Copy-Move Forgery Detection Based on Enhanced Patch-Match

Younis E. Abdalla[1], M. Tariq Iqbal[2] and M. Shehata[3]

**[1] Faculty of Engineering and Applied Science, Memorial University of Newfoundland
St. John's, Newfoundland A1B 2K6, Canada**

**[2] Faculty of Engineering and Applied Science, Memorial University of Newfoundland St.
John's, Newfoundland A1B 2K6, Canada**

**[3] Faculty of Engineering and Applied Science, Memorial University of Newfoundland St.
John's, Newfoundland A1B 2K6, Canada**

Abstract

Image forgery detection approaches are varied and serve same objectives. However, the difference in image properties causes some limitations of most of these approaches. Integrate multiple forensic approaches to increase the efficiency of detecting and localize the forgery was proposed based on the same image input source. In this paper, we propose a new detector algorithm based on different image source format. We propose approach to detect a copy-move forgery based on PatchMatch enhanced by the dense field technique. The F-measure score used same evaluation function to make the system more robust. The output result shows high efficiency of detecting and localizing the forgery in different image formats, for passive forgery detection.

Keywords: *Copy-move detect; forgery localization; image forgery; score evaluation*

1. Introduction

One way to divide the professionals from the amateurs in any given field is to take a look at the equipment they use to accomplish their tasks. Advanced technology is currently the go-to equipment used by forgers via computer graphics and digital image processing. In fact, the use of digital imagery to create forgeries is one of the biggest problems emerging from the technology. However, experts working together with law enforcement are devising systems that employ advanced algorithms in order to ferret out the forgeries [1, 2]. What may be surprising to those not working in the field is that very few digital documents today (especially those produced from medical, legal and government sources) are entirely free of some aspect of forgery. Detecting forgery algorithms is possible but depends almost entirely on the image source. Digital photographs and documents are easily changed to suit the purposes of the user, with copy-move being the most popular approach to forgeries [3]. It is considered a type of passive forgery [4, 5] and is very widespread. Figure 1 below shows some different kinds of common forgeries [6].

One classic approach to digital image forgery is enhancing. This is the easiest approach and also is considered the least violating (that is, has the lowest repercussion if the forger is caught). To counteract these forgeries, active and passive detection mechanisms have been developed. In the active approach, digital watermarking or signatures are employed to make documentation more concise and genuine [6, 4].

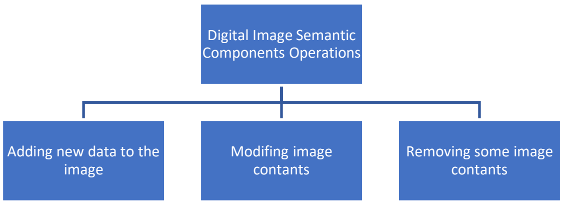
Digital Image Semantic Components Operations
Adding new data to the image
Modifing image contants
Removing some image contants

Fig. 1. Different types of forgeries.

The work is organized as follows. Following the introduction, we will provide an overview and revision of the algorithms used here. In the subsequent sections, we will delve deeper into the topics mentioned in the overview and also perform some tests to validate the methods.

2. Background

The history of forgery is as old as mankind. Throughout the centuries, it has primarily been used as a means to acquire access to power or money illegally [7]. Although this motivation persists, many cases of forgery today are focused instead on gaining access to systems for a variety of purposes. So, for instance, people engage in forgeries across fields as diverse as healthcare, surveillance, insurance, and even the media. To counteract forging activities, researchers are exploring algorithms as a means to detect image forgery. In the majority of the algorithms used thus far, lighting is analyzed to see whether or not copy-move forgery is present. During the forgery process, the image becomes "messy", and it is this "mess" that forgery detectors look for through the application of algorithms, as explained in [8]. The researchers in [8] also demonstrate how shadows can generate similar lighting artifacts within an image.

As touched on earlier, there are several different algorithm-based approaches for forgery detection, but the most popular techniques are block-based and feature-based. For block-based approaches, the detector needs access to the original image, whereas for feature-based strategies, the detector removes features by means of overlapping blocks that are typically used in the block-based approach. Several different kinds of characteristics can be input to the overlapping blocks (this will be explained in greater detail later in this work), and the matching among the boxes is performed on the basis of the feature-extraction strategy.

