Copy Move Forgery Detection on Digital Images

Ruchita Singh
Department of Computer Science and Engineering, MMU, Haryana, India

Ashish Oberoi
Department of Computer Science and Engineering, MMU, Haryana, India

Nishi Goel
Department of Computer Science and Engineering, MMU, Haryana, India

ABSTRACT
In today's scenario forging of the Digital images has become a common phenomena. The availability of low cost manipulation software also boost to this practice. The foremost practice of manipulating the digital images employed by the most forgerer is the copy move forgery. Copy move forgery is basically concerned with concealing or duplicating one region in an image by pasting certain portions of the same image on it. Numerous Algorithms are proposed to detect copy move forgery in digital images. In this paper an enhanced way to detect copy move forgery is proposed. It is analyzed that block based methods are secured against noise and JPEG compression where as feature based methods are robust to the rotation and scaling operations .The proposed approach use both block based method and feature based method to increase the accuracy rate of forgery detection. The Proposed method employed DCT and SIFT to extract features from image and matching those collected features to detect forgery on image and also perform the localization of the Forged Regions in the Digital Image.

General Terms
Digital Images, Forgery.

Keywords
Forgery, DCT, SIFT, Copy-Move, Block-Based Method, Feature-Based Method.

1. INTRODUCTION
Authenticity of digital images is a major concern now a days, due to the advancement in the availability of powerful digital image processing programs such as Adobe Photoshop, Corel Draw etc, which makes it relatively easy to create digital forgeries from same or multiple images. Digital images are the foremost source of information when we used them as an evidence for any event in the court of law. Digital images are being used in many more applications ranging from military to medical diagnosis and from art to user photography. Now-a-days, digital crime is growing at a faster rate that even surpasses defensive measures. Sometimes a digital media content may be found to be incontrovertible evidence of a crime or of a malevolent action. To determine whether the digital image is authentic or not is a key purpose of image forensics. There are several different types of tampering attacks but the most common and the immediate
One is the copy move forgery. In Figure 1 sample case of forgery is depicted.

(a)

(b)

Figure 1: Example of Copy Move Forgery. (a) Original Image (b) Forged Image.

1.1 COPY MOVE FORGERY
Copy-Move image forgery is the widely used technique to edit the digital image. Copy-move forgery involves the pasting of image blocks in same image and conceal important information or object from the image. As a result of this the originality of the image is lost and puts at stake the authenticity of that digital image. In Copy-Move Forgery detection copied blocks are from same image so they sustain the same properties as the other blocks of image and therefore makes it very difficult to detect the forgery

1.2 FORGERY DETECTION METHODS
To determine whether the digital image is authentic or not is a key purpose of image forensics. There are several different types of tampering attacks but the most common and the immediate one is the copy move forgery. Copy move forgery involves concealing or duplicating one region in an image by pasting certain portions of the same image on it. Digital forensics [1], deals with developing systems in the absence of watermarks [2] or signatures inserted in the image.
Digital image forensics has two principal approaches to detect forgery as shown in Figure 2; first one is active approach

which includes watermarking and stenography. These are implemented at the time of image acquisition.
Active approach requires a special hardware implementation to mark the authenticity of the digital image such as including the digital signature in the image or encrypting the digital image. The water marking consist of hiding certain information in an image at the time of image acquisition and to check the authenticity of the image, embedded information is extracted from the image and verified with the original watermarks. Hence, this method relies on the source information before hand. Second one is passive approach which does not require any prior information about the image and only depends on traces left on the image by different processing steps during image manipulation. There are two methods of passive approach. First one is image source identification, which identifies the device used for the acquisition of the digital image.
It tells that the image is computer generated or digital camera image. By using this method the location of forgery in image cannot be determined.

Second one is tampering detection; it detects the intentional manipulation of images. Image manipulation is denoted as tampering when it aims at modifying the content of the visual message. Numerous techniques are proposed to manipulate digital image either by copy-move forgery or by image composition and tampering image features.

