Fusion Approaches System of Copy-Move Forgery Detection

Article · August 2018

CITATIONS
0

READS
244

3 authors, including:

Dnon Dnon
Memorial University of Newfoundland
11 PUBLICATIONS **2** CITATIONS
SEE PROFILE

Tariq Iqbal
Memorial University of Newfoundland
459 PUBLICATIONS **5,076** CITATIONS
SEE PROFILE

Fusion Approaches System of Copy-Move Forgery Detection

Younis E. Abdalla
Faculty of Engineering and applied science
Memorial University of Newfoundland
St. John's, Canada
yea764@mun.ca

M. T. Iqbal
Faculty of Engineering and applied science
Memorial University of Newfoundland
St. John's, Canada
tariq@mun.ca

M. Shehata
Faculty of Engineering and applied science
Memorial University of Newfoundland
St. John's, Canada
mshehata@mun.ca

***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 a fusion approach to detect a copy-move forgery based on PatchMatch enhanced by the dense field technique, and sensor pattern noise based on photo response non-uniformity (PRNU). 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 both passive and active forgery detection.**

***Keywords* — Copy-move detection; localize the forgery; Present Image; Image forgery; Features; Score Evaluation.**

I. Introduction

The software and hardware technologies reduce the gap between the professional people and the amateurs in different fields. Digital image processing, computer graphics and computer vision have some advantages and disadvantages of the use of the technology. Forgery is one of the challenging issues of digital image processing in recent decades. As a result of using a new algorithms and investigation techniques it becomes possible to detect the forgery [1, 2]. However, there is no guaranty that all the digital documents, especially in medical, curt and academic journals, will be free of forgery. There are many digital copies and photographs were detected as altered and manipulated publication. Addressing this type of alternation and forgery will make the publication more authenticated [3]. The is a different type of forgery techniques. However, the copy-move the common used forgery for the digital documents and images. The detection of forgery algorithm will depend on the image source. The copy-move, in practice, is a technique to manipulate the digital documents and images where a part of that document copied and pasted again over different part of the same document. This type of forgery is classified as a passive forgery [4, 5] which, in fact, the most common forgery technique is used for digital documents and images forensics. Nevertheless, adding and/or removing some data to the image or documents is indeed other types of widely used in the forgery activities. Figure 1 classify the common type of forgery.

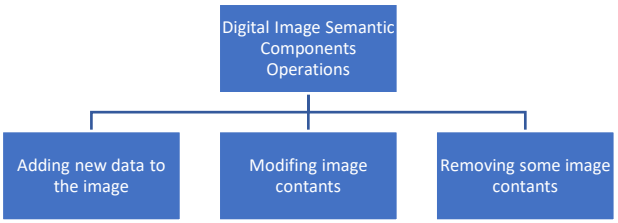


Fig. 1. Some common forgery classifications.

Digital image forgery can be very varying between the enhancement, which in the most cases is accepted or free of risk to the other types which more dangerous. Figure 1 shows the forgery types classification [6]. However, image forgery detection mechanisms can be classified to two major categories of methods: active and passive methods. The active method can be presented by either by digital signature or digital watermarking [6, 4]. These mechanisms are serving same objectives; For instance, concise documentations, robustness of image processing field, and make the professional authenticate research works more exist and eliminate the fake works.

The forgery detectors, basically, share same fundamentals to detect the forgery which is the image information, either that information is included or attached. For example, the color image filter used to enhance the image, the used acquisition phase, or the camera lens characteristics. All this information can be detected professionally by using photo-response non-uniformity noise sensor (PRNU), and indeed it is a powerful algorithm to detect the copy-move forgery, and it is unique for each camera [4]. As there are more many other powerful algorithms to detect the copy-move forgery, in fact, all these algorithms have three main processes which are: feature extraction, matching and post-process at a pixel's level to reduce the false alarms. Scale and rotation invariant feature selection is important to provide the robustness. The PatchMatching offset field will implement more efficient and smoothness of detecting copy-move forgery. In order to speed the matching of the offset

points, the PatchMatching algorithm in this work, runs Denesfield to find the nearest neighbor field (NN) as follows.

$$\delta(s) = \arg \ \ min_{\emptyset: s+\emptyset \in \Omega, \emptyset \neq 0} D\big(f(s), f(s+\emptyset)\big) \quad (1)$$

$$NN \ \cong \ s' = s + \ \delta(s) \quad (2)$$

Where s is the pixel in the neighborhood field Ω. $\delta(s)$ is the offset field.