A. Type of Features

The present work involves three kinds of feature extraction, as follows: Fourier Mellin Transform (FMT), Zernike Moments (ZM), and Polar Cosine Transform (PCT). The latter two approaches are further subcategorized into "cartesian" and "polar" as in figure 2, respectively, and all three strategies are explained in detail below.

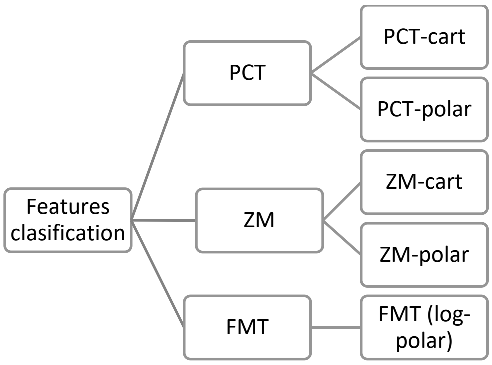

Fig. 2. Feature-extraction categories.

A.1 Fourier-Mellin Transform-based feature extraction.

Most of the currently employed copy-move forgery detection approaches that use a block-matching-based detection strategy utilize Fourier-Mellin Transform (FMT), as introduced in [9]. The FMT carries out radial projection for log-polar Fourier transformation in image blocks, as stated below:

a- Find the block's translation invariant $i(x,y)$. This can be done by using Fourier transformation representation.

$$|I'(f_x,f_y)| = |\sigma|^{-2}\left|I'(\sigma^{-1}((f_x\cos\alpha, f_y\sin\alpha),(-f_x\sin\alpha, f_y\cos\alpha))\right| \quad (1)$$

b- Input, via the resampling method, all results of magnitude values in log-polar coordinates.

$$|I'(\rho,\theta)| = |\sigma|^{-2}|I(\rho-\log\sigma),\theta-\alpha| \quad (2)$$

c- Use the log-polar values in 1-D to get $\theta = 45$ features via quantization the values (added together) in other forms of θ.

$$g(\theta) = \sum_i \log(|I(\rho_j,\theta|) \quad (3)$$

This approach performs best when detecting forgeries in flat regions.

A.2 Zernike Moment Transformation.

The Zernike moments method is generally applied in image recognition (i.e., to obtain image orientation, size, etc.). Therefore, as shown in [10], this approach is essentially an extinction of geometric moments as well as a description of their connection. The Zernike approach is written thus:

$$V_{nm}(\rho,\theta) = R_{nm}(\rho)e^{jm\theta} \quad for\ \rho \le 1 \quad (4)$$

Where n, m are the order and the rotation respectively. $R_{nm}(\rho)$ is the radial polynomial, and it can be given as:

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

The two-dimensional ZM for continuous image function $f(\rho,\theta)$ can be described as:

$$Z_{nm} = \frac{n+1}{\pi}\int_0^{2\pi}\int_0^1 f(\rho,\theta)V_{nm}^*(\rho,\theta)\rho d\rho d\theta \quad (6)$$

$$= \frac{n+1}{\pi}\int_0^{2\pi} e^{-jm\theta}\int_0^1 f(\rho,\theta)R_{nm}(\rho)\rho d\rho d\theta \quad (7)$$

In the digital image form in 2-D the ZM will be as:

$$Z_{nm} = \frac{n+1}{2}\sum_{(\rho,\theta)\in unit\ disk}\sum f(\rho,\theta)V_{nm}^*(\rho,\theta) \quad (8)$$

An important feature of the Zernike moment is that it is rotation invariant. This characteristic is used to find out whether or not the forgery has been rotated. There are many studies that use the Zernike moment for forgery detection [11, 12, 13].

