Comparative Study of Copy Move Forgery Techniques

Ms. Gurpreet Kaur[#1], Dr. RajanManro
ResearchScholar(Assistant Professor),Associate Professor
Department of Computer Science,Desh Bhagat University,Mandi Gobindgarh,India
Department of Computer Science,Desh Bhagat University,MandiGobindgarh,India

Abstract

Digital images are broadlyused in today'sworld because they are the main base of information. However,due to image changing tools it is easy to forge the contents of a digital image; The particular image is reliable or not is the main problem in image processing. When these particular images are used in a court of law,to influence judgment it creates lot of problem.Copy-move tampering is a basic typeof image synthesizing, where some part of an image is copied and pasted to another place. Many techniques can be used to forge the digital images. Here,we attempted to review some feature extraction methods for copy move forgery detection techniques.In other words,weexplore the problem of identifying the copy-move forgery and describe an efficient and reliable detection method. The method,we described may successfully discover the forged part even when the copied area is enhanced/retouched to merge it with the background and even when the forged image is saved in a lossy format, such as JPEG. The results of the proposed method is applied on several forged images and it indicates that theproposed method is valid in detecting the image region duplication and quite strong to additive noise and blurring.

Keywords: *Passive, Copy move, Forensics, Forgery, Genuineness, Digital image*

I. INTRODUCTION

Due to the availability of powerful digital image processing programs such as photoshop,3D max.it is relatively easy to create digital forgery from one or multiple images.It creates a serious problem when these particular images are used to the level of trust,especially in cases like presents a paper in front of courtroom as some evidence. With the use of different photo editing software's such as Adobe Photoshop,it is very difficult to trust on originality of image and it has become a challenging problem. Due to this problem, researchers suggestsome methods to examine the originality of digital images. In this paper, we discover the problem of identifying the type of digital forgery – the copy moveforgery. Copy move forgery is one of the most popular image forgery techniques .The purpose of copy-move image forgery is to cover evident details or to duplicate some region of an image. A portion of an image is copied and pasted into another region in the same image. It is very difficult to detect forgery with naked eyes, thus forgery detection method should detect the duplicated regions, even though they are slightly notsimilar. Digital forgery techniques can be classified into two approaches which are active and passive approach. The passive technique of digital image forgery tries to identify forgery in digital images without any previous information and the copy move forgery is a type of passive method.

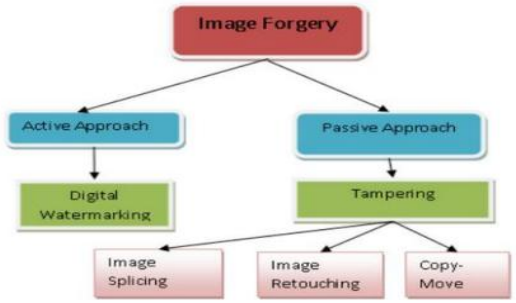

Figure-1:
Image Forgery Methods

II. THE NEED FOR DETECTION OF DIGITAL FORGERIES

Due to the availability of powerful digital image processing programs, such as Photoshop, it is relatively easy to create digital forgeries from one or multiple images. An example of a digital forgery is shown in Figure 2.


INTERNET

Spies turn to high-tech info ops

PCs, Internet used for manipulating images, public opinion

BY DANIEL VERTON

ALTERED IMAGE

Federal intelligence agencie are studying ways to use com puters and the Internet, rathe than just leaflets and radi broadcasts, to shape and dis seminate information designe to sway public opinion in th world's hot spots.

As part of its so-called "per ception management" progra the intelligence community ha for decades created misinforma tion to trigger political chang without direct political or mil tary involvement in countrie where the United States ha vested interests, such as Ira and North Korea.

Acting on congressional re ommendations to bolster re search and development in ir formation technology, intell gence agencies are turning t PCs to develop more sophist cated means of manipulatin and delivering digital photo video clips and recorded soun to portray fictitious events hopes of provoking desirabl

Altered Egos

The top photo, of a fictitious meeting between President Clinton and Saddam Hussein, was generated by digitally altering and combining elements from three photos, shown below the altered image. Intelligence agencies plan to use similar techniques to create images and then disseminate them via the In-ternet in their efforts to influence events in foreign countries, such as Iraq.