In the following, after the general introduction, the next section will revise the principles of the used algorithms. The following sections will expand the discussion to provide more details about the proposed algorithm and some conducted experiments.

II. Back Ground

Forgery activities started in early 1840s [7] and become a tool which can harm many people and miss used different systems. For example, criminal investigation system, surveillance camera systems, insurance application, medical images, and publication and journalism corporation. Therefore, this fact encourages many researchers to propose different algorithms to detect forgery, in the other words, reduce the risk of these activities. Copy-move forgery got high intention from research as groups and individuals result to produce and propose many algorithms to detect and localize this type of forgery. Detecting the forgery in most of these algorithms is based on lighting analyzing. To make the image looks as pristine, after the tampering done with that image, the light should be reconciled and this is a big challenge. Therefore, forgery detection algorithms can analyze this issue and can detect it [8]. the same study [8] shows that, the shadow makes same light effect on the image. Indeed, there are techniques to achieve better forgery detection.

The detection techniques are varied. However, the main two categories are feature based and block based. The block based technique requires the original image. While the feature based technique extract the features though the overlapping blocks which are applied in the block technique. There are diverse types of features, as we will explain later, which can be computed over all overlapping blocks. The matching between these box's will be done based on feature extraction process.

A. Type of Features

In this study, we included three types based features extractions: Polar Cosine Transform (PCT), Zernike Moments (ZM), and Fourier Mellin Transform (FMT). For the first two types, will be having two distinct categories: polar and cartesian.

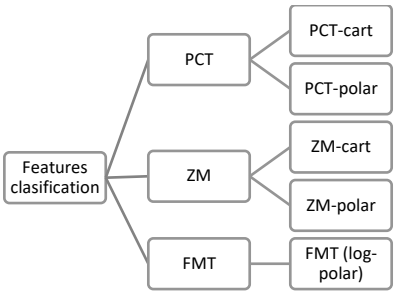


Fig. 2. The feature classification

1- Polar Cosine Transform.

Polar cosine transforms (PCT) is fast algorithm which suits more for large images and real-time application, and it was proposed to represent the pattern of 2-D image $f(x,y)$ by transforming it from cartesian to polar form $f(r,\theta)$, where r is the reduce and θ is the azimuth.

$$r = \sqrt{x^2 + y^2} \quad (3)$$

$$\theta = \arctan\frac{y}{x} \quad (4)$$

The polar form will be fond as:

$$f(r,\theta) = \sum_{n=1}^{\infty}\sum_{l=1}^{\infty} M_{nl}^{c} H_{nl}^{c}(r,\theta) \quad (5)$$

Where $r \ \leq 1$.

$$M_{nl}^{c} = \Omega_n \int_0^{2\pi}\int_0^{1} f(r,\theta) H_{nl}^{c*}(r,\theta) \quad (6)$$

$$H_{nl}^{c}(r,\theta) = R_n^{c}(r) e^{iln} \quad (7)$$

$$R_n^{c}(r) = \cos(\pi n r^2) \quad (8)$$

$$\Omega_n = \begin{cases} \frac{1}{\pi} & if \ n = 0 \\ \frac{2}{\pi} & if \ n \neq 0 \end{cases} \quad (9)$$

The PCT will be defined on the unit circle, and to generate the Kernel coefficient for each point, three trigonometric functions [9].

2- Zernike Moments Transformation.

