American Journal of Computer Science and Engineering Survey

Research Article

Fusion Approaches System of Copy-Move Forgery Detection

ABDALLA YE*, IQBAL MT, SHEHATA M

Faculty of Engineering and applied science, Memorial University of New found land, St. John's, Canada

*Corresponding author e-mail: yea764@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 Patch Match 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

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. Digital image forgery can be very varying between the enhancements, which in the most cases is accepted or free of risk to the other types which more dangerous. In Figure 1, 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 [4,6]. 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 Patch Matching offset field will implement more efficient and smoothness of detecting copy-move forgery. In order to speed the matching of the offset points, the Patch Matching algorithm in this work runs Denes-field to find the nearest neighbour field (NN) as follows.

$$(s) = \arg\min \phi \in \Omega \in, \theta \# 0(f(s), f(s+\phi)) \quad (1)$$

$$\mathcal{NN} \cong \mathcal{S}' = \mathcal{S} + (\mathcal{S}) \quad (2)$$

Where s is the pixel in the neighbourhood field Ω. (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.

BACKGROUND

Forgery activities started in early 1840s 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 [7]. The same study [7] 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.

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 (Figure 2).

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.

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

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

The polar form will be fond as:

The Polar form will be fond as:

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

$r \leq 1$.

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

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

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

$$\Omega_n = \{ \frac{\frac{1}{\pi}}{\frac{2}{\pi}} \quad (9)$$

The PCT will be defined on the unit circle, and to generate the Kernel coefficient for each point, three trigonometric functions [8].

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 [9] describe the relationship between them. The Zernike

function can be presented as follows:

$$R_n^c(r) = \cos(\pi n r)^2 \quad (10)$$

Where n, are the order and the rotation respectively. (ρ) is the radial polynomial, and it can be given as:

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

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

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

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

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

$$Z_{nm} \frac{n+1}{2} \sum_{I(p,\theta)} \Sigma(p,\theta) V_{nm}(p,\theta) V_{nm}(p,\theta) \quad (14)$$

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 [10-12].

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 [13]. In fact, this method performs radial projection on the log-polar organize Fourier transformation of image blocks as following:

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

Resample the magnitude values result in to log-polar coordinates

$$|I'(p,\theta)| = |\sigma|^{-2} |p - \log\sigma), \theta - \alpha \quad (16, 17)$$
$$(\theta) = \Sigma \log(|(pj,\theta|)$$

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

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) [14]. The coefficient of the CHT can be estimated by Projecting the image $I(\rho,\theta)$ over the basis function $Kn,m(\rho,\theta)$ of transforming.

$$F_1(n,m) = \int_0^\infty p R_{nm}(p) \times [\frac{1}{\sqrt{2\pi}} \int_0^{2\pi} I(p,\theta) e^{-jm\theta} d\theta] dp \quad (18)$$

The image $(\rho,)$ 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 $(\rho,)$ 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 [15]. The radial function will be variant based on the feature type. The PCT radial function is a cosine function with the argument of $\rho 2$ and normalize the coefficients Cn.

$$(\rho) = C_n \cos(n\pi\rho_2) \quad (19)$$

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

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

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

$$R_r(p) = \frac{1}{p^2} e^{jrIn(p)} \quad (21)$$

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 [16].

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:

$$\in^2 (S) = \sum_{i=1}^{N} || \delta(S_i) - \delta(S_i) ||^2 \quad (22)$$

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).

$$\epsilon^2(S) = \sum_{i=1}^{N} \| \delta(S_i) - \delta(S_i) \|^2 \quad (23)$$

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 (Figure 3).

Table 1 classifies the all predicted conditions based on the scores collected. 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 ground root==max;

TN = sum of detected no forged features with ground root==0);

FP = sum (of detected forged features with ground root==0);

FN = Sum of detected no forged features with ground root==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 (ground root==max), and the rest of the mask will be labeled with low value (ground root==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 an 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.

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 propagation, or by doing a random search. For any region scan, we specify a vector (s), which use a s pixel as patch centre 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 (Figure 6).