Figure-2:
Example of Copy Move Forgery

As the above example shows, with the help of threedifferent photographs(White House, Bill Clinton, and Saddam Hussein),A new composite image can be created. To create an illusion of an out-of-focus

background, the White House was rescaled and blurred. Then, Bill Clinton and Saddam were cut off from two different images and pasted on the White House image. Attention was taken to bring in the speaker stands with microphones while preserving the correct shadows and lighting. Another example of digital forgeries was given in the plenary talk by Dr. Tomaso A. Poggio at Electronic Imaging 2003 in Santa Clara. In his talk, Dr. Poggio showed how engineers can watch and learn the lip movements of any person from a short video clip and then digitally manipulate the lips to randomly alter the spoken content of a person. In this example, they showed the match between the sound and lip movement that how a TV anchor announcing evening news was altered to make the anchor appear singing a popular song. The fact that one can use these type of refined tools to digitally manipulate images and video to create non-existing situations threatens to shrink the credibility and value of video tapes and images presented as evidence in court independently of the fact whether the video is in a digital or analog form. To alter an analogue video, one can easily digitize the analog video stream, upload it into a computer, perform the forgeries, and then save the result in the NTSC format on an ordinary videotape. As one can expect, the situation will only get more inferior when the tools are needed to perform the forgeries from research labs to commercial software. Despite the fact that the need for detection of digital forgeries has been accepted by the research community, very few publications are currently available. Digital watermarks have been proposed as a means for brittle authentication, content authentication, detection of tampering, localization of changes, and recovery of original content [1]. While digital watermarks can provide valuable information about the image reliability and its processing history, the watermark must be present in the image before the tampering occurs. This bounds their application to controlled environments that include military systems or surveillance cameras. Unless all digital acquisition devices are prepared with a watermarking chip, it will be unlikely that a forgery-inthe-wild will be detectable using a watermark. It might be possible, but very difficult, to use unintentional camera "fingerprints" related to sensor noise, its color gamut, and/or its dynamic range to find tampered areas in images. Another possibility for blind forgery detection is to categorize textures that occur in natural images using statistical measures and find differences in those statistics between different portions of the image ([2], [3]). At this point, however, it appears that such approaches will create a large number of missed detections as well as false positives. In the next section, we introduce one common type of digital forgeries – the copy-move forgery – and show a few examples.

III. COPY MOVE FORGERY

In a Copy-Move forgery, a portion of the image itself is copied and injected into another portion of the same image. This is usually performed with the purpose to make an object "disappear" from the image by covering it with a segment copied from another portion of the image. Textured areas, such as grass, foliage, gravel, or fabric with irregular patterns, are ideal for this purpose because the copied areas will likely merge with the background and the human eye cannot easily detect any doubtful artifacts. As the copied parts come from the same image, its noise component, color palette, dynamic range, and most other important properties will be well-matched with the rest of the image and thus will not be visible. To make the forgery even hard to detect, one can practice the feathered crop or the retouch tool to further find any traces of the copied-and-moved segments.

FIGURE-3:
Copy Moveforgery
(a)Original image; (b)Forged Image

IV. KEY STEPS FOR COPY MOVE FORGERY DETECTION

This section describes the basic steps used for detecting the copy move forgery.

Step-1- ***Preprocessing*****:**Here, it converts the color image into a gray scale image by using three input channels R,G,B with their values I=0.299R+0.587G+0.114B channels, and I is obtained the gray image.

Step-2- ***Feature Extraction*****:** Under this, the feature vectors are identified. In block based method, the image is fragmented into overlapping or non-overlapping blocks of fixed size. From each block of the image, the features are extracted . While in key

point based methods, the features are extracted around the key points.

Step-3 - *Matching*: This step mainly identifies the duplicated regions of the image. The duplicated regions present in an image can be found in matching step by comparing their feature vectors. In block based methods, lexicographical sorting is applied to find similar feature vectors. Onthe anotherhand, the approximate nearest neighbor can be identified by any searching procedure for the feature matching in key point based methods.

