bounded by rectangles which detect the presence of copy-move objects in the image depending on the matching of the features for each object with the other objects in the same image.

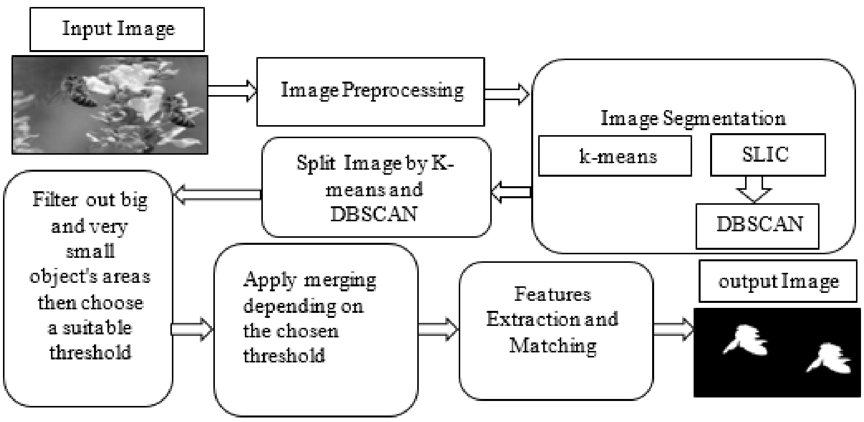


Figure 1. Steps of the proposed work

4. RESULTS AND DISCUSSION

This work concerned copy-move forgery detection regardless of which part in the image is the original and which one is the copy. To measure the effectiveness of the proposed algorithms the following parameters calculated: i) true positive (TP) which refers to the total number of pixels that are forged regions and recognized by the algorithms as forged regions; ii) true negative (TN) which refers to the total number of pixels that are forged regions but recognized by the algorithm as not forged regions; iii) false positive (FP) which refers to the total number of pixels that are not forged regions but recognized by the algorithm as forged regions; iv) false negative (FN) which refers to the total number of pixels that are not forged regions and recognized by the algorithm as not forged regions. Then the evaluation metrics calculated according to the previous measures as described in the (2)-(5) [56].

$$Verification\ rate(V_r) = \frac{TP}{TP+FN} \tag{2}$$

$$Accuracy\ rate(A_r) = \frac{TP+TN}{TP+TN+FP+FN} \tag{3}$$

$$Error\ rate\ (E_r) = \frac{FP+FN}{TP+FN} \tag{4}$$

$$False\ Possitive\ rate(FP_r) = \frac{FP}{FP+TN} \tag{5}$$

To test the proposed work, the dataset named free-form copy-move dataset [57] is used. This dataset contains 160 test images. In this dataset, all the test images contain free-form copy-move forgery operations. The tested images have been derived from 5 distinct main images. The images used for testing were processed by JPEG compression, Gaussian filtering, and combinations of these two processes. Figure 2 shows some examples of forged images after applying (k-means) and the detected copy-move regions, where we use 4 clusters for the first image, 5 clusters for the second one and 3 clusters for the last image.

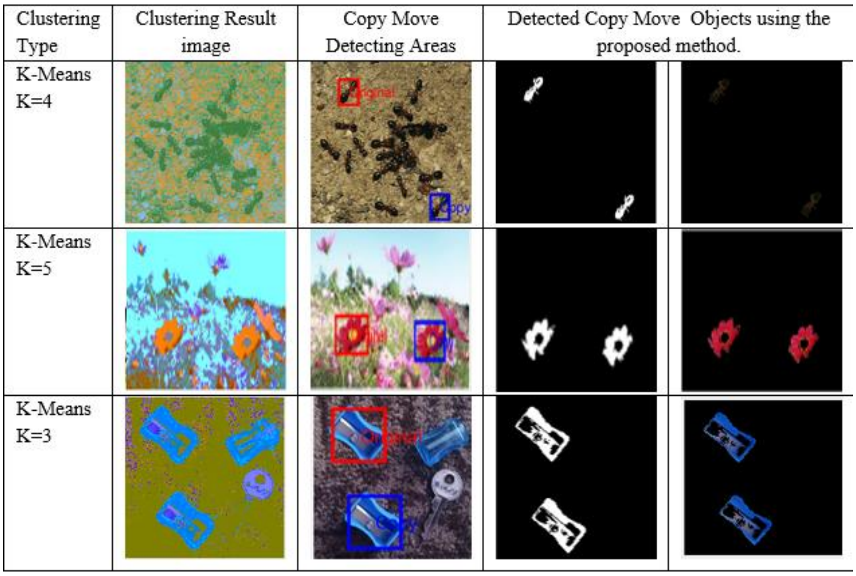


Figure 2. Examples of forged images after applying (k-means) and the corresponding detected copy move regions

Figure 3 shows the same images that used in Figure 2 after applying (SLIC-DBSCAN clustering) and the detected copy-move regions. It can be seen obviously after using the SLIC-DBSCAN clustering method in Figure 3, the detecting forgery objects are clearer and colored in more thoroughness compared with Figure 2. Figures 4-6 show a complete description for all the available accuracy metrics used to compare the executed methods and the method used in [57].