Zernike moments are used for image recognition and find an image orientation, size and position. So, it is basically an extinction of geometric moments and [10] describe the relationship between them. The Zernike function can be presented as follows:

$$V_{nm}(\rho,\theta) = R_{nm}(\rho) e^{jm\theta} \quad for \ \rho \leq 1 \quad (10)$$

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

$$R_{nm}(\rho) = \sum_{x=0}^{(n-|m|)/2} (-1)^x \frac{(n-x)!}{x!\left(\frac{n+|m|}{2}-x\right)!\left(\frac{n-|m|}{2}\right)!} \rho^{n-2x} \quad (11)$$

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

$$Z_{nm} = \frac{n+1}{\pi} \int_0^{2\pi} \int_0^1 f(\rho,\theta) V_{nm}^*(\rho,\theta) \rho d\rho d\theta \quad (12)$$

$$= \frac{n+1}{\pi} \int_0^{2\pi} e^{-jm\theta} \int_0^1 f(\rho,\theta) R_{nm}(\rho) \rho d\rho d\theta \quad (13)$$

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

$$Z_{nm} = \frac{n+1}{2} \sum_{(\rho,\theta)\in unit\ disk} \sum f(\rho,\theta) V_{nm}^*(\rho,\theta) \quad (14)$$

The Zernike moment is rotation invariant, this helps to detect the rotated forgery. Therefore, the literature shows many algorithms use the Zernike moment to detect the forgery [11, 12, 13].

3- Fourier-Mellin Transform based feature extraction.

The recent efficient block-matching based copy-move forgery detection approaches are using Fourier-Mellin Transform (FMT) which was proposed by [14]. In fact, this method performs radial projection on the log-polar organize Fourier transformation of image blocks as following:

a- Obtain translation invariant for each block $i(x,y)$ by applying Fourier transformation representation.

$$|I'(f_x,f_y)| = |\sigma|^{-2} |I'(\sigma^{-1}((f_x \cos\alpha, f_y \sin\alpha), (-f_x \sin\alpha, f_y \cos\alpha))| \quad (15)$$

b- Resample the magnitude values result into log-polar coordinates.

$$|I'(\rho,\theta)| = |\sigma|^{-2} |I(\rho - \log\sigma), \theta - \alpha| \quad (16)$$

c- Project log-polar values onto 1-D, and obtain $\theta = 45$ features by quantization these summed values for different θ.

$$g(\theta) = \sum_i \log(|I(\rho_j,\theta|) \quad (17)$$

The FMT achieve high performance in forgery detection of flat regions.

B. Feature extraction

There are many types of features in the literature, which have been proposed for copy-move forgery detection. However, this work considered only the three types of features which mentioned above: the polar cosine transforms (PCT), Zernike moments (ZM), and the Fourier-Mellin transform (FMT). These features have same circular harmonic transforms expansions (CHT) [15]. The coefficient of the CHT can be estimated by projecting the image $I(\rho,\theta)$ over the basis function $K_{n,m}(\rho,\theta)$ of transforming

$$F_I(n,m) = \int_0^\infty \rho R_{n,m}^*(\rho) \times [\frac{1}{\sqrt{2\pi}} \int_0^{2\pi} I(\rho,\theta) e^{-jm\theta} d\theta] d\rho \quad (18)$$

The image $I(\rho,\theta)$ in the polar form, where $\rho \in [0,\infty]$, $\theta \in [0,2\pi]$. The above function shows a combination from two equations. The first part represents the integration of Zernike radial, function (11), with integration of ρ value. While the second part between the brackets, show the Fourier series function of the image $I(\rho,\theta)$ with the phase term $e^{-jm\theta}$ by rotation of θ radians. Therefore, achieving the rotation invariance is by applying the coefficient magnitude. Indeed, the absolute value of the FMT coefficient will obtain scale invariance since the change of image scale will only contribute the phase term [16]. The radial function will be variant based on the feature type. The PCT radial function is a cosine function with the argument of ρ^2 and normalize the coefficients C_n.

$$R_n(\rho) = C_n \cos(n\pi\rho^2) \quad (19)$$

The Zernike radial function shows same PCT radial function with more appropriate coefficient values and for both functions $\rho \in [0,1]$, and is written as

$$R_{n,m}(\rho) = \sum_{h=0}^{(n-|m|)/2} C_{n,m,h} \rho^{2-2h} \quad (20)$$

On the other hand, the radial function of FMT are non-zero function for $\rho \geq 0$, with continuous value r over the argument value ρ^2 as follows

$$R_r(\rho) = \frac{1}{\rho^2} e^{jr \ln(\rho)} \quad (21)$$

These models will be applied to predefined patch size, which neither too small nor too large for decent resolution. To achieve good matching between the features in both patches, the feature length should not be well extended. The both sampling will be used, the cartesian sampling and the polar sampling for the PCT and ZM, while the FMT uses the log-polar sampling. However, computing the rotation and scaling will be only on polar sampling to insure the perfected invariance angle and scalar values [17].