A.3 Polar Cosine Transform

The Polar cosine transform (PCT) is a fast algorithm that is well-known for its speed, which makes it a good candidate for dealing with larger images as well as real-time application. PCT can simulate 2-D image patterns from a 2-D image $f(x,y)$ via changing it (transformation) to polar form from cartesian $f(r,\theta)$, where r indicates reduction and θ signifies the azimuth.

$$r = \sqrt{x^2+y^2} \quad (9)$$

$$\theta = \arctan\frac{y}{x} \quad (10)$$

The polar form can be written as:

$$f(r,\theta) = \sum_{n=1}^{\infty}\sum_{l=1}^{\infty} M_{nl}^c H_{nl}^c(r,\theta) \quad (11)$$

Where $r \le 1$.

$$M_{nl}^c = \Omega_n\int_0^{2\pi}\int_0^1 f(r,\theta)H_{nl}^{c*}(r,\theta) \quad (12)$$

$$H^c_{nl}(r,\theta) = R^c_n(r)e^{iln} \tag{13}$$

$$R^c_n(r) = \cos(\pi n r^2) \tag{14}$$

$$\Omega_n = \begin{cases} \frac{1}{\pi} & if\ n = 0 \\ \frac{2}{\pi} & if\ n \neq 0 \end{cases} \tag{15}$$

As PCT occurs at the unit circle, a total of three trigonometric functions are used to create a Kernel coefficient [14].

B. Feature extraction

As mentioned previously, there are several kinds of features available in published work and online. They all suggest the efficacy of one or more approaches for the detection of copy-move forgery, but this present work only looks into 3 main classifications of features, namely: the Fourier-Mellin transform (FMT), the Zernike moments (ZM), and the polar cosine transforms (PCT). The features in all 3 of these approaches share highly similar circular harmonic transform expansions (CHT) [15]. Therefore, we can measure the CHT coefficient through image projection $I(\rho,\theta)$ using the basis function of $K_{n,m}(\rho,\theta)$ to effect the transformation:

$$F_I(n,m) = \int_0^{\infty} \rho R^*_{n,m}(\rho) \times [\frac{1}{\sqrt{2\pi}} \int_0^{2\pi} I(\rho,\theta) e^{-jm\theta} d\theta] d\rho \tag{16}$$

As can be seen, image $I(\rho,\theta)$ appears in the polar scheme, with $\rho \in [0,\infty]$, $\theta \in [0,2\pi]$. This particular approach entails combining aspects of 2 formulations: 1. integrating the Zernike radial, function and the ρ value integration; and, in brackets, indicating the Fourier series function for image $I(\rho,\theta)$ together with phase term $e^{-jm\theta}$ with rotation of θ radians. Thus, to obtain rotation invariance, we simply use coefficient magnitude, such that FMT's coefficient absolute value will then give scale invariance, as any alterations in image scale adds to the phase term [16]. Hence, radial function is then variant-based according to feature designation. Therefore, we can assert that PCT radial function acts as a cosine function arguing ρ^2 while normalizing coefficients C_n.

$$R_n(\rho) = C_n \cos(n\pi\rho^2) \tag{17}$$

In this case, the Zernike radial function demonstrates the identical radial function of PCT, but includes coefficient values that are more apt and uses the formulation $\rho \in [0,1]$ in both functions. This is formulated as follows:

$$R_{n,m}(\rho) = \sum_{h=0}^{(n-|m|)/2} C_{n,m,h}\rho^{2-2h} \tag{18}$$

At the same time, we can show the FMT radial function as non-zero in $\rho \geq 0$, using a continuous value r above the argument value of ρ^2:

$$R_r(\rho) = \frac{1}{\rho^2} e^{jr\ln(\rho)} \tag{19}$$

It is worth noting that the models mentioned above can be used in a patch size with good resolution. So, in order to obtain achieve good matching with features from both patches, the extension on the feature length must remain lax (that is, in only a loosely extended state). Furthermore, we will apply sampling from cartesian and polar for ZM and PCT, respectively, whereas FMT will employ log-polar sampling. In this work, however, we will use polar sampling only to compute scaling and rotation in order to obtain the optimized invariance angle as well as scalar values [17].

C. Evaluating Performance

We will estimate both the accuracy and time requirements of the detection / localization forgery performance by finding the F-measure. In order to designate F-measure, we first must find which is true positive (TP), false positive (FP), false negative (FN) and true negative (TN). The IEEE F-measure can be written thus:

$$F = \frac{2|TP|}{2|TP| + |FP| + |FN|} \tag{20}$$

Therefore, if the ground truth and detection map occur simultaneously or act the same way, then both FN and FP are zero and the F-measure is normalized, such that $F = 1$. Here, we can find the F-measure for two levels (i.e., pixel and image levels). The pixel level is suitable for localization forgery for identical images [17].