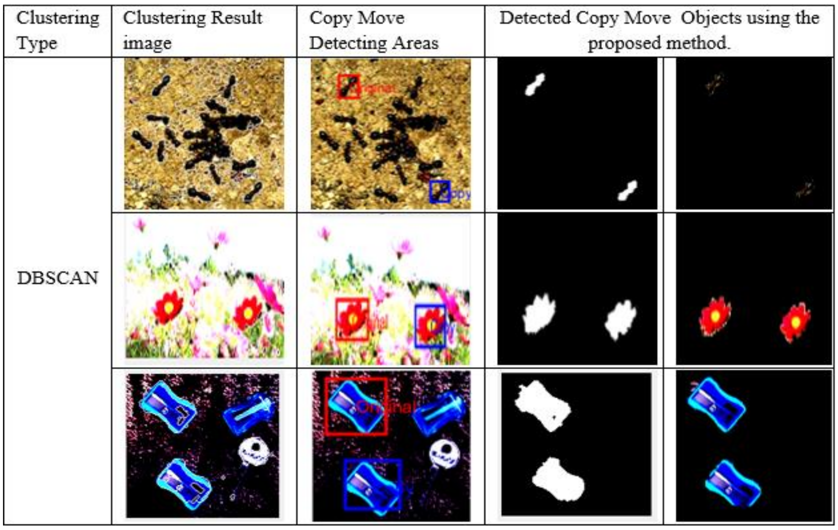
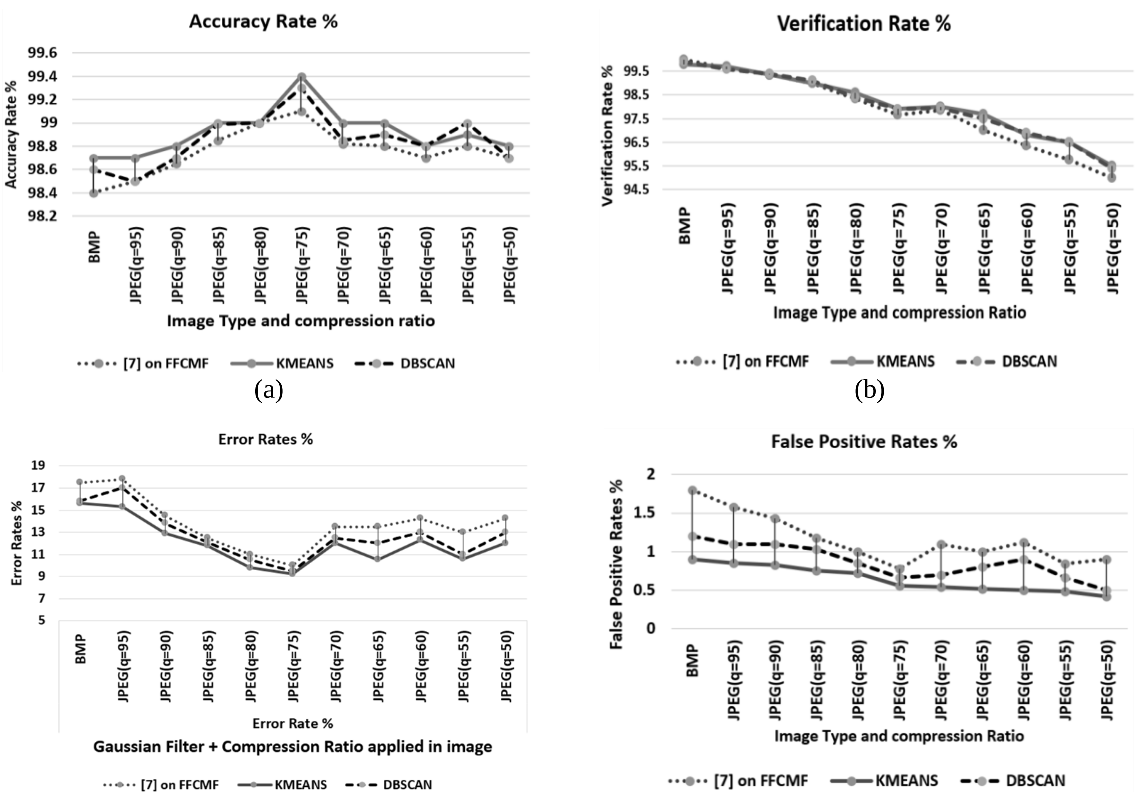


Figure 3. Same examples of Figure 2 after applying (SLIC-DBSCAN clustering) and the corresponding detected copy move regions

Figures 4, 5 and 6 compare the obtained results by applying KMEANS and DBSCAN with the results using FFCMF included in [57]. The images used in Figure 4 were in different formats, one of these formats was without applying any type of compression on the image (BMP) and the other format was compressed images with different compression factor (q=95, 90, 85, 80, 75, 70, 65, 60, 55, 50) then the evaluation metrics; Figure 4(a) accuracy rates, Figure 4(b) verification rates, Figure 4(c) error rates, and Figure 4(d) false positive rates in equations two to five were calculated using (2) to (5), respectively.



(a) (b) (c) (d)

Figure 4. The verification rates and accuracies for CMFD with no postprocessing and JPEG compression (a) accuracy rates, (b) verification rates, (c) error rates, and (d) false positive rates

In Figure 5, the images used contained two types of images, the first type was without compression but filtered using a gaussian filter (GF on BMP) and the second type included Gaussian filtered images followed by compression with different compression factors (q=95, 90, 85, 80, 75, 70, 65, 60, 55, 50). where Figure 5(a)-(d) illustrated the accuracy rates, verification rates, false positive rates, and error rates, respectively. In Figure 6, the images used were included JPEG compression images with different compression factors also followed by applying Gaussian filtering.