C. Performance Evaluation Task

Detection and localization forgery performance will be declared by estimate the accuracy and time conception to full processing duty. This matter would be tackled by measuring the F-measure. To indicate the F-measure we need to determine all false positive FP, true positive TP, false negative FN and true negative TN. The IEEE F-measure is defined as:

$$F = \frac{2|TP|}{2|TP| + |FP| + |FN|} \quad (22)$$

When the detection map and ground truth are happening at the same time or behaving in an exact manner, then false negative FN and false positive FP will equal to zero, also, the F-measure will be normalized, means $F = 1$. F-measure is obtained in two levels: image level and pixel level. In the image level to detect if there is a forgery or not, while the pixel level is used to localize the forgery in the same image [17].
The accuracy of any approach is depending on the true positive rate (TPR) and false positive rate (FPR).

$$Acc = \frac{TPR + (1 - FPR)}{2} \quad (23)$$

D. F-measure Procedure

F-measure score as an IEEE stander is based on the true condition in both positive and negative conditions. This procedure includes image level and pixel level measures as mentioned above. Table 1. classifies the all predicted conditions based on the scores collected.

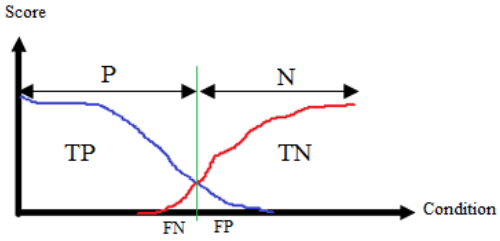


Fig. 3.....

True positive will display all the high output scores which present the number of correct detected forged image, while true negative will display the non-output scores with zero scores, means correctly detected pristine image. The false positive and false negative will be the other scores out of AND operation to present wrongly detected pristine image and non-detected forged image respectively.

```
TP = sum of detected forged features with
groundroot==max;
TN = sum of detected no forged features with
groundroot==0);
FP = sum (of detected forged features with
groundroot==0);
FN = sum of detected no forged features with
groundroot==max);
```

The output of CMFD shows either forged or pristine image mask. On the other hand, the ground root mask is a binary mask (0, 1). It is manually designed to designate the copied region and the relocation of that region in the same image with high value (groundroot==max), and the rest of the mask will be labeled with low value (groundroot==0). The F-measure score will be measured after getting all the predicted condition values. To test the procedure, we presume the CMFD output and the ground root as an actual input for this enquiry. The first test, both inputs will be same mask to get the ideal a F-measure score. After that, we used different inputs to get different F-measure based on the predicted condition values. The figures (4, 5) show the result of F-measure with inputs. The ideal value of F-measure is one that will be result of a perfect matching between the output mask of forgery detection function (CMFD) with the ground root mask (GT). Therefore, the outlier of CMFD will cause low F-measure, and reduce the accuracy of the system.

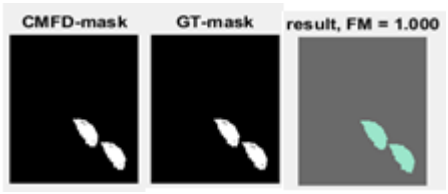


Fig. 4. When the CMFD mask is identical with the GT mask the F-measure will be ideal

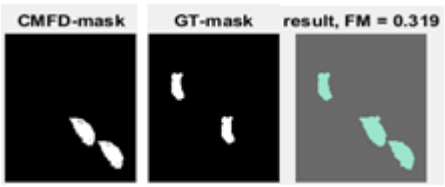


Fig. 5. The F-measure decries when the CMFD mask GT mask become variant

III. Copy-move Forgery Detection based on Patch-Matching Approach

The PatchMatch algorithm is fast and randomize algorithm based on dense approximation field matching technique. The main advantage of using this technique is to quicker propagation of all the offset fields. The iteration can be done either by applying full image scanning, which called a propagation, or by doing a random search. For any region scan, we specify a vector $f(s)$, which use a s pixel as patch center and consider all the pixels in sized patch. The features give a good description of the patch, therefor, the distance between these features should be well measured.