Step-4-*Filtering*:By using any filtering techniques. The number of false matches can be reduced.

V. TECHNIQUES IN COPY MOVE FORGERY DETECTION

The following section describes the various techniques in copy move forgery.

A. Block Based Image Forgery Detection Techniques

Here the image is divided into blocks of equal size to bring out the features of each block. Then these features are matched with each other to find out suitable match. After finding these match, the equal block pairs are treated as copy move.

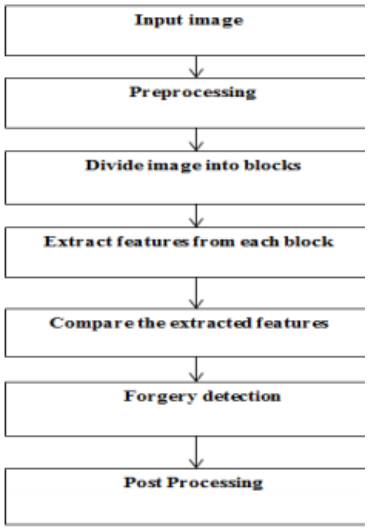

Figure-4:
Block Based Method

For feature extraction, any of the following methods can be used.

Several **Block based Copy Move Image forgery detection techniques** are described as follows.

Fridrich et al [4] proposed a method for detecting copy move forgery based on DCT.Thevarious steps involved in this method are described as follows:

(a) Preprocessing the input image.
(b) Divide the image into blocks of the same size.
(c) For each block, apply DCT.
(d) Create feature vectors and sort lexicographically. If two blocks in input image are same then their corresponding feature vectors will also be same.
(e) If the two feature vectors will be same and the distance between two should be more than block size then calculate the shift vector s and increase the count for s where s= (s1, s2) = (x1-x2, y1-y2), (x1,y1) and (x2,y2) are the coordinates of the upper left corner of the similar block pairs.
(f) For each shift vector a counter c is considered and for the same block pairs the counter is increment by 1 as C(s1,s2)= (s1,s2)+1.
(g) If the counter exceeds the threshold value,then mark that region as duplicated.
(h) The pixels in the forged region are colored to highlight the duplication.

The Wavelet based region duplication forgery detection was proposed by Wang et al [6]. The steps are explained as below:

(a) Preprocessing the input image.
(b) Divide the image into blocks of equal size.
(c) Create feature vectors by applying DWT in each block.
(d) The sorting operation like lexicographic is performed in the rows of feature vectors. Now compare the feature vectors and ifthe two consecutive rows of the vectors are similar, then record the positions of the identical blocks.
(e) Then calculate the shift vector for a doubted pair of blocks and for each shift vector a counter c is taken and the counter is increment by 1for similar block pairs.
(f) If the counter is exceeding the user defined threshold value, mark that region as duplicated and forged.

In [7] Farid et al presented a technique for copy move forgery detection based on Principal Component Analysis. Under this technique, the length of the feature vector is reduced and also the computational cost is reduced.