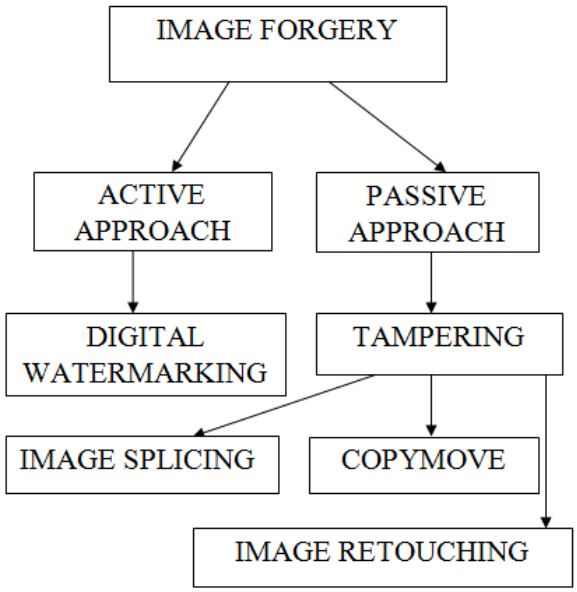


Figure 2: Methods to Detect Forgery

2. LITERATURE REVIEW

There were several techniques proposed to detect image forgery in the literature of digital image forensics .Copy move forgery is one of the popular method to create the image forgery in which the part is copied and moved to the other place in the same image. There are so many techniques as shown in Figure 3, are used to detect such type of forgeries.
Author proposed one such approach to detect copy move forgery, which basically perform rigorous search by comparing the image to every cyclic-shifted versions of it [3].There is a technique based on the radon transform and phase correlation in order to improve the robustness in forgery detection. The proposed technique can detect forgeries even if the forged images were undergone some image processing operations such as rotation ,scaling, Gaussian noise addition, [4] etc.
Author proposed a copy move image forgery detection algorithm using block matching approach and Principal Component Analysis (PCA).In order to detect images through post-processing operations quickly and efficiently, forged image detection based on radon and Fourier-Mellin transform is presented [5]. Another possibility for forgery detection is to classify textures that occur in natural images using statistical measures and find discrepancies in those statistics between different portions of the image [6]. At this point, however, it appears that such approaches will produce a large number of missed detections as well as false positives. Since the key characteristics of Copy-Move forgery is that, copied part and the pasted part belongs to the same image, one technique to detect forgery is exhaustive search, but it is computationally complex because, blocks are directly extracted from original image and thus resulting in a large number of blocks.
Author proposed copy-move forgery detection method based on speeded up robust features (SURF), which detects duplication region with different size [7].

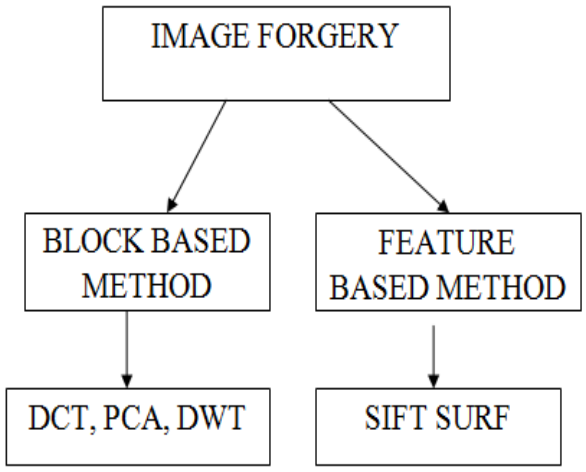


Figure 3: Copy Move Forgery Detection Method.

The proposed method can detect copy-move forgery with minimum false match for images with high resolution. To increase the speed of operation process many researchers use blocking approaches .In robust match algorithm, author used Discrete Cosine Transform (DCT) for the detection [8]. It was based on quantized DCT coefficient of each overlapping block of the image. However this method fails for any type of geometrical transformations of the query block e.g. rotation, scaling. A key point based methods were proposed to overcome the rate complexity of block based method. Author proposed the method of detection using scale invariant feature transform (SIFT) key point [9]. It detects the key point and match them using nearest neighbourhood search. SIFT is robust to rotation and scaling but unable detect forgery by smooth surfaces. Author analyzed different algorithms based on their performance. As a result it was shown that different key point-based methods like SIFT and SURF, and block-based methods like DCT, PCA, Discrete Wavelet Transform (DWT), perform that deals at exposing the malicious image manipulation [10]. Author proposed method relies on Scale