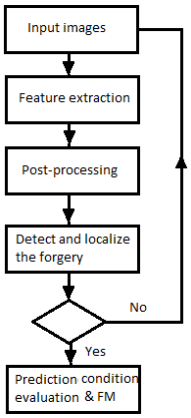


Fig. 6. Shows the Copy-move forgery detection algorithm based on PatchMatching

A. Post-Processing Based on Denes Liner Fitting

Feature matching is the key of most of image comparison, stitching and matching. A PatchMatch algorithm uses the feature

search and matching through the offset points and generate the offset field. The linear offset will perform a correct offset field over the copy-move region, and this propagation may take many iterations. Dense-field matching techniques widely used in [18, 19, 20, 17], which increases the efficiency. However, image mostly has some noise effect, illumination fluctuations, compression, and geometric deformation that make offset field failed to achieve good feature matching. Post-processing is to take off or reduce that mentioned effects on the image, Indeed, to regularize the offset field and increase the chance of detecting the copy-move and reduce the false alarms. The offset field should fit all the neighborhood pixels of s through a liner model, then use a transformation parameters to minimize the sum of square error (SSE).

$$\delta`(s_i) = As_i \tag{24}$$

$$\epsilon^2(s) = \sum_{i=1}^{N} \left\| \delta(s_i) - \delta`(s_i) \right\|^2 \tag{25}$$

The post-processing follows the next procedure: 1) median filtering on a circular window of radius ρ_M; 2) computation of the fitting error, $\epsilon^2(s)$, w.r.t. a least-squares linear model over a circular neighborhood of radiusρ_N; 3) thresholding of $\epsilon^2(s)$ at level T_ϵ^2 ; 4) removal of couples of the regions closer than T_{D2} pixels; 5) removal of the regions smaller than T_S pixels; 6) mirroring of detecting regions; 7) morphological dilation with a circular structuring element of radius $\rho_D = \rho_M + \rho_N$. Following the above steps, we start by the removing all outliers from the image by applying a median filter. The minimum mean square fitting error will be applied when all the outliers are removed. Images have repeated patterns or uniform background are highly challenged because they have similar details which make miss matching regions. To solve this issue, we apply different thresholds as T_ϵ^2 , T_{D2}, and T_S which explained the steps 3, 4, 5. When the copy-move pixel detected s, in specific region, same pixel in the mirrored region $s + \delta(s)$ will be marked as copy-move pixel. Last step will treat the morphological effects as a result of the previous steps.

IV. Sensor Pattern Noise Based Approach

This approach is used to approve the authenticity of the image based on sensor pattern noise or the camera signature. This can help to evaluate the truthfulness of an image by estimating the pattern noise of the same camera sensor. The noise pattern which be introduced by any type of cameras will be divided to two main types: A random noise pattern and fixed pattern noise. The random noise is changing from exposure to another. Fixed pattern noise is a Photo Response Non-Uniformity (PRNU). This produces as result of pixel light sensitivity, and this is very dependent noise. PRNU is kind of intrinsic property of all digital cameras [21].

The PRNU is stable and unique to each camera. Therefore, by calculating the correlation between the designated image with PRNU signal of the known camera, we can specify if that image was captured by that camera or wasn't. They will be obtained by using the correlated a specific PRNU pattern with the query image noise residual and apply it a specific a threshold, if the correlation value is less than the threshold the means the image wasn't captured by the known camera, otherwise the image was captured by the known camera. The next diagram shows the algorithm stapes.