D. F-measure Procedure

The F-measure standing (i.e., score) within the IEEE designation is determined by a procedure which determines the true condition for negative and positive conditions. This must have in it both pixel- and image-level images, as we mentioned earlier. Table 1 below categorizes all conditions according to the scoring outcome, while the figure 3, illustrate the PDF curve of the predictive condition.

Table 1. Shows the predictive conditions

Predictive Conditions			
Predictive Positive		Predictive Negative	
TP	$TPR = \frac{TP}{\sum condition\ positive}$	FN	$FNR = \frac{FN}{\sum condition\ positive}$
FP	$FPR = \frac{FP}{\sum condition\ negative}$	TN	$TNR = \frac{TN}{\sum condition\ negative}$

The accuracy of any approach depends on the all area under the PDF curve. Based on that, we can write the equation as following:

$$Acc = \frac{TP + TN}{P + N} = \frac{TP + TN}{TP + TN + FP + FN} \tag{21}$$

In brief, true positive shows the highest-output standings regarding accuracy in detecting forged images, and true negative shows zero-output tallies featuring zero scores. This indicates that the approach has in fact detected zero evidence of forgery. Conversely, false negative and false positive indicate, respectively, a non-detected forged image and an image which was assumed false, but the assumption was inaccurate. For CMFD, the output can indicate a pure image mask or a forgery. Conversely, the ground root mask presents as a binary mask (0, 1) which can be created by hand to signify the region copies as well as removing the high-value image elsewhere within the same shot (groundroot==max). In this instance, the remaining mask is considered low value (groundroot==0). Once the condition values are obtained, we can verify the process, assuming that the CMFD output / ground root constitute genuine inputs. In the initial test, we can make both inputs the same in order to obtain a valid F-measure score. Next, we can apply various inputs to achieve a range of F-measures depending on the predicted condition values. Figures 3 and 4 indicate F-measure results from the inputs. In this work, the "ideal" value for F-measure will be the outcome of an ideal matching of the ground root mask (GT) and the output mask of forgery detection function. In so doing, outliers of CMFD will likely lead to low F-measure and thus limit the validity of the system.

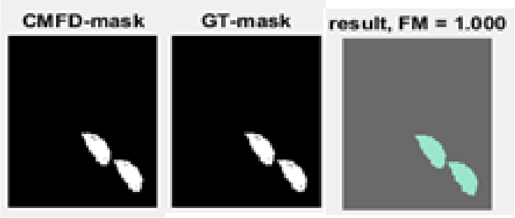

Fig. 3. If the CMFD mask and the GT mask are the same, the F-measure is considered ideal.

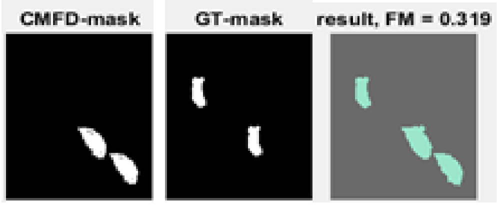

Fig. 4. If the CMFD and GT masks turn variant, the F-measure is invalidated.

3. USING THE Patch-Matching Approach ON Copy-move Forgery Detection

A PatchMatching algorithm is faster than most other algorithms and uses a matching approach that applies dense approximation field matching. The primary reason for choosing this approach over others is its fast propagation in offset fields. Iterations are performed by performing a randomized search or by doing full-image scanning (propagation). Generally, in a scan, we can first choose a specific vector $f(s)$, that utilizes an s pixel for its patch center. Because the features essentially characterize the patch, the distance between and among the features need to be carefully and accurately measured. Figure 5 shows the main blocks of the algorithm in the processing sequence.

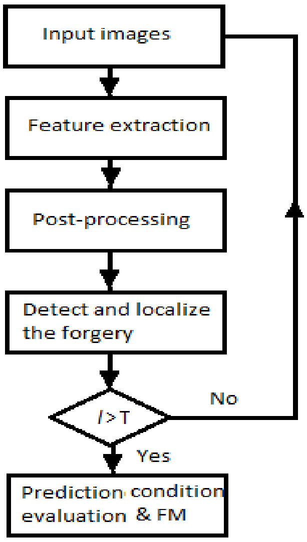
Input images
Feature extraction
Post-processing
Detect and localize the forgery
I>T
No
Yes
Prediction condition evaluation & FM

Fig. 5. PatchMatching-based copy-move forgery detection algorithm.