Invariant Features Transform (SIFT) and features matching, and improves previous work by introducing a new robust clustering phase based on the J-Linkage algorithm, and an accurate forgery localization procedure[11]. Author summarizes the three robust feature detection methods: Scale Invariant Feature Transform (SIFT), Principal Component Analysis (PCA)–SIFT and Speeded Up Robust Features (SURF). This paper uses KNN (K-Nearest Neighbor) and Random Sample Consensus (RANSAC) to the three methods in order to analyze the results of the methods' application in recognition[12]

3. PROPOSED METHOD

In this proposed method an input image is taken and converted into grayscale, then we apply DCT on it to find the intensity of that image and store the intensity levels in a separate Matrix. Image is then divided into the multipliers of two. In our proposed method we have used the block size of 16x16.After that apply the SIFT feature extraction on the each 16x16 block size image to extract the features of the image. That extracted feature vector is stored in matrix sort them lexicographically, apply quantization to assign some values to array and save the coordinate values. Identify the outliers if the norm of the sift vector is greater than set threshold, then keep pairs otherwise discard them. Perform Matching and then localization of forged regions.

3.1 PROPOSED ALGORITHM

Step 1: An input image is taken and Convert the RGB image into Gray Scale.

Step 2: Apply (Discrete Cosine Transform) DCT and store the intensity levels in a separate matrix.

Step 3: Divide image into a block size in the multipliers of 2(16x16).

Step 4: Apply (Scale Invariant Feature Transform) SIFT to compute the feature vector for each block.

Step 5: Store the feature vectors in rows of matrix and save all the coordinates value.

Step 7: Perform quantization to assign value to the obtained feature vectors and Lexicographically sort them.

Step 6: Identification of outliers based on the similarity features and save the coordinate values and also find the intensity of the outliers.

Step 7: Perform Matching to find the same area.

Step 8: Localization of the forged region.

Step 9: Display Image with the Forged Regions.

3.2 FLOWCHAT

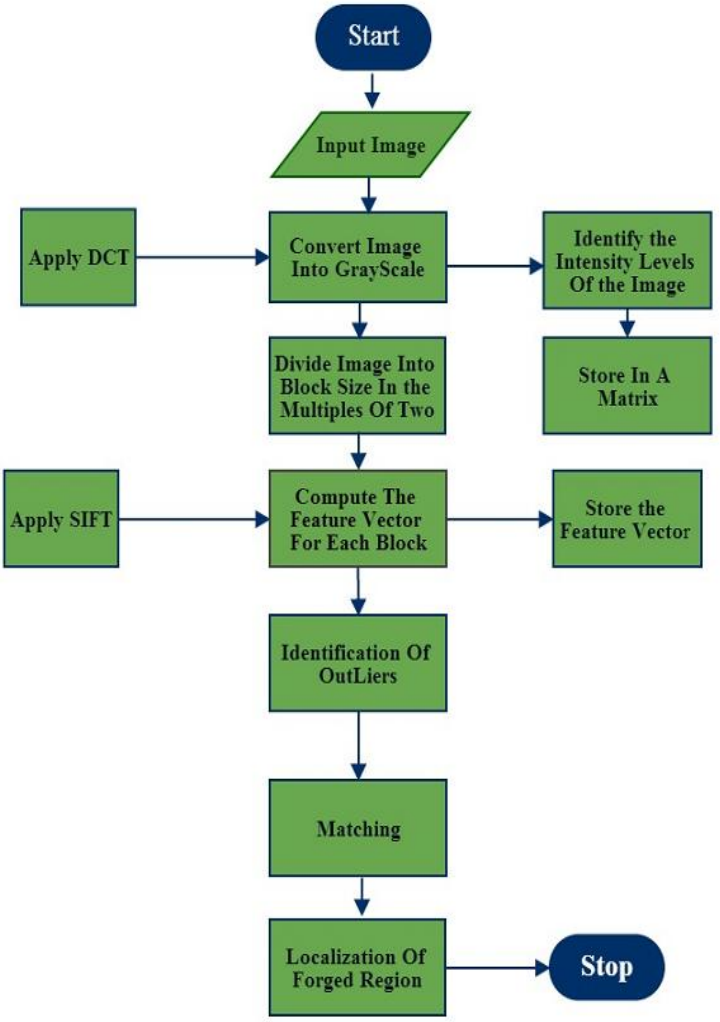


Figure 4: Shows Flow Chart of Proposed Method

4. RESULTS AND ANALYSIS

The proposed method is tested on various images. Each forged image is first divided into 16x16 block size and feature vector is calculated and pixel position is stored. Quantization of feature vector is performed for each block. Outliers are found for each image and then matching is performed. Finally localization of key points is done. The proposed algorithm is tested on single or multiple forged images and analyzed on parameters such as processing time , accuracy rate, localization of correct forged area on image.