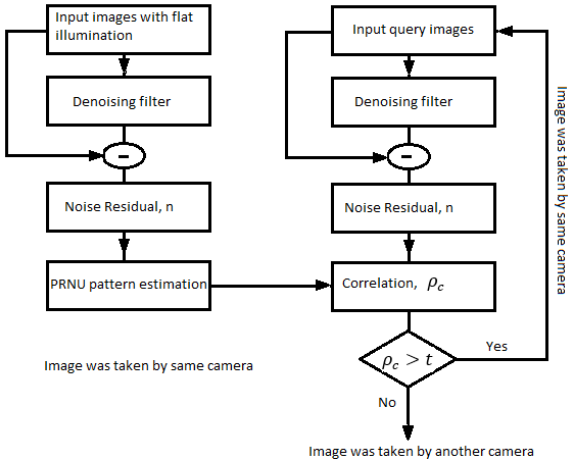


Fig.7. PRNU algorithm for forgery detection

According to the above diagram, it is obvious that the same process will be taken for both images, the original image and the query image, for the first three main steps ended by computed the noise residual for both images.

$$r = yk + n \tag{26}$$

The PRNU will be generated as a camera finger print. After that, normalized correlation will be computed to detect if there is any forgery was done on the image:

$$\rho_c = Corr\left(r_{w_c}\,,\ Z_{w_c}\right) \tag{27}$$

Where the $z = yk$, and this presented the PRNU value as $\{0, 1\}$. When the image is forged, then the values will by 0 to present the absence of PRNU, and one when the image is present. The final decision is based on the selective threshold t provided by a Neyman-Pearson approach [22].

V. Proposed Approach

The aims of forgery detection are to determine whether an image is pristine or forged. The literature shows that there are two main categories of the forgery detectors. The single approach and fusion approach. It is a dilemma to say which one is the best. However, we agree that integrating different forensic approaches will achieve better results. Indeed, has more universal input options. Therefore, we propose to integrate two forensic approaches. First, PatchMatch approach enhanced by Denes field linear fitting technique (DLF). The other approach is the photo-response non-uniformity (PRNU), based on Markov Random Field (MRF) to achieve simpler and efficient distribution imaging system [22, 23, 24, 25].To achieve high efficiency of copy-move forgery detection, figure (8) show the

two approaches processing steps. The given image will be classified either if the camera of that image was known or the image is coming from a dataset. After we determine which approach process the image will follow, here the major process will follow either PRNU approach as presented in [25], or will follow the PatchMatch procedure as in [17] to combine a fully fusion algorithm of CMFD.

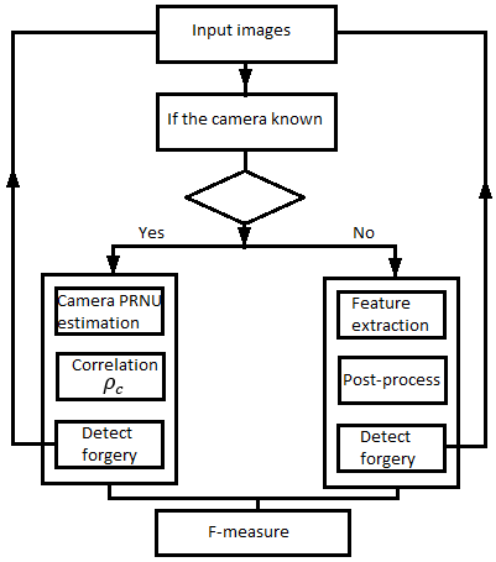


Fig. 8. Integrated Approach

There will be cases where the image can be gotten analyzing by both approaches. However, this case can be solved by making a condition which enables the image to be redirected to one of the two approaches. Since the noise sensor requires a camera reference, in fact, the images which have the camera's fingerprint, by extraction noise residual from the image, there will be more grantee to analyze it by using RPNU approach, also maybe there will be the original image copy that helps to recognize the difference between both images. In both situations either there was the original image or wasn't, still the same approach the best choice to investigate whether that image is present or forged copy.

VI. Experiment Result

The algorithm solved the cases which are mentioned above, and it can detect the copy-move and localize it. The figure (9) summarizes these cases. However, there is other scenarios as in figure (10), may happen in the copy-move which we still working on to make them detectable.

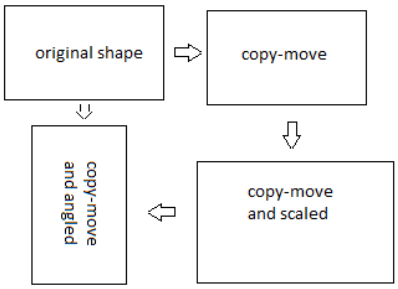


Fig.9. Copy-move in the most cases which can be detected.