4. Post-Processing using Denes Liner Fitting

Comparison of images, along with matching and stitching, is more or less based on feature matching. To create an offset field, the PatchMatch algorithm employs matching and a feature search using offset points and generates the offset field. In this system, a linear offset will formulate an accurate offset field on top of the copy-move region. Referred to as "propagation", this step might require several iterations. Dense-field matching strategies enhance the efficacy of the strategy and thus have already been the choice of many scholars, as shown in [18, 19, 20, 17]. Yet, despite the method's popularity, this type of image can suffer from geometric deformation, compression, the noise effect, and illumination fluctuations, compression, and geometric deformation. When this occurs, the offset field is significantly less successful at feature-matching.

In the post-processing stage, the objective is to remove or at least mitigate all negative impacts on the image. To achieve this aim, it is important to regularize offset fields and thereby heighten the opportunity to enhance the detection of copy-move and decrease false alarms. To be viable, offset fields must be able to fit all neighborhood pixels of s through a liner model, after which a transformation sets parameters to obtain the sum of square error (SSE).

$$\delta^{`}(s_i) = As_i \tag{22}$$

$$\epsilon^2(s) = \sum_{i=1}^{N} \left\| \delta(s_i) - \delta^{`}(s_i) \right\|^2 \tag{23}$$

In the post-processing strategy, a number of steps need to be adhered to for the tests to be valid: 1) filtering median material using a circular window with a radius of ρ_M; 2) computing fitting errors, $\epsilon^2(s)$, w.r.t. using a least-squares linear model over a circular neighborhood of radius ρ_N; 3) bringing $\epsilon^2(s)$ to level T_ϵ^2 ; 4) deleting regional couples that are actually closer positioned than T_{D2} pixels; 5) deleting of all regions not larger than T_S pixels; 6) mirroring the regions;

and 7) morphological dilation of the elements using a circular structuring element featuring a radius of $\rho_D = \rho_M + \rho_N$. If we choose to use these clearly defined stages, our first step is to get rid of all outliers from the image using a median filter. In fact, not until all of the outliers have been deleted or demoted will the minimum mean square fitting be used. Pictures and other images that exhibit repeating patterns, including monochrome, can be extremely problematic because their identical or near-identical details can lead to mismatching entire areas. To overcome this problem, we use the thresholds T_ϵ^2 , T_{D2}, and T_S, whose usage is indicated in steps 3, 4, 5. So, if a copy-move pixel is suspected, s, for a particular area, the mirrored pixel "twin" in $s + \delta(s)$ is designated as a copy-move pixel. The final stage will view morphological effects as an outcome of immediately preceding steps.

5. Experiment Result

The proposed algorithm was able to resolve all the issues presented above and successfully apply the most apt forgery detection method for detecting copy-move and localizing it. Figure 6 provides a summation of the details.

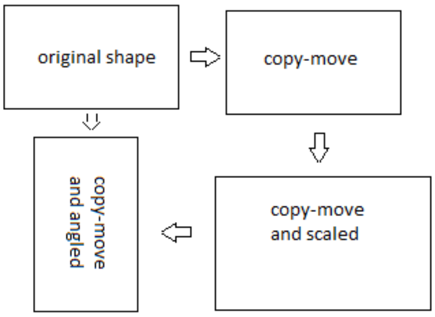

Fig. 6. Copy-move that can be detected.

As shown, there are situations when the process will be less efficient, especially if the image contains too many vivid colors, no colors, or is in black and white. Overall, the detector process requires the use of a variety of images and datasets, including the Loughborough University dataset[1] and the GRIP database[2].