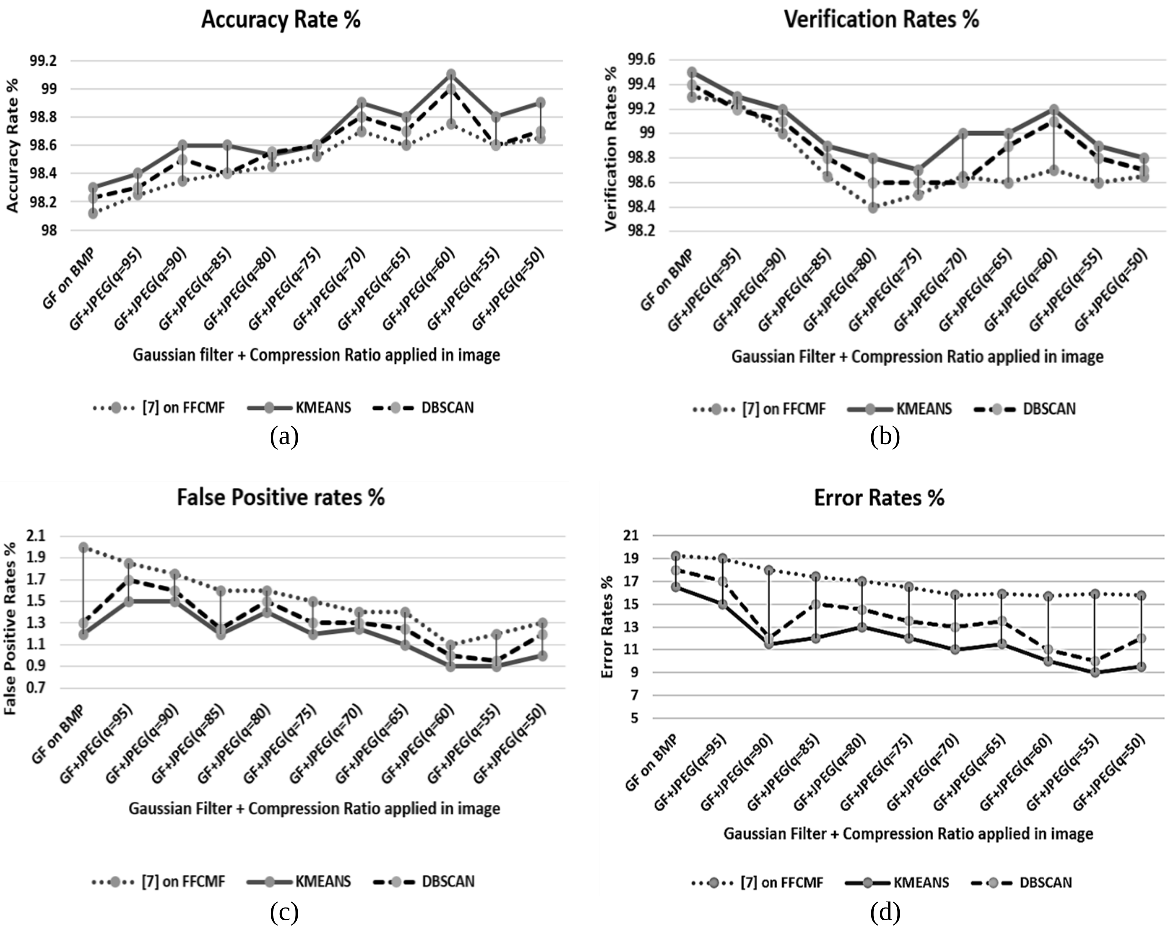


Figure 5. The verification rates and accuracies for CMFD with only Gaussian filtering or Gaussian filtering followed by JPEG compression (a) accuracy rates, (b) verification rates, (c) false positive rates, and (d) error rates

Figures 4 and 5 (a and b) show the fluctuate in the line when they have been plotted in order of accuracy rate and verification rate for the CMFD without postprocessing and they show the KMEAN as the best method where it gives more accuracy and verification rate, and Figures 4(c) and 4(d) illustrates that the KMEAN gives the less error rate and false positive. In Figure 6(a) the k-mean method shows high accuracy comparing with Figures 4 and 5 and other methods where it arrives to 99.85% after using the JPEG compression and afterward Gaussian filtering, and for the verification rate in Figure 6(b) it arrives to 99.5%. Regarding the error rate and false positive rate, all the values that achieved is better as illustrated in Figures 6(c) and 6(d).

As shown from the Figures 4 to 6 the verification rates and accuracies for CMFD with no postprocessing and JPEG compression and also with only Gaussian filtering or Gaussian filtering afterward JPEG compression and with JPEG compression afterward Gaussian filtering for the proposed work were approximately similar to the results obtained in [56] and k-means achieved better than SLIC-DBSCAN with some images but error rate (Er) and false-positive rate (FPr) for the proposed work was better than the results obtained in [56] which means that the total number of pixels that are forged region pairs but detected as forged by the proposed work was smaller and this also reflects on the error rates.