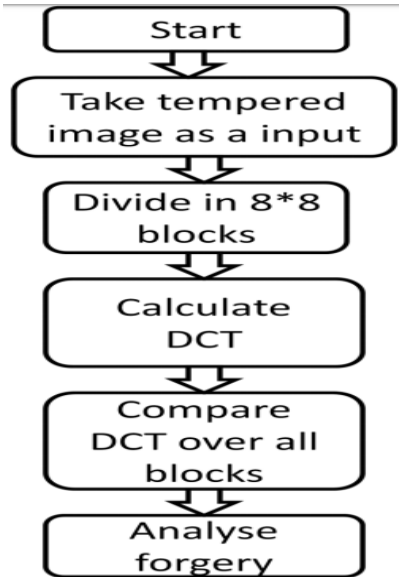

figure-5:
flowchart of dct

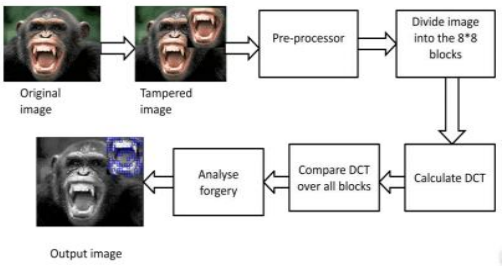

Figure-6:
Block Diagram Of DCT Algo

VI. RESULTS OF DCT ALGORITHM

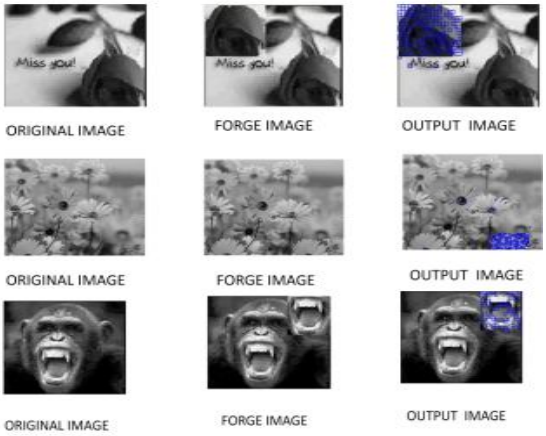

FIGURE-7:
Results Of DCtAlgo

A. Key point Based Image Forgery Detection Techniques

To identify the key points, variouskey point detector algorithms are used. Then the feature extraction is performed by matching the feature vectors which is extracted from a region around these key points. In other words the feature points are extracted by using different methods like **SIFT, SURF**etc without any image subdivision.The approaches like clustering, Euclidean distance, the nearest neighbor etc can be used for feature point matching. A forgery can be found if matching features are found. The post processing techniques, such as RANSAC can also be used for removing false matches.

Various techniques for detecting copy move forgery in images are discussed as follows:

Baboo et al [8] proposed a method for detecting region duplication forgery using SURF. The steps involved in this method are discussed below:

SURF (Speeded Up Robust Features) is used to extract features and it is a robust local feature detector. The feature detector is based on Hessian matrix. For image duplication, any geometric transformations such as scaling and rotation are applied to the image but SURF is invariant to these transformations.

The various steps for SURF detectors and descriptors are explained as follows:

(a)Preprocessing the input image**.**

(b)Integral Image: Create the integral image representation of the input image. Then the pixel sums over upright rectangular areas can be calculated. The speed up of the calculation of any upright rectangular area can be increased in this way. The integral image is calculated by taking the sum of the values between the point and the origin at any point in an image

(c)Keypoint Detection: For detecting the key points in an image, SURF uses Hessian matrix. Then calculate the determinant of Hessian matrix. If it is positive ,the points will be treated as extremeaotherwise they will be discarded.