FORMULA USED

To calculate the feature vector for each block

$$\text{Sum}(i, j) = \sum \text{image}(i-1, j-1) * \text{kernel}(i, j)$$

Quantization of feature vector

$$QP = 100 * T\_present$$

$$FQ = \text{floor}(\text{feature vector}(i)/QP)$$

$$X = FQ * QP$$

Where, T_present is set to 0.1 and x is the quantized value.

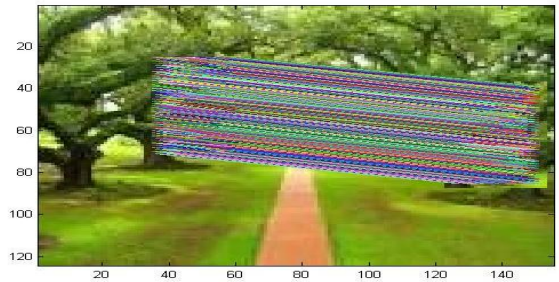
(a)

(b)

(c)

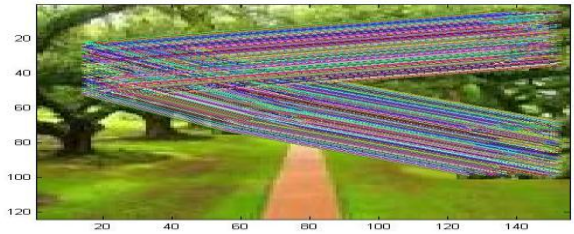
(d)

(e)



(f)

(g)



(h)

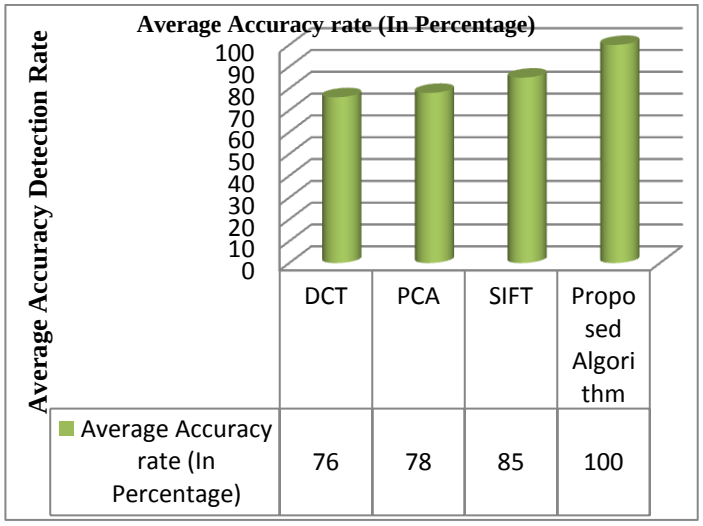
Figure 5: (a) Forged Image of Mall of Mysore. (b) Forgery Detection for the Single Copy Move by Proposed Algorithm.(c) Forged Image of Mall of Mysore. (d) Forgery Detection for the Multiple Copy Move by Proposed Algorithm.(e) Forged Image of Forest. (f) Forgery Detection for the Single Copy Move by Proposed Algorithm.
(g)Forged Image of Forest.(h) Forgery Detection for the Multiple Copy Move by Proposed Algorithm.

Table 1: Comparative Results of Proposed Algorithm generated for the Image of Mall of Mysore

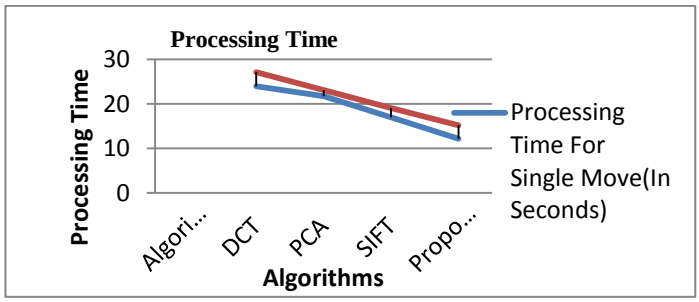
Algorithm	Processing Time For Single Move(In Seconds)	Processing Time For Multiple Move(In Seconds)	Size (In Pixel)	Average Accuracy rate (In Percentage)
DCT	24.005	27.167	357X141	76
PCA	21.714	23.113	357x141	78
SIFT	17.009	19.112	357x141	85
Proposed Algorithm	12.162	15.156	357x141	100