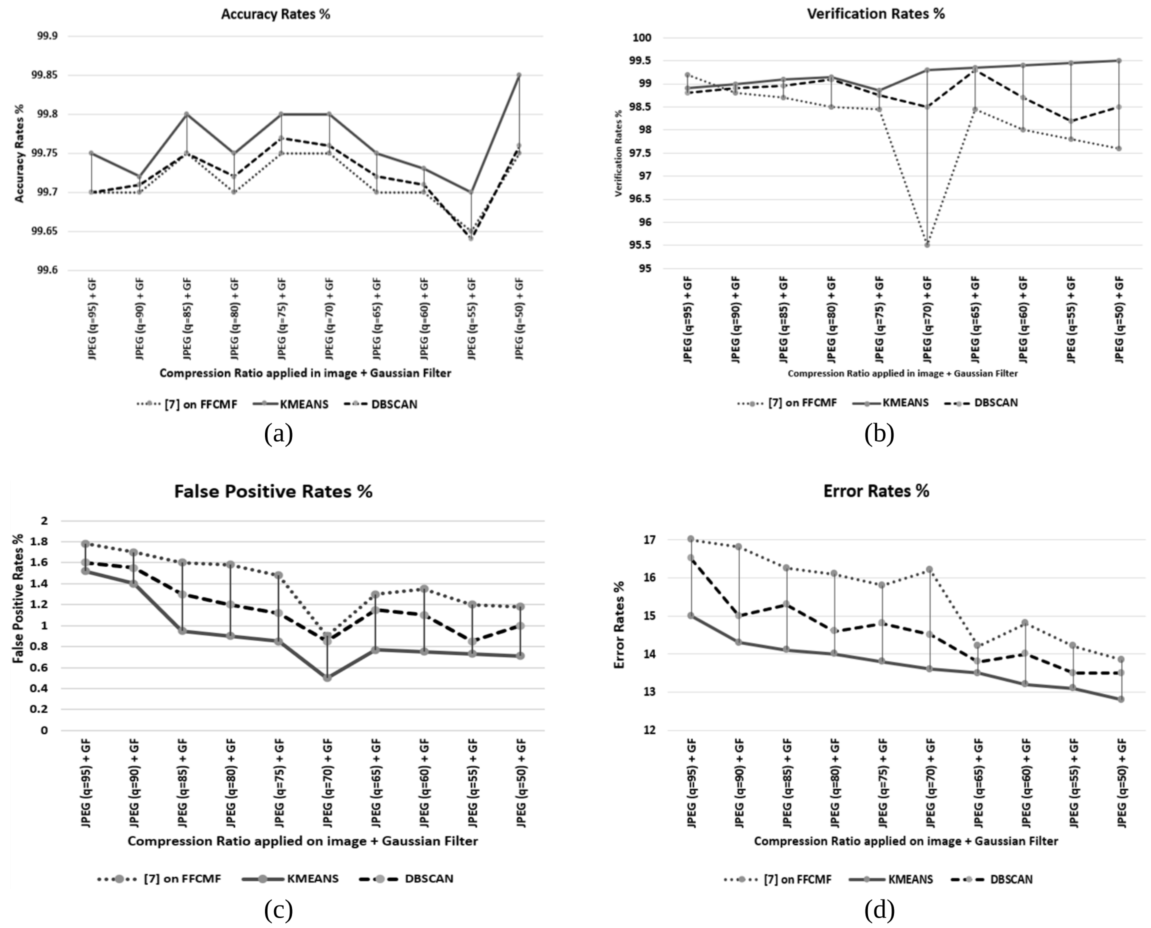


Figure 6. The verification rates and accuracies for CMFD with JPEG compression followed by Gaussian filtering (a) accuracy rates, (b) verification rates, (c) false positive rates, and (d) error rates

5. CONCLUSION

This paper has introduced a comparison for image segmentation methods used for copy move detection. Two methods for segmentation based on two clustering algorithms (i.e., k-means and super pixel segmentation with DBSCAN) were implemented and some morphological cleanup operations were executed to improve the accuracy of detecting the forgery regions of digital images. The results showed improvements in the accuracy of detecting the forgery regions of digital images with k-means algorithm and this algorithm shows better performance compared with other techniques in the literature. As future work, the implementation of the multi clustering method will be used by applying the subtractive clustering algorithm.

REFERENCES

[1] H. Farid, “Image forgery detection,” *IEEE Signal Processing Magazine*, vol. 26, no. 2, pp. 16–25, Mar. 2009, doi: 10.1109/MSP.2008.931079.

[2] S. Bayram, H. T. Sencar, and N. Memon, “An efficient and robust method for detecting copy-move forgery,” in *2009 IEEE International Conference on Acoustics, Speech and Signal Processing*, Apr. 2009, pp. 1053–1056, doi: 10.1109/ICASSP.2009.4959768.

[3] H.-J. Lin, C.-W. Wang, and Y.-T. Kao, “Fast copy-move forgery detection,” *WSEAS Transactions on Signal Processing*, vol. 5, no. 5, pp. 188–197, 2009.

[4] M. Zimba and S. Xingming, “DWT-PCA (EVD) based copy-move image forgery detection,” *International Journal of Digital Content Technology and its Applications*, vol. 5, no. 1, pp. 251–258, Jan. 2011, doi: 10.4156/jdcta.vol5.issue1.27.