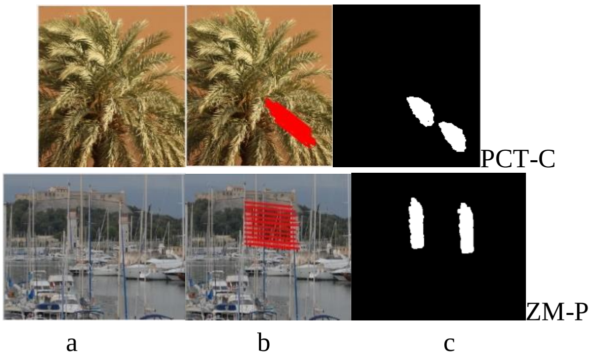

Fig. 7. Searching for forged images in the GRIP dataset: (a) forged image, (b) offset points, (c) localization copy-move forgery mask.

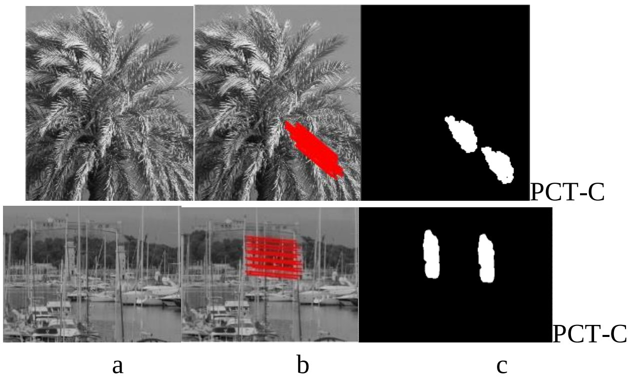

Fig. 8. Searching for forgery in a gray image: (a) forged image, (b) offset points, (c) localization copy-move forgery mask.

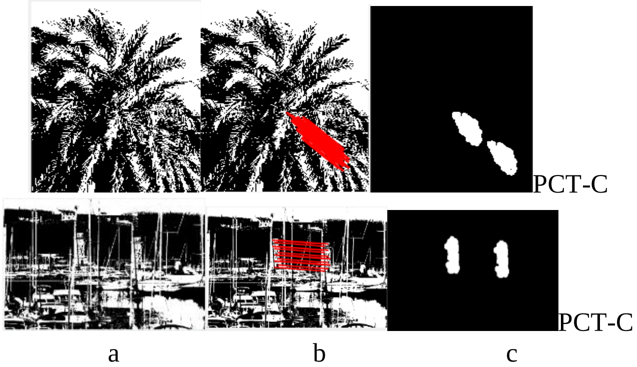

Fig. 9. Searching for forgery in black and white image: (a) forged image, (b) offset points, (c) localization copy-move forgery mask.

In searching the three instances given in Figures. 7 to 9, we see several different offset points and also notice the reduction in efficiency when there are fewer colors. Moreover, when presented from exceedingly "flat" viewpoints, changing image formatting to BW from RGB could lead to even further reductions in features, which means that the forgery, if present, might not be viewable with the tools provided.

Table 2. FM Parameters of Image as Given by the Proposed Method vs. Some Literature

	PRNU	PatchMatch
TP	67619	79201
TN	700375	635571
FP	2775	67579
FN	15663	4081
Acc	0.977	0.9088
FM	0.88	0.6885

In order objectively evaluate the usefulness and applicability of the methods, we decided to apply the identical function as outlined by researchers in [21, 17]. In examining Table 1, however, it becomes clear that the conditions are different. However, at the end they gave very close FM value. The algorithm was examined on many different images. The difference of the FM in these experiments is negligible. Tables 3 and 4 show some results of these experiments. In fact, table 2 shows inclusive comparison of the algorithm with literature, and in this table, it shows clearly that the FM of the proposed algorithm is 0.2 higher than photo response non-uniformity PRNU.

[1] http://www.grip.unina.it

[2] http://homepages.lboro.ac.uk/ cogs/datasets/ucid/ucid.html

6. Conclusion and Future Work

To conclude, copy-move forgery detection (CMFD) had been widely adopted for use by people of all skill levels, due mainly to its user-friendly and ease-of-use approach. However, despite the relative simplicity of the strategy, there are still some challenges that go along with it that make the outcome sometimes invalid or at least questionable. On the whole, there is a main issue affecting most CMFD algorithms. If a copy-move is performed by applying something in the image background to obscure evidence of forgery, but this can be overcome by employing PatchMatching on the forged images' offset points. In this situation, the authentic image is needed to proceed with forgery detection, so different method should be adopted. Our experiments indicate the presence of variance within the evaluations, which occurs also in identical images where there are alterations to the resolution or color, giving unequal F-scores. Despite these slight problems, the F-score generally exhibits optimal efficiency in the enhanced approach. In future studies, we would use the identical idea to test for forgeries in videos and include studies from the literature to evaluate F-score results.