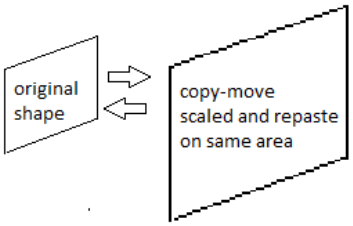


Fig. 10. Shows when the same area is coped and scaled and repasted on the same place

As we can see from the figure (10) it is big challenge to detect the forgery in this situation, also there are other cases where the efficiency will be less than that according to if the image either is colorful, colorless, or black and white.

In our work, we use different image and datasets such as: the GRIP database[1] and Loughborough University dataset[2] besides collective image.

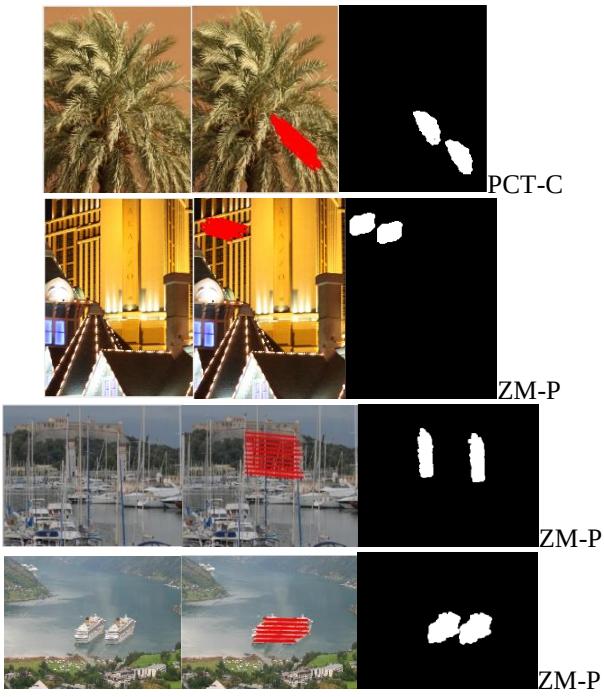
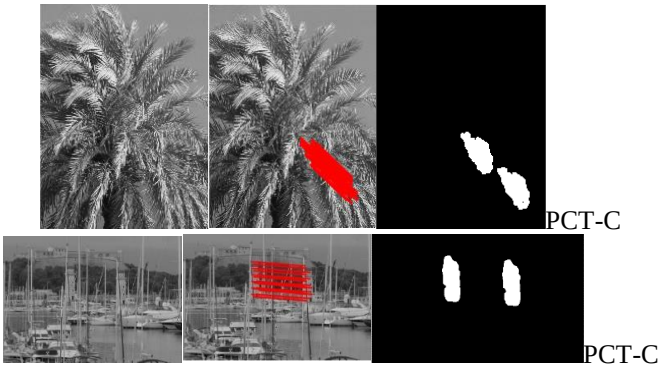


Fig. 11. Detecting the forgery form RGB images form GRIP dataset, (a) the forged image, (b) the selected offset points, (c) localization copy-move forgery mask

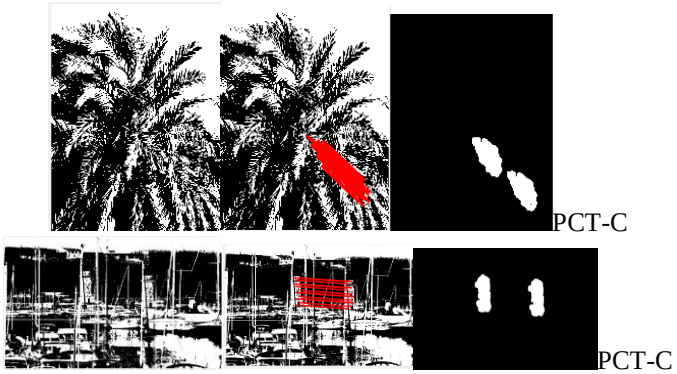
[1] http://www.grip.unina.it

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



a b c

Fig. 12. Detecting the forgery form gray image (a) the forged image, (b) the selected offset points, (c) localization copy-move forgery mask