[5] J. Hu, H. Zhang, Q. Gao, and H. Huang, “An improved lexicographical sort algorithm of copy-move forgery detection,” in *2011 Second International Conference on Networking and Distributed Computing*, 2011, pp. 23–27, doi: 10.1109/ICNDC.2011.12.

[6] L. Li, S. Li, H. Zhu, and X. Wu, “Detecting copy-move forgery under affine transforms for image forensics,” *Computers and Electrical Engineering*, vol. 40, no. 6, pp. 1951–1962, Aug. 2014, doi: 10.1016/j.compeleceng.2013.11.034.

[7] R. Kushol, M. S. Salekin, M. H. Kabir, and A. A. Khan, “Copy-move forgery detection using color space and moment invariants-based features,” in *2016 International Conference on Digital Image Computing: Techniques and Applications (DICTA)*, Nov. 2016, pp. 1–6, doi: 10.1109/DICTA.2016.7797027.

[8] S. Prasad and B. Ramkumar, "Passive copy-move forgery detection using SIFT, HOG and SURF features," in *2016 IEEE International Conference on Recent Trends in Electronics, Information and Communication Technology (RTEICT),* May 2016, pp. 706–710, doi: 10.1109/RTEICT.2016.7807915.

[9] M. M. Al-Hammadi and S. Emmanuel, "Improving SURF based copy-move forgery detection using super resolution," in *2016 IEEE International Symposium on Multimedia (ISM)*, Dec. 2016, pp. 341–344, doi: 10.1109/ISM.2016.0075.

[10] V. Agarwal and V. Mane, "Reflective SIFT for improving the detection of copy-move image forgery," in *2016 Second International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN)*, Sep. 2016, pp. 84–88, doi: 10.1109/ICRCICN.2016.7813636.

[11] S. Wenchang, Z. Fei, Q. Bo, and L. Bin, "Improving image copy-move forgery detection with particle swarm optimization techniques," *China Communications*, vol. 13, no. 1, pp. 139–149, Jan. 2016, doi: 10.1109/CC.2016.7405711.

[12] H. Moradi-Gharghani and M. Nasri, "A new block-based copy-move forgery detection method in digital images," in *2016 International Conference on Communication and Signal Processing (ICCSP)*, Apr. 2016, pp. 1208–1212, doi: 10.1109/ICCSP.2016.7754344.

[13] S. M. Fadl and N. A. Semary, "A proposed accelerated image copy-move forgery detection," in *2014 IEEE Visual Communications and Image Processing Conference*, Dec. 2014, pp. 253–257, doi: 10.1109/VCIP.2014.7051552.

[14] T. Mahmood, T. Nawaz, Z. Mehmood, Z. Khan, M. Shah, and R. Ashraf, "Forensic analysis of copy-move forgery in digital images using the stationary wavelets," in *2016 Sixth International Conference on Innovative Computing Technology (INTECH)*, Aug. 2016, pp. 578–583, doi: 10.1109/INTECH.2016.7845040.

[15] R. Dixit and R. Naskar, "DyWT based copy-move forgery detection with improved detection accuracy," in *2016 3rd International Conference on Signal Processing and Integrated Networks (SPIN)*, Feb. 2016, pp. 133–138, doi: 10.1109/SPIN.2016.7566676.

[16] F. Zhao, W. Shi, B. Qin, and B. Liang, "A copy-move forgery detection scheme with improved clone region estimation," in *2016 Third International Conference on Trustworthy Systems and their Applications (TSA)*, Sep. 2016, pp. 8–16, doi: 10.1109/TSA.2016.12.

[17] M. M. Isaac and M. Wilscy, "A key point based copy-move forgery detection using HOG features," in *2016 International Conference on Circuit, Power and Computing Technologies (ICCPCT),* Mar. 2016, pp. 1–6, doi: 10.1109/ICCPCT.2016.7530253.

[18] Y. Rao and J. Ni, "A deep learning approach to detection of splicing and copy-move forgeries in images," in *2016 IEEE International Workshop on Information Forensics and Security (WIFS),* Dec. 2016, pp. 1–6, doi: 10.1109/WIFS.2016.7823911.

[19] A. D. Warbhe, R. V. Dharaskar, and V. M. Thakare, "A survey on keypoint based copy-paste forgery detection techniques," *Procedia Computer Science*, vol. 78, pp. 61–67, 2016, doi: 10.1016/j.procs.2016.02.011.

[20] Q.-C. Yang and C.-L. Huang, "Copy-move forgery detection in digital image," in *Advances in Multimedia Information Processing-PCM 2009*, Springer Berlin Heidelberg, 2009, pp. 816–825.

[21] K. Tejas, C. Swathi, and M. R. Kumar, "Intensity and rescale invariant copy move forgery detection techniques," *CoRR*, Sep. 2018.

[22] O. M. Al-Qershi and B. E. Khoo, "Copy-move forgery detection using on locality sensitive hashing and k-means clustering," in *Lecture Notes in Electrical Engineering*, Springer Singapore, 2016, pp. 663–672.

[23] A. J. Fridrich, B. D. Soukal, and A. J. Lukas, "Detection of copy-move forgery in digital images," *Proceedings of Digital Forensic Research Workshop*, 2003.