7. Acknowledgement

This work is funded by the ministry of higher education of Libyan Government, which managed by CBIE in Canada. The authors acknowledged Mr. T. Iqbal, who make most of the help and reviews to make this work existed.

Author's Contributions

The authors confirm that the manuscript has been read and approved by all authors and that there are no other persons who satisfied the criteria for authorship but are not listed.

Conflict of Interest

The authors declare that there is no actual or potential conflict of interest regarding the publication of this article.

Table 3. The evaluation values for detecting CMFD in two different RGB images shown in Fig. 7

Image	FM	TPR	TNR	FNR	FPR	PPV	NPV	TFE	TPM	TPP
1.	0.999	0.9958	0.9995	0.0042	0.0005	0.9862	0.999	1.292	12.235	1.465
2.	0.9992	0.9987	1.0000	0.0013	0.00001	0.9997	1.0000	1.945	10.179	1.687
3.	0.9727	0.9972	0.9977	0.0028	0.0023	0.9493	0.999	1.912	10.871	1.703
4.	0.5633	0.7210	0.9683	0.2790	0.0317	0.4622	0.9892	1.892	11.131	1.753

Table 4. The evaluation values for detecting CMFD to same image in assorted color format.

	FM	TPR	TNR	FNR	FPR	PPV	NPV	TFE	TPM	TPP
PCT-BW	0.9896	0.9905	0.9996	0.0095	0.0004	0.9888	0.9997	1.230	8.765	1.579
PCT-RGB	0.999	0.9958	0.9995	0.0042	0.0005	0.9862	0.999	1.292	12.235	1.465
ZM-Gray	0.9802	0.9733	0.9996	0.0267	0.00049	0.9873	0.9990	2.060	11.657	1.790

8. References

[1] V. A. a. V. Mane, "Reflection SIFT for Improving the Detection of Copy-Move Image Forgery," *ICRCICN*, pp. 84 - 88, 2016.

[2] R. V. D. V. M. T. Anil Dada Warbhe, "Block Based Image Forgery Detection Techniques," *International journal of engineering science and research technology*, pp. 289 - 297, 2015.

[3] a. V. H. M. Gajanan K. Bitajdar, "Dgigtal image forgery detection using passive techniques: A survey," *Digital Investigation 10 (2013), Elsevier*, pp. 226 - 245, 2013.

[4] K. B. Al-Qershi OM, "Passive detection of copy-move forgery in digital images: state-of-the-art.," *Forensic Sci Int.*, pp. 1-3, 2013.

[5] a. N. S. Pravin Kakar, "Exposing Postprocessed Copy–Paste Forgeries Through Transform-Invariant Features," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 3, pp. 1018-1028, 2012.

[6] A. Rizvi, "Digital Image Forgery Detection," Lincoln University , A New Zealand, 2015.

[7] V. M. Vanita Agarwal, "Reflective SIFT for Improveing the Detection of Copy-Move Image Forgery," *Second International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN)*, pp. 84-88, 2016.

[8] E. T. a. M. B. Ira Tuba, "Digital Image Forgery Detection Based on Shadow Texture Feature," *Telecommunications Forum (TELFOR), 2016 24th* , pp. 22-23 .

[9] H. T. S. a. N. M. Sevinc Bayram, "An efficient and robust method for detecting copy-move forgery," *Proc. IEEE CASSP*, pp. 1053-1056, 2009.

[10] M. Teague', "Image analysis via the general theory of

moments," *Journal of the Optical Society of America,* vol. 70, no. 8, pp. 920-930, 1980.

[11] M.-J. L. a. H.-K. L. Seung-Jin Ryu, "Detection of Copy-Rotate-Move Forgery Using Zernike Moments," *LNCS 6387, Springer Verlag Berlin Heidelberg,* p. 51–65, 2010.