Table 2: Comparative Results of Proposed Algorithm generated for the Image of Forest

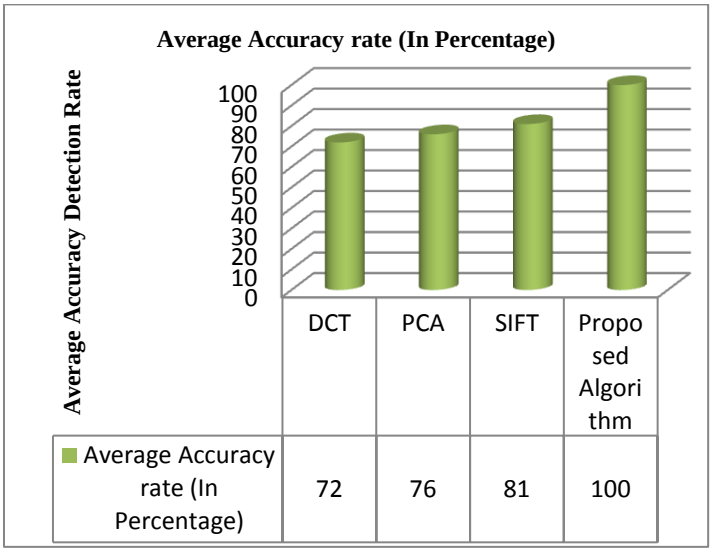
Algorithm	Processing Time For Single Move(In Seconds)	Processing Time For Multiple Move(In Seconds)	Size (In Pixel)	Average Accuracy rate (In Percentage)
DCT	21.771	25.559	155X124	72
PCA	22.153	24.547	155X124	76
SIFT	16.907	18.528	155X124	81
Proposed Algorithm	16.775	25.865	155X124	100



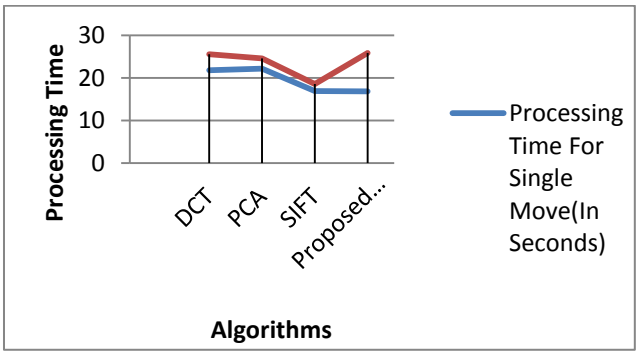
Graph 1: Accuracy Rate of Proposed Algorithm with respect to DCT,SIFT,PCA for the Image of Mall of Mysore .



Graph 2: Processing Time of Proposed Algorithm with respect to DCT,SIFT,PCA for the Image of Mall of Mysore .



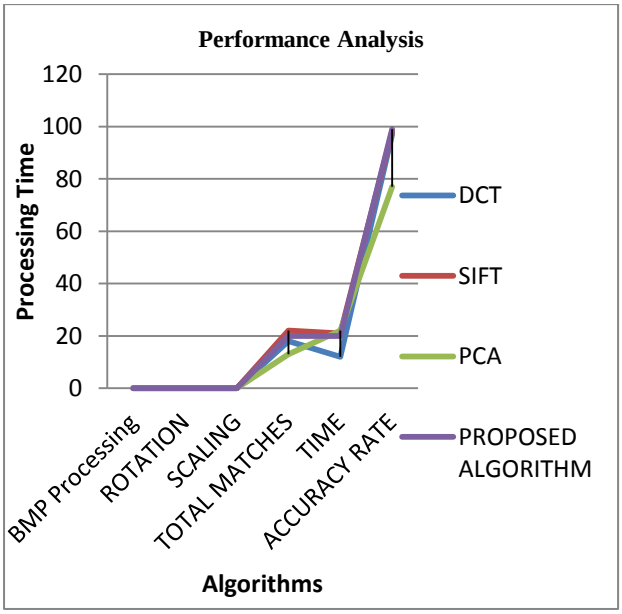
Graph 3: Accuracy Rate of Proposed Algorithm with respect to DCT,SIFT,PCA for the Image of Forest