[24] A. C. Popescu and H. Farid, "Exposing digital forgeries by detecting traces of resampling," *IEEE Transactions on Signal Processing*, vol. 53, no. 2, pp. 758–767, Feb. 2005, doi: 10.1109/TSP.2004.839932.

[25] G. Li, Q. Wu, D. Tu, and S. Sun, "A sorted neighborhood approach for detecting duplicated regions in image forgeries based on DWT and SVD," in *2007 IEEE International Conference on Multimedia and Expo*, Jul. 2007, pp. 1750–1753, doi: 10.1109/ICME.2007.4285009.

[26] B. Mahdian and S. Saic, "Detection of copy-move forgery using a method based on blur moment invariants," *Forensic Science International*, vol. 171, no. 2–3, pp. 180–189, Sep. 2007, doi: 10.1016/j.forsciint.2006.11.002.

[27] Y. Huang, W. Lu, W. Sun, and D. Long, "Improved DCT-based detection of copy-move forgery in images," *Forensic Science International*, vol. 206, no. 1–3, pp. 178–184, Mar. 2011, doi: 10.1016/j.forsciint.2010.08.001.

[28] J. Zhao and J. Guo, "Passive forensics for copy-move image forgery using a method based on DCT and SVD," *Forensic Science International*, vol. 233, no. 1–3, pp. 158–166, Dec. 2013, doi: 10.1016/j.forsciint.2013.09.013.

[29] G. Lynch, F. Y. Shih, and H.-Y. M. Liao, "An efficient expanding block algorithm for image copy-move forgery detection," *Information Sciences*, vol. 239, pp. 253–265, Aug. 2013, doi: 10.1016/j.ins.2013.03.028.

[30] L. Li, S. Li, H. Zhu, S.-C. Chu, J. F. Roddick, and J.-S. Pan, "An efficient scheme for detecting copy-move forged images by local binary patterns," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 4, no. 1, pp. 46–56, 2013.

[31] M. Jaberi, G. Bebis, M. Hussain, and G. Muhammad, "Accurate and robust localization of duplicated region in copy-move image forgery," *Machine Vision and Applications*, vol. 25, no. 2, pp. 451–475, Feb. 2014, doi: 10.1007/s00138-013-0522-0.

[32] M. Zandi, A. Mahmoudi-Aznaveh, and A. Mansouri, "Adaptive matching for copy-move forgery detection," in *2014 IEEE International Workshop on Information Forensics and Security (WIFS)*, 2014, pp. 119–124, doi: 10.1109/WIFS.2014.7084314.

[33] J.-C. Lee, C.-P. Chang, and W.-K. Chen, "Detection of copy-move image forgery using histogram of orientated gradients," *Information Sciences*, vol. 321, pp. 250–262, Nov. 2015, doi: 10.1016/j.ins.2015.03.009.

[34] M. Hussain, S. Qasem, G. Bebis, G. Muhammad, H. Aboalsamh, and H. Mathkour, "Evaluation of image forgery detection using multi-scale weber local descriptors," *International Journal on Artificial Intelligence Tools*, vol. 24, no. 4, Aug. 2015, doi: 10.1142/s0218213015400163.

[35] G. Zhou, X. Tian, and A. Zhou, "Image copy-move forgery passive detection based on improved PCNN and self-selected sub-images," *Frontiers of Computer Science*, vol. 16, no. 4, Aug. 2022, doi: 10.1007/s11704-021-0450-5.

[36] Y. Zhu, X. Shen, and H. Chen, "Copy-move forgery detection based on scaled ORB," *Multimedia Tools and Applications*, vol. 75, no. 6, pp. 3221–3233, Mar. 2016, doi: 10.1007/s11042-014-2431-2.

[37] C. S. Prakash, P. P. Panzade, H. Om, and S. Maheshkar, "Detection of copy-move forgery using AKAZE and SIFT keypoint extraction," *Multimedia Tools and Applications*, vol. 78, no. 16, pp. 23535–23558, Aug. 2019, doi: 10.1007/s11042-019-7629-x.

[38] K. H. Paul, K. R. Akshatha, A. K. Karunakar, and S. Seshadri, "SURF based copy move forgery detection using kNN mapping," in *Advances in Intelligent Systems and Computing, Springer International Publishing*, 2020, pp. 234–245.

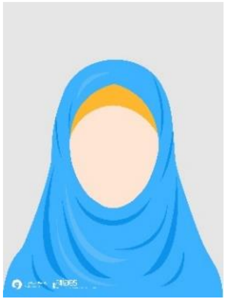
[39] C.-C. Chen, W.-Y. Lu, and C.-H. Chou, "Rotational copy-move forgery detection using SIFT and region growing strategies," *Multimedia Tools and Applications*, vol. 78, no. 13, pp. 18293–18308, Jul. 2019, doi: 10.1007/s11042-019-7165-8.

[40] M. K. Alsmadi, "A hybrid fuzzy C-Means and neutrosophic for jaw lesions segmentation," *Ain Shams Engineering Journal*, vol. 9, no. 4, pp. 697–706, Dec. 2018, doi: 10.1016/j.asej.2016.03.016.

[41] M. K. Alsmadi, "Content-based image retrieval using color, shape and texture descriptors and features," *Arabian Journal for Science and Engineering*, vol. 45, no. 4, pp. 3317–3330, Apr. 2020, doi: 10.1007/s13369-020-04384-y.