[12] S. X. L. a. M. Pawlak, "On the Accuracy of Zernike Moments for Image Analysis," *IEEE Transactions on Pattern Analysis and Machine Intelligence,* vol. 20, no. 12, pp. 1358-1364, 1988.

[13] MiaoZhenjiang, "Zernike moment-based image shape analysis and its application," *ELSEVIER Jornal ,* vol. 21, no. 2, pp. 169-177, 2000.

[14] a. S. K. Zhuo Yang, "Fast Polar Cosine Transform for Image Description," *MVA2011 IAPR Conference on Machine Vision Applications, Nara, JAPAN,* pp. 320-323, 2011.

[15] H. H. A. a. G. A. Yuan-Neng Hsu, "Rotation-invariant digital pattern recognition using circular harmonic expansion," *OSA Publishing,* vol. 21, no. 22, pp. 4012-4015, 1982.

[16] M. K. M.-J. L. a. H.-K. L. Seung-Jin Ryu, "RotationInvariantLocalizationofDuplicatedImage Regions Based on Zernike Moments," *IEEE Transactions on Information Forensics and Security,* vol. 8, no. 8, pp. 1355-1370, 2013.

[17] G. P. a. L. V. Davide Cozzolino, "Efficient Dense-Field Copy–Move Forgery Detection," *IEEE Transactions on Information Forensics and Security,* vol. 10, no. 11, pp. 2284-2297, 2015.

[18] S. K. a. S. Avidan, "CoherencySensitiveHashing," *in Proc. Int. Conf. Comput. Vis.,* p. 1607–1614, 2011.

[19] I. O. a. S. Avidan, "TreeCANN - k-d tree Coherence Approximate Nearest Neighbor algorithm," *Proc. 12th Eur. Conf. Comput. Vis,* p. 602–615, 2012.

[20] D. C. G. P. a. L. V. L. D’Amiano, "Video forgery detection and localization based on 3d patchmatch," *Multimedia & Expo Workshops (ICMEW), 2015 IEEE International Conference on,* pp. 1-6, 2015.

[21] G. P. S. a. L. V. Giovanni Chierchia, "A Bayesian-MRF Approach for PRNU-Based Image Forgery Detection," *IEEE Transactions on Information Forensics and Security,* vol. 9, no. 4, pp. 554-567, 2014.

[22] F. J. a. G. M. Lukas J., "Digital camera identification from sensor pattern noise," *IEEE Transactions on Information Forensics and Security,* pp. 205-214, 2006.

[23] a. D. G. Stuart Geman, "Stochastic relaxation, Gibbs distributions, and the Bayesian restoration of images," *IEEE Transactions on Pattern Analysis and Machine Intelligence,* vol. 6, no. 6, p. 721–741, 1984.

[24] P. G. a. S. G. D'Elia C, "A tree-structured Markov random field model for Bayesian image segmentation," *IEEE Transactions on Image Processing,* vol. 12, no. 10, p. 1259–1273, 2003.

[25] J. Besag, "On the statistical analysis of dirty pictures," *Journal of the Royal Statistical Society, Series B 48,* p. 259–302, 1986.

Younis Abdalla Received his B.Sc. in 2002, Computer and Telecommunication engineering, Subha University, Libya. In 2007 received his M.Sc. Electronic and Telecommunication engineering, University Technology Malaysia UTM, Malaysia. Currently, a PhD student at Memorial University, Newfoundland, Canada. Department of Electrical and Computer Engineering. Faculty of Engineering and Applied Science. IEEE member.

M. Tariq Iqbal B.Sc. (UET, Lahore), M.Sc. (QAU, Islamabad), Ph.D. (Imperial College London), P. Eng. Now, Prof. in the Department of Electrical and Computer Engineering Faculty of Engineering and Applied Science Memorial University of Newfoundland St. John's, Newfoundland, Canada. Senior member in IEEE

M. Shehata B.Sc.(Zagazig University), 1996. M.Sc.(Zagazig University), 2001 Ph.D. (University of Calgary), 2005. Currently, Faculty of Engineering and Applied Science Memorial University of Newfoundland St. John's, Newfoundland, Canada. Professional Engineer Senior Member IEEE