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 [17-19], 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 neighbourhood pixels of s through a liner model, and then use transformation parameters to minimize the sum of square error (SSE).

$$\delta`(si) = Asi \quad (24)$$

$$\epsilon^2(S) = \sum_{i=1}^{N} \| \delta(S_i) - \delta(S_i) \|^2 \quad (25)$$

The post-processing follows the next procedure: 1) median filtering on a circular window of radius ρM; 2) computation of the fitting error, $\epsilon 2(s)$, w.r.t. at least-squares linear model over a circular neighbourhood of radius ρN; 3) thresholding of $\epsilon 2(s)$ at level $T\epsilon 2$; 4; removal of couples of the regions closer than $TD2$ pixels; 5) removal of the regions smaller than TS 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 $T\epsilon 2$, $TD2$, and TS

which explained the steps 3, 4, 5. When the copy-move pixel detected s, in specific region, same pixel in the mirrored region $s+(s)$ will be marked as copy-move pixel. Last step will treat the morphological effects as a result of the previous steps.

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 is 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 [20].

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 (Figure 7).

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:

$$pc = (,) \tag{27}$$

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, have more universal input options. Therefore, we propose to integrate two forensic approaches. First, Patch Match 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 [21-23].To achieve high efficiency of copy-move forgery detection, (Figure 8) shows 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 [24], or will follow the PatchMatch procedure as in [17] to combine a fully fusion algorithm of CMFD.

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.

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. 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 colourful, colourless, or black and white. In our work, we use different image and datasets such as: the GRIP database1 and Loughborough University dataset2 besides collective image (Figure 11). 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 (Figure 12). 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. We make comparison between the algorithms: PatchMatch vs PRNU, by using the same dataset in order to know which one works better and where. 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 (Tables 2 and 3) 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 (Figure 13). To make a fair judgment on both approaches, In Table 4 we used same function which was proposed [17,24]. However, from the above table, we can notice that, all the predicted conditions are varied (Figure 14, 15).

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 Patch Matching 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.

REFERENCES

1. Agarwal V, Mane V (2016) Reflection SIFT for Improving the Detection of Copy-Move Image Forgery. ICRCICN 84-88.
2. Anil Dada Warbhe (2015) Block Based Image Forgery Detection Techniques. Int J Eng Sci Res Tech 289 - 297
3. VH Gajanan, Bitajdar K (2013) Dgigtal image forgery detection using passive techniques a survey Digital Investigation 10: 226-245.
4. Al Qershi OM, Khoo B (2013) Passive detection of copy-move forgery in digital images: state of the art. Forensic Sci Int 231: 284-295.
5. NS Pravin Kakar, Exposing Post processed Copy Paste Forgeries through Transform-Invariant Features. Trans info foren sec 7: 1018-1028.
6. Rizvi (2015) Digital Image Forgery Detection.
7. Ira Tuba (2016) Digital Image Forgery Detection Based on Shadow Texture Feature. Tele com Forum 22-23.
8. SK Zhuo Yang (2011) Fast Polar Cosine Transform for Image Description. MVA2011 IAPR Conf on Mach Vision App 320-323.
9. M Teague (1980) Image analysis via the general theory of moments. J Opt Soc America 70: 920-930.
10. Seung JR, Min JL, Heung KL (2010) Detection of Copy Rotate Move Forgery Using Zernike Moments. 51-65.
11. M Pawlak (1988) On the Accuracy of Zernike Moments for Image Analysis. Trans on Pattern Analysis and Mach Int 20: 1358-1364.
12. MiaoZhenjiang (2000) Zernike moment-based image shape analysis and its application 21: 169-177.
13. M Sevinc Bayram (2009) An efficient and robust method for detecting copy-move forgery. 1053-1056.
14. Neng Y, Arsenault H, April G (1982) Rotation invariant digital pattern recognition using circular harmonic expansion. 21: 4012-4015.
15. Seung JR, Kirchner M, Min Jeong L (2013) RotationInvariantLocalizationofDuplicatedImage Regions Based on Zernike Moments, Trans info foren sec 8: 1355-1370.
16. Davide Cozzolino (2013) Efficient Dense Field Copy Move Forgery Detection. Trans Info Foren Sec 10: 2284-2297.
17. Simon K, Shai A (2011) CoherencySensitiveHashing. Int Conf Comput Vis 1607-1614.
18. Avidan S (2012) Tree CANN - k-d tree Coherence Approximate Nearest Neighbor algorithm. Eur Conf Comput Vis 602-615.
19. D Amiano L, Cozzolino D, Poggi G (2015) Video forgery detection and localization based on 3d Patch Match. Int Conf 1-6.
20. Lukas J (2006) Digital camera identification from sensor pattern noise. Trans Info Foren Sec 205-214.
21. Giovanni C, Giovanni P, Carlo S (2014) A Bayesian MRF Approach for PRNU-Based Image Forgery Detection. Trans Info Foren Sec 9: 554-567.
22. Stuart G (1984) Stochastic relaxation, Gibbs distributions, and the Bayesian restoration of images. Trans Pattern Analysis Mach Int 6: 721-741.
23. D Elia C, Poggi G, Scarpa G (2003) A tree structured Markov random field model for Bayesian image segmentation. Trans Image Process 12: 1259-1273.
24. J Besag (1986) On the statistical analysis of dirty pictures J Royal Stat Soc Series 48: 259-302.