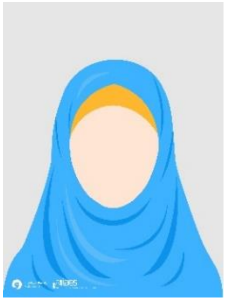
[42] M. K. Alsmadi, "An efficient similarity measure for content based image retrieval using memetic algorithm," *Egyptian Journal of Basic and Applied Sciences*, vol. 4, no. 2, pp. 112–122, Jun. 2017, doi: 10.1016/j.ejbas.2017.02.004.
[43] M. K. Alsmadi, M. Tayfour, R. A. Alkhasawneh, U. Badawi, I. Almarashdeh, and F. Haddad, "Robust features extraction for general fish classification," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 9, no. 6, pp. 5192–5204, Dec. 2019, doi: 10.11591/ijece.v9i6.pp5192-5204.
[44] M. K. Alsmadi, "A hybrid firefly algorithm with fuzzy-c mean algorithm for MRI brain segmentation," *American Journal of Applied Sciences*, vol. 11, no. 9, pp. 1676–1691, Sep. 2014, doi: 10.3844/ajassp.2014.1676.1691.
[45] M. K. Alsmadi, "MRI brain segmentation using a hybrid artificial bee colony algorithm with fuzzy-c mean algorithm," *Journal of Applied Sciences*, vol. 15, no. 1, pp. 100–109, Dec. 2014, doi: 10.3923/jas.2015.100.109.
[46] M. K. Alsmadi, "Facial expression recognition," *US20180211102A1*, 2018.
[47] M. K. Alsmadi and I. Almarashdeh, "A survey on fish classification techniques," *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 5, pp. 1625–1638, May 2022, doi: 10.1016/j.jksuci.2020.07.005.
[48] M. Alzaqebah et al., "Memory based cuckoo search algorithm for feature selection of gene expression dataset," *Informatics in Medicine Unlocked*, vol. 24, 2021, doi: 10.1016/j.imu.2021.100572.
[49] M. K. Alsmadi, "Query-sensitive similarity measure for content-based image retrieval using meta-heuristic algorithm," *Journal of King Saud University-Computer and Information Sciences*, vol. 30, no. 3, pp. 373–381, 2018, doi: 10.1016/j.jksuci.2017.05.002.
[50] A. Abuhamdah, G. M. Jaradat, and M. Alsmadi, "Deep learning for COVID-19 cases-based XCR and chest CT images," in *Advances on Smart and Soft Computing*, Springer Singapore, 2022, pp. 285–299.
[51] N. Dhanachandra, K. Manglem, and Y. J. Chanu, "Image segmentation using k-means clustering algorithm and subtractive clustering algorithm," *Procedia Computer Science*, vol. 54, pp. 764–771, 2015, doi: 10.1016/j.procs.2015.06.090.
[52] R. Achanta, A. Shaji, K. Smith, A. Lucchi, P. Fua, and S. Susstrunk, "Slic superpixels," *Technical report*, EPFL, 2010.
[53] A. Dhua, D. N. Sarma, S. Singh, and B. Roy, "Segmentation of images using density-based algorithms," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 4, no. 5, pp. 273–277, 2015.
[54] Q. Ye, W. Gao, and W. Zeng, "Color image segmentation using density-based clustering," in *2003 International Conference on Multimedia and Expo. ICME'03, Proceedings (Cat. No. 03TH8698)*, vol. 2, 2003, doi: 10.1109/ICME.2003.1221638.
[55] N. S. Chauhan, "Introduction to image segmentation with k-means clustering." https://www.kdnuggets.com/2019/08/introduction-image-segmentation-k-means-clustering.html (accessed Jul. 05, 2022).
[56] E. Gürbüz, G. Ulutas, and M. Ulutas, "Detection of free-form copy-move forgery on digital images," *Security and Communication Networks*, vol. 2019, Art. no. 8124521, pp. 1-14, 2019. doi: 10.1155/2019/8124521.
[57] N. Dhanachandra and Y. J. Chanu, "A survey on image segmentation methods using clustering techniques," *European Journal of Engineering Research and Science*, vol. 2, no. 1, Jan. 2017, doi: 10.24018/ejers.2017.2.1.237.

BIOGRAPHIES OF AUTHORS



Eman Abdulazeem Ahmed is currently an assistant professor at the Faculty of Science, Department of Mathematics, Imam Abdulrahman Bin Faisal University, Dammam, Saudi Arabia. She received her BS degree in Electronics Engineering in 1999 and M.Sc. degree and Ph.D. in Electrical Communications Engineering from Mansoura University, Faculty of Engineering, Electronics and Communications Engineering Department, Egypt. Her research interests include image and video processing, pattern recognition, information security, optimization and computer vision. She can be contacted at email: eabdulazeem00@gmail.com.

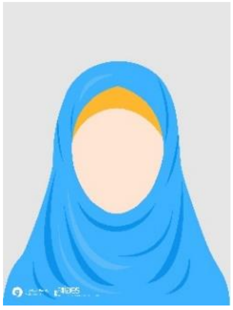
Malek Alzaqebah obtained his B.Sc. in computer science from Al-Balqa Applied University, Jordan and his master degree specializing in information technology from University Utara Malaysia (UUM). He did his Ph.D. in computer science at University Kebangsaan Malaysia (UKM). Now, he is an assistant professor at the Department of Mathematics, Faculty of Science, Imam Abdulrahman Bin Faisal University, Dammam, Saudi Arabia. His research interest involves data mining and metaheuristic algorithms for combinatorial optimization problems such as university timetabling, job shop scheduling, vehicle routing and search-based software engineering. He can be contacted at email: maafehaid@iau.edu.sa.