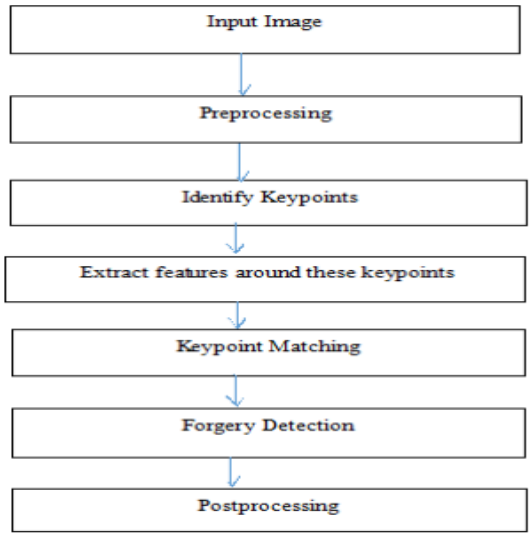

FIGURE-8:
FLOWCHART OF KEY POINT BASED IMAGE FORGERY

B. Gabor Filter

In image processing, a gabor filter is a type of linear filter used for edge detection.It is named after Dennis Gabor [8].Frequency and orientation representations of gabor filters are indistinguishable to those of human visual system and they have been found to be preciselysuitable for texture representation and discrimination. In the spatial domain, a 2D gabor filter is a Gaussian kernel function modulated by a sinusoidal plane wave. The general form of a 2D gabor filter is expressed as:- $G\sigma,f,\theta=g\sigma(x,y).\ \exp\ [2\Pi jf(x\ \cos\theta+\ y\ \sin\theta)]$ Where $g\sigma(x,y)=1/2\Pi\sigma2\ \exp[-(x2\ +y2\ )/2\sigma2]]$ where $j=\sqrt{(-1)}$,f is the frequency of the sinusoidal wave, ɵ controls the orientation of the function and gσ(x, y) is the Gaussian function with scale parameter σ. The parameters of the Gaborfilter are therefore given by frequency f,orientation h, and the scale σ.

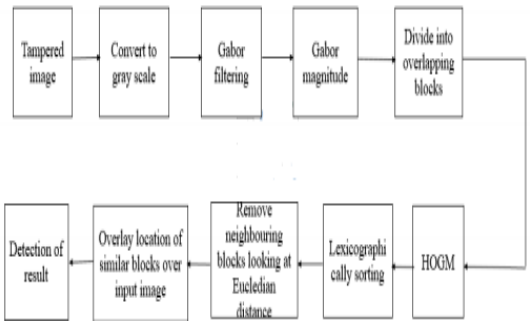

Figure-9:
Working Of Gabor Filter

C. Results using Gabor Filter:

Figure-10
Input Image and Gray Scale Image Using Gabor Filter

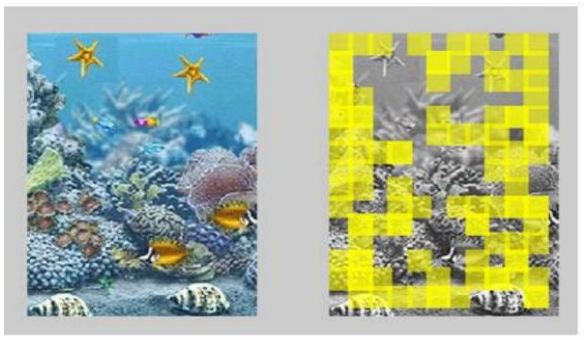

Figure-11:
Output Results Using Gabor filter

VI. COMPARISON OF VARIOUS FEATURE EXTRACTION METHODS

Image Forgery is the process of making an illegal alteration or imitation of an image information. In this paper, we used DCT algorithm for forgery detection. There is amethod that can find tampered JPEG images and further pinpoint the tempered portions, by observing the double quantization effectthatwas hidden among the DCT coefficients. The JPEG process is a broadly used form of lossy image compression that only used by the DCT.The JPEG method is used for both Black & white and colored images. Our method discoversreplicated forgery regions by splitting the image into 8*8 overlapping blocks and then we explore for the identical regions in the image. We show the potential of this method on capable forgeries and evaluate its strongness also.

Reference no	Feature Extraction Method	Feature Matching Parameter	Performance
[1]	SIFT	Hierarchical clustering	Multiple copied region is detected
[1]	SIFT	Euclidean distance	Give good performance and invariant to scale and rotation of the pasted object.
[2]	SURF	Feature Vector	Fast process, Detect Scaled and rotated object , reduce computational complexity
[4]	DCT	Feature length	Computational complexity is high.Some limitations are there in case of natural images.
[6]	DWT	Feature length	The feature vector dimension reduction, but gives low accuracy if the forged area is at center.

Table 1: Comparison of Various Feature Extraction methods

VII. CONCLUSION

As the copy move forgeries have taken conservative in our daily lives, there is a budding need of passive image forgery detection techniques to discourse various types of image forensics. Although various methods have been developed in the field of copy move image forgery detection for certain cases, but a technique which gives a complete solution is still needed. This study presented here a short-term review on various methods in copy move forgery detection

Experimentation results indicate that these techniquescanidentify the copy-move forgery rapidly, and can stand certain transformations and post processing such as, scaling, rotation, noise blurring and so on. However, further analysis is still needed to automatically locate the forged region and its boundary.