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

Table 2: The Evolution values for detecting CMFD in two different RGB images shown in Figure 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
	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
	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

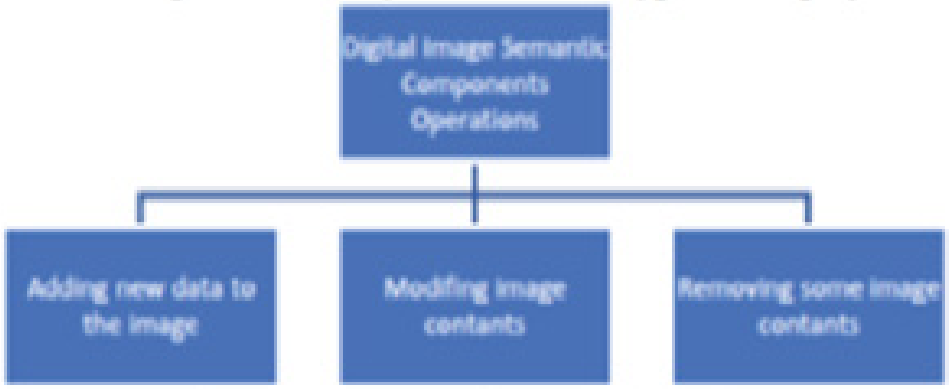

Figure 1: Some Common Forgery Classification.

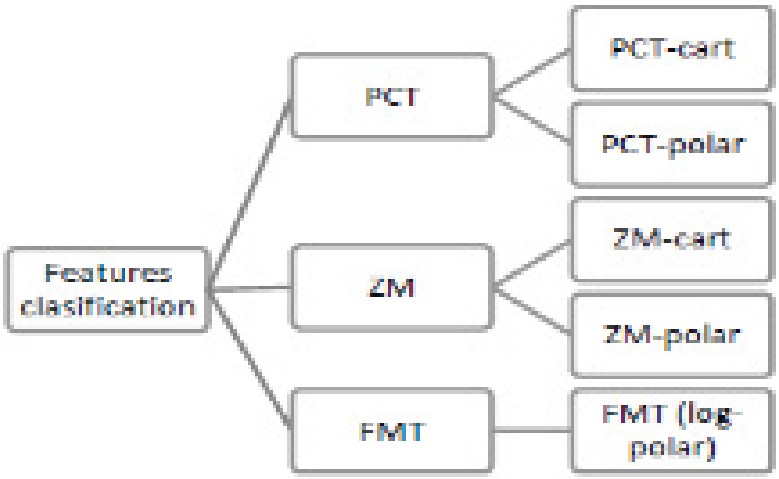

Figure 2: The Feature Classification.

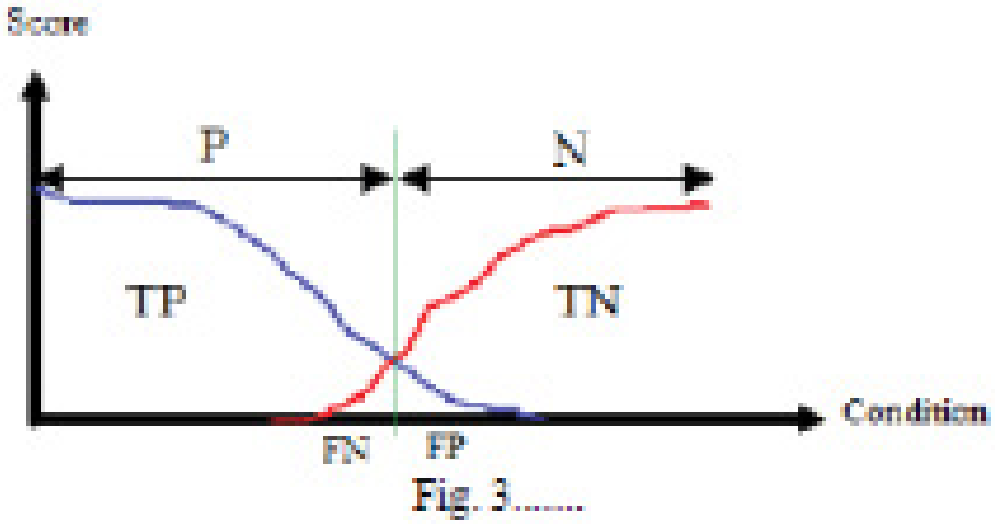

Figure 3: The false positive and false negative will be the other scores out of AND operation to present wrongly detected pristine image and non-detected forged image respectively.

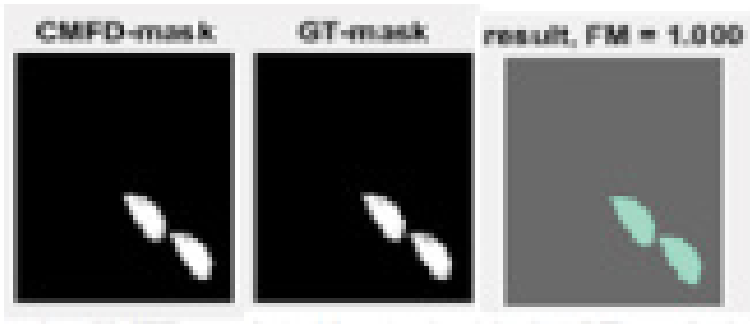

Figure 4: When the CMFD mask is identical with the GT mask the F-measure will be ideal.

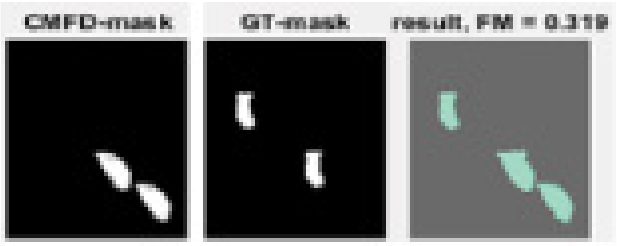

Figure 5: The F-measure when the CMFD mask GT mask become variant.

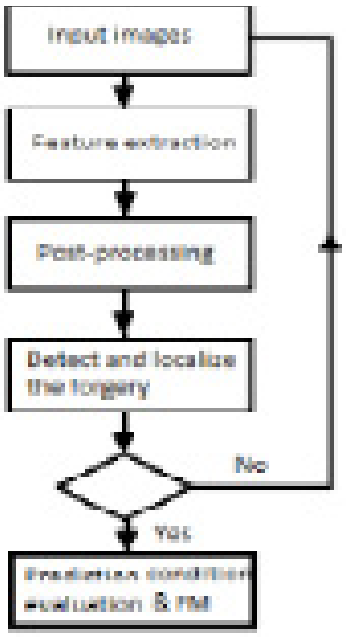

Figure 6: Shows the Copy –move forgery detection algorithm based on Patch Matching.

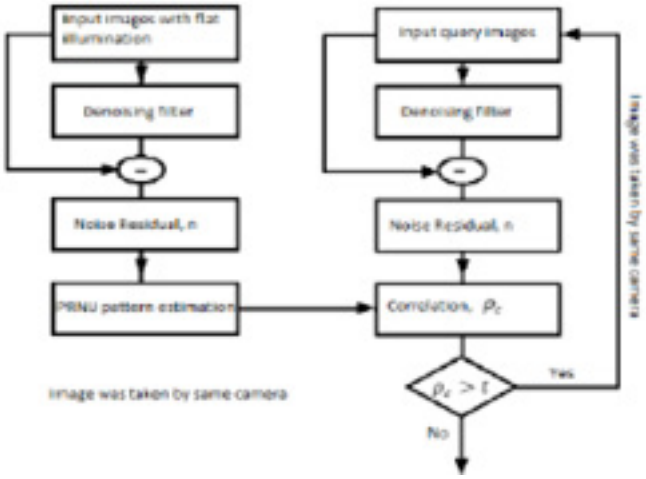

Figure 7: PRNU algorithm for forgery detection.

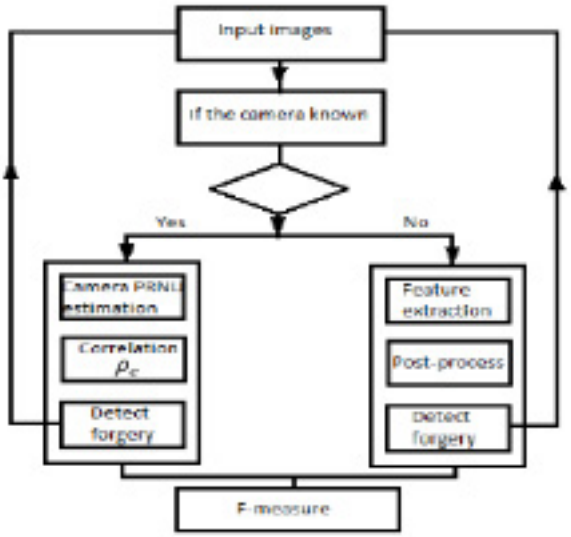

Figure 8: Integrated Approach.

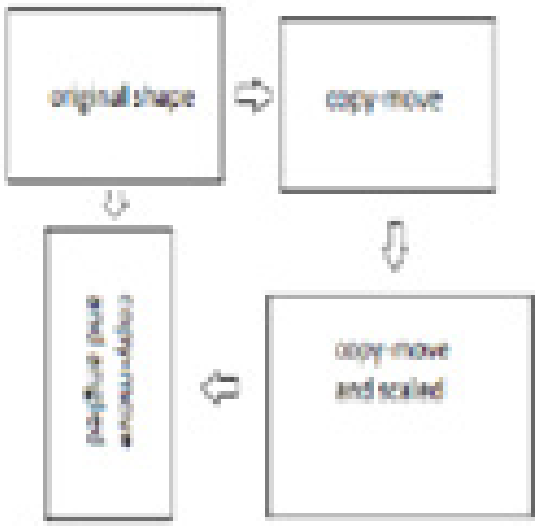

Figure 9: Copy-move in the most cases which can be detected.

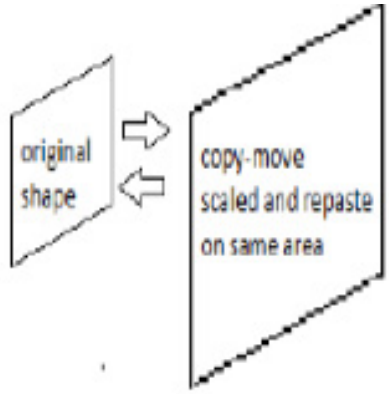

Figure 10: Shows when the same area is copies and scaled and repeated on the same place.

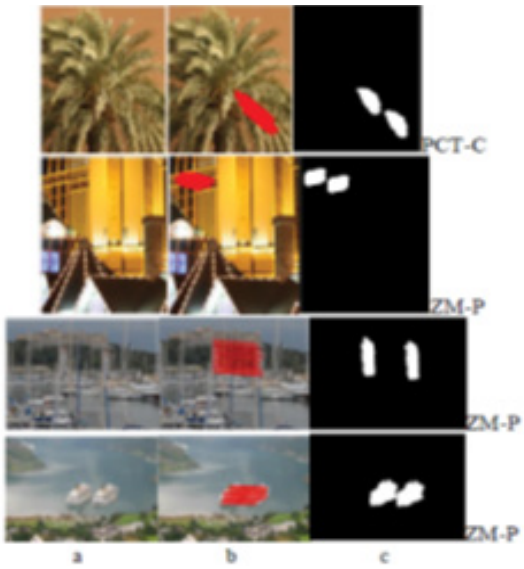

Figure 11: Detecting the forgery form RGM images from GRIP dataset. (a) The forged image, (b) The selected offset points, (c) localization copy-move forgery mask.

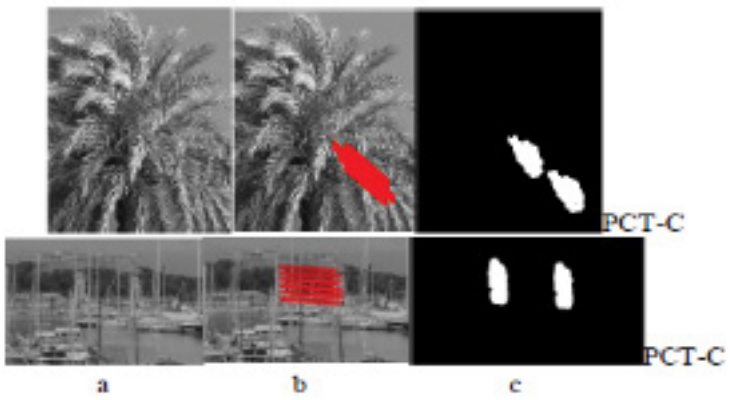

Figure 12: Detecting the forgery form gray image (a) the forged image, (b) the selected offset points, (c) localization copy-move forgery mask.

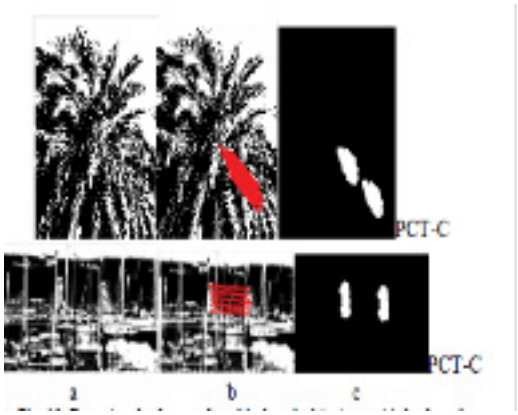

Figure 13: Detecting the forgery black and white image (a) the forged image (b the selected offset points, (c) localization copy-move forgery mask.

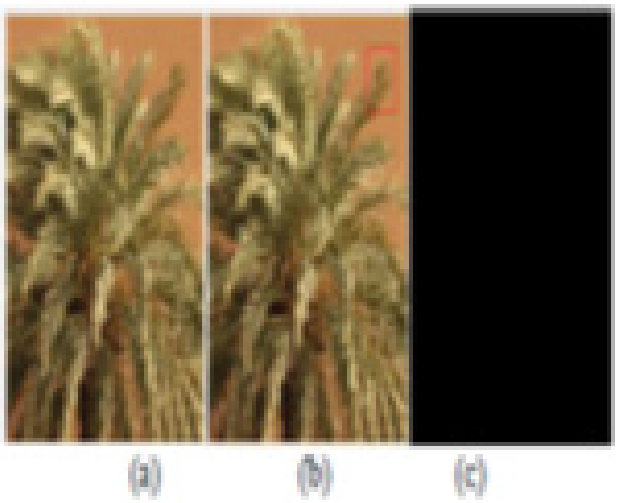

Figure 14: The forgery done on RGB image by copy and scaled the copied patch and re-paste on the same image in same location (a) the forged image, (b) no selected offset points, (c) fail to detect and localize copy-move forgery.

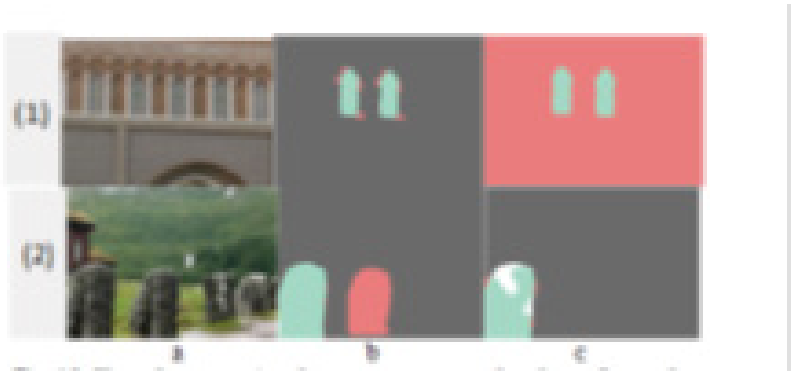

Figure 15: Show the comparison between two approaches detect forgery by using Patch Matching and by using photo-response Nonuniformities noise (PRNU), (a) is a tampered image, (b) the output mask shows the forgery locations by using PatchMatch for CMFD, (c) shows the output of the forgery detection and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