a b c

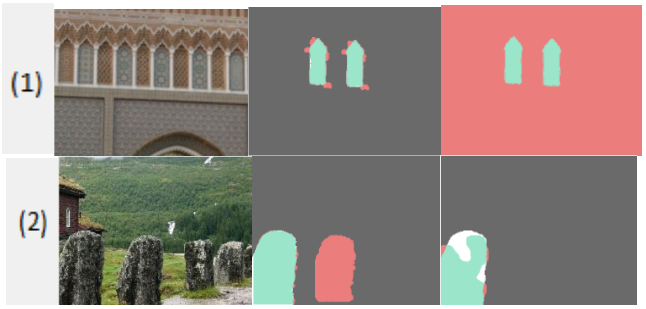
Fig. 13. Detecting the forgery form black and white image (a) the forged image, (b) the selected offset points, (c) localization copy-move forgery mask

When we look to the three above cases and we can notice that number of offset points and the forgery mask is less efficient when the colors are less. If the view is very flat, switching the image from RGB format to BW format may cause loss more feature and as a result, the forgery cannot be detected.

(a) (b) (c)

Fig. 14. The forgery done on RGB image by copy and scaled the copied patch and re-paste on the same image in same location (a) the forged image, (b) no selected offset points, (c) fail to detect and localize copy-move forgery

We make comparison between the algorithms: PatchMatch vs PRNU, by using the same dataset in order to know which one work better and where.



a b c

Fig. 15. Show the comparison between two approaches detect forgery by using PatchMatching and by using photo-response nonuniformity noise (PRNU), (a) is a tampered image, (b) the output mask shows the forgery locations by using PatchMatch for CMFD, (c) shows the output of the forgery detection and location using PRUN.

The is a difference between the F-measure in both approaches, even when the same forged image, is used with same ground root mask. Next table (1) shows the different values which cause the FM verity. However, the PRNU approach evaluation will be the guarantee that the images carry the cameras fingerprint.

Table 1. Show the FM parameters for one image where defined by the proposed approach

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

To make a fair judgment on both approaches, we used same function which was proposed by [25, 17]. However, from the above table, we can notice that, all the predicted conditions are varied.

VII. Conclusion and Future Work

The Copy- move forgery is widely used, and because it can be done very proficiently by beginners. On the other hand, detecting this type of forgery is difficult and it is not guaranteed. There are two intensive challenges for most CMFD algorithms. First one when the copy-move is done by using the background to hide some seen in the image. This case can be detected by using PatchMatching of the offset points in the forged image. The other challenge case when the copy-move done by rescale the copied part and baste it on same location to make it more visible, for instance. This case of forgery requires the original image and PRNU approach will be the best way to detect that type of forgery. The experiment shows that the evaluation is variant even for same image when the color or the resolution change result different F-score. However, F-score overall shoes high efficiency when we used the fusion technique, indeed, we were able to detect different Copy-move forgery format. For future work, we will apply the same concept to forged video and compare the F-score result with litterateur.

Table 2. The evaluation values for detecting CMFD in two different RGB images shown in Fig. 11

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 3. The evaluation values for detecting CMFD to same image in different 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

Table 4. Show the different measurement to same forged image

Image	Algorithm	FM	TPR	TNR	FNR	FPR	PPV	NPV
1.	PatchMatch	0.9138	0.9924	0.9917	0.0076	0.0083	0.8467	0.9996
	PRNU	0.0847	1	0	0	1	0.0442	NaN
2.	PatchMatch	0.6885	0.9510	0.9039	0.0490	0.0961	0.5396	0.9936
	PRNU	0.8800	0.8119	0.9961	0.1881	0.0039	0.9606	0.9781

VIII. 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," *IEEETRANSACTIONSONINFORMATIONFORENSICSANDSECURITY*, 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] 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.

[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] 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.

[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," *IEEETRANSACTIONSONINFORMATIONFORENSICSANDSECURITY,* 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] 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.

[22] 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.

[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.