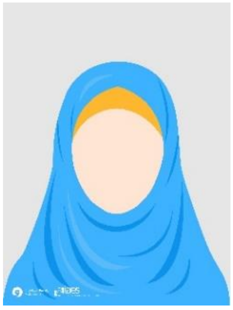
Sana Jawarneh obtained her B.Sc. in computer engineering from Yarmouk University and her Ph.D. in computer science at University Kebangsaan Malaysia. Now, she is an assistant professor at Department of computer science, The applied college, Imam Abdulrahman Bin Faisal University, Dammam, Saudi Arabia. Her research interest falls under meta-heuristic algorithms in various optimization problems. She can be contacted at email: sijawarneh@iau.edu.sa.

Jehad Saad Alqurni received the M.S. degree in computer science (software engineering) from the University of Wollongong, Wollongong, Australia, in 2009, and the Ph.D. degree in computer science from the Heriot-Watt University, U.K., in 2020. From 2005 to 2010, he was a Teaching Assistant with the Imam Abdulrahman Bin Faisal University, Saudi Arabia, a Lecturer from 2010 to 2019, and has been an Assistant Professor since 2020. His research interests include the software engineering, human computer interaction, usability, web usability, E-Learning and information systems. He can be contacted at email: jalqurni@iau.edu.sa.

Fahad A. Alghamdi is currently an assistant at the Faculty of Applied Studies and Community Service, Department of Management of Information Systems, Imam Abdurrahman Bin Faisal University, Saudi Arabia. He received his BS degree in computer science in 2002 from Imam Abdurrahman Bin Faisal University, Saudi Arabia, his MSc degree in computer science in 2009 from University Wollongong, Australia, and his Ph.D. in Computer Science in 2017 from Aberystwyth University in UK. His research interests include network, applied computer software, cloud computing and online learning. He is currently the Vice Dean of Faculty of Applied Studies and Community Service, Imam Abdurrahman Bin Faisal University, Saudi Arabia. He can be contacted at email: faghamdi@iau.edu.sa.



Hayat Alfagham received her BS degree in Computer Information Systems from King Faisal University, Saudi Arabia, her MSc degree in intelligent systems in 2015 from Kings College London, United Kingdom, and her Ph.D. in Computer Science in 2020 from Queen Mary University of London. She is currently an associate professor at the Faculty of Applied Studies and Community Service, Department of Management of Information Systems, Imam Abdurrahman Bin Faisal University. Her research interests include Link prediction, Big Data, Pattern recognition, Machine Learning, Network evolution. She can be contacted at email: hmalfagham@iau.edu.sa.



Lubna Mahmoud Abdel Jawad is currently an innovation and technology lecturer at Healthcare Management and Economic collage, Gulf Medical university. She received her BS degree in software engineering in 2008 from Petra University, Jordan. Her MSc degree in 2012 from Al-Balqa' Applied University, Jordan. She can be contacted at email: lubnaabdeljawad@gmail.com.

Usama A. Badawi An Assistant Professor of computer Science. His Ph.D. degree in the field of object-oriented distributed systems that is practically performed in the Technical University of Darmstadt-Germany. Has attended many scientific activities such as CIMPA school in Nice-France. Has published many scientific researches in different computer application areas (RG-Score 10.62). Dr. Badawi is a member in the reviewing board in many scientific journals such as the International Journal of Research in Engineering, Science and Management (IJRESM), The International Journal of parallel and Distributed systems, Elsevier Publications, The International Computer Journal, Oxford University Press and the Journal of Advances in Information Sciences and Service Sciences. He has supervised many M.Sc. and Ph.D. theses as well. Dr. Badawi research interests are computer applications in business, artificial intelligence, distributed systems, image processing, and blockchain applications. He can be contacted at email: ubadawi@gmail.com.

Mutasem K. Alsmadi is currently an associate professor at the Faculty of Applied Studies and Community Service, Department of Management of Information Systems, Imam Abdurrahman Bin Faisal University. He received his BS degree in Software engineering in 2006 from Philadelphia University, Jordan, his MSc degree in intelligent systems in 2007 from University Utara Malaysia, Malaysia, and his Ph.D. in Computer Science from The National University of Malaysia. He has published more than one hundred papers in the image processing and Algorithm optimization areas. His research interests include artificial intelligence, pattern recognition, algorithms optimization and computer vision. He can be contacted at email: mksalsmadi@gmail.com.

Ibrahim Almarashdeh is currently an associate professor at the Faculty of Applied Studies and Community Service, Department of Management of Information Systems, Imam Abdurrahman Bin Faisal University. He received his B.Sc. from University of Jordan in 2001. His M.Sc. degree in information and communication technology in in 2007 from University Utara Malaysia, and his Ph.D. in Software engineering/Industrial computing from The National University of Malaysia award in 2012. He has published number of research papers and his research include: human computer interaction, image processing and algorithm optimization areas and software development and usability, requirements analysis, mobile government and mobile learning. He can be contacted at email: ibramars@gmail.com.