REFERENCES

[1] R.Singh, A. Oberoi, and N. Goel, "Copy move forgery detection on digital images," International Journal of Computer Applications, vol. 98, no. 9, pp. 17–22, 2014.

[2] E. Ardizzone, A. Bruno, and G. Mazzola, "Copy-move forgery detection via texture description," in Proceedings of the 2nd ACM workshop on Multimedia in forensics, security and intelligence, pp. 59–64, ACM, 2010.

[3] J. Fridrich, D. Soukal, and J. Lukáš, "Detection of copy-move forgery in digital images," in Proceedings of Digital Forensic Research Workshop, Cleveland, Ohio, USA, August 2003.

[4] Ardizzone E, Bruno A, Mazzola G. Detecting multiple copies in tampered images. In: Image Processing (ICIP), 2010 17th IEEE International Conference on. IEEE; 2010. p. 2117–20.

[5] David G. Lowe., "Distinctive Image Features from Scale-Invariant Key-Points", International Journal of Computer Vision ,2004,60(2), pp.91-1

[6] Xu Bo, Wang Junwen, Liu Guangie and Dai Yuewei., "Image Copy-Move forgery Detection Based on Surf", International Conference on Multi-media Information Networking and Security, 2010 , pp.889-892

[7] Mohammad FarukhHashmi, AadityaHambarde., "Copy move forgery detection using DWT and SIFT", International Conference on Intelligent System Design and applications, 2013, pp.188-193.

[8] J. Fridrich, D. Soukal, and J. Lukas, "Detection of Copy-Move Forgery in Digital Images", in Proceedings of Digital Forensic Research Workshop, August 2003

[9] NehaJadhav, SuvarnaKharat, PunamNangare,"Copy-Move Forgery Detection using DCT", International Journal for emerging Technologies and Engineering, Vol 2 Isuue 3 March 2015, ISSN 2348-8050.

[10] Wang Y, Gurule K, Wise J, Zheng J. "Wavelet based region duplication forgery detection." ,Proceedings of the 9th International Conference on Information Technology: New Generatio (ITNG '12); April 2012; IEEE; pp. 30–35.

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

[12] B L Shivakumar and Lt.Dr.SSanthoshBaboo, "Detection Of Region Duplication Forgery in DigitalImages using SURF, International Journal Of Computer Science Issues, Vol 8, Issue 4, No 1, July 2011.

[13] SwapnilH.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

[14] I.Amerini,L.Ballan,R.Caldelli,A.D.Bimbo,andG.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.

[15] 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

[16] David G. Lowe., ―Distinctive Image Features from Scale-Invariant Key-Points‖, International Journal of Computer Vision ,2004,60(2), pp.91-1

[17] Xu Bo, Wang Junwen, Liu Guangie and Dai Yuewei., ―Image Copy-Move forgery Detection Based on Surf‖, International Conference on Multi-media Information Networking and Security, 2010 , pp.889-892

[18] Mohammad FarukhHashmi, AadityaHambarde., ―Copy move forgery detection using DWT and SIFT‖, International Conference on Intelligent System Design and applications, 2013, pp.188-193.

[19] J.Fridrich, D. Soukal, and J. Lukas, ―Detection of Copy-Move Forgery in Digital Images‖, in Proceedings of Digital Forensic Research Workshop, August 2003.

[20] Tao Jing Xinghua li, Feifei Zhang, Image Tamper Detection Algorithm Based on Radon and fourier-Mellin Transform",pp 212-215 IEEE2010

[21] Sarah A. Summers, Sarah C. Wahl"Multimedia Security and Forensic Authentication of Digital images, "http://cs.uccs.edu/~cs525/studentproj/poj52006/sasummer/doc/cs525projsumm ersWahl.doc".

[22] J. Fridrich, D. Soukal, and J. Lukas, "Detection of Copy-Move Forgery in Digital Images", in Proceedings of Digital Forensic Research Workshop, August 2003.

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

[24] X.Kang and S. Wei, "Identifying