Graph 4: Processing Time of Proposed Algorithm with respect to DCT,SIFT,PCA for the Image Forest

Table 3: Concluded Results of Proposed Algorithm

Algorithm	BMP Processing	Rotation	Scaling	Total Matches	Time	Accuracy Rate
DCT	Y	N	N	18	12	97
SIFT	N	Y	Y	22	21	98
PCA	Y	N	N	13	22	77
PROPOSED ALGORITHM	Y	Y	Y	20	10	99



Graph 5: Performance Analysis of Proposed Algorithm

5. CONCLUSION

In this research work our proposed algorithm is analyzed on various parameters like processing time, accuracy rate, rotation, scaling, bmp processing and it is concluded that this proposed approach has generated better results. Comparative analysis also justifies the performance of this approach. The Proposed algorithm is also tested for multiple forgery detection and results obtained depicted that this algorithm is efficient in detecting multiple forgery. Proposed algorithm takes less time than conventional block based method. Results generated by proposed Algorithm is better as compared to other block based and feature based methods. Hence it is concluded that this technique and algorithmic approach is efficient in terms of the results and complexity, still there is scope of the future work for further enhancement of the results.

In future scope of work, the method can be extended to detect forgery by more post-processing operations on snippet and further techniques can be associated such as genetic algorithms, neural networks.

6. REFERENCES

[1] S. Ly u and H. Farid, "How realistic is p hotorealistic?", IEEE Transactions on Signal Processing, vol. 53, no. 2, pp. 845–850, 2005.

[2] I. J. Cox, M. L. Miller, and J. A. Bloom, Digital watermarking. San Francisco, CA: Morgan Kaufmann, 2002.

[3] Ashima Gupta, Nisheeth Saxena and S.K.Vasistha, "Detecting Copy move Forgery using DCT," International Journal of Scientific and Research Publications, Vol 3(5), ISSN 2250-3251, 2013.

[4] Hieu Cuong Nguyen and Stefan Katzenbeisser, "Detection of copy move forgery in Digital images using Radon transformation and phase correlation," Eighth InternationalConference on Intelligent information hiding and Multimedia Signal Processing, IEEE, pp.134-137, 2012

[5] A.C.Popescu and H.Farid, "Exposing Digital Forgeries by Detecting Duplicated Image Regions," Technical Report, TR2004-515, Department of computer Science, Darmouth College, pp.758-767, 2006

[6] Swapnil H.Kudke, A.D.Gawande, "Copy-Move Attack Forgery Detection by Using SIFT," International Journal of Innovative Technology and Engineering (IJITEE), Vol.(5), ISSN 2278-3075, 2013

[7] B.L.Shivakumar and Lt.Dr.S.Santhosh Baboo, "Detection of Region Duplication Forgery in Digital Images Using SURF," International Journal of computer science Issues, Vol.8(4), ISSN 1694-0814, 2011

[8] I.Amerini,L.Ballan,R.Caldelli,A.D.Bimbo,and G.Serra, "A SIFT-based Forensics Method for Copy-Move Attack Detection and Transformation Recovery," IEEE Transaction on Information Forensics and Security, Vol.6, no.3, pp.1099-1110, 2011.

[9] V.Christlein,C.Riess, J.Jordan, C.Riess, and E.Angelopoulou, "An Evaluation of popular Copy-Move Forgery Detection Approaches," IEEE Transactions on Information Forensicsand Security, Vol.7, pp.1841-1854, 2012

[10] Preeti Yadav, Yogesh Rathore and Aarti Yadu, "DWT Based Copy-Move Image Forgery Detection," International Journal of Advanced Research in Computer Science and Electronics Engineering, Vol.1(5), ISSN 2277-9043, 2012.

[11] B.L.Shivakumar and Dr.S.Santhosh Baboo, "Automated Forensics Method for Copy- MoveForgery Detection based on Harris Interest Points and Sift Descriptors," International Journal of Computer Applications, Vol.27(3), pp.0975-8887, 2011.

[12] Nattapol Chaitawittanun, "Detection of Copy-Move Forgery by Clustering Technique," International Conference on Image, Vision and Computing, Vol.50(10), pp-3948-3959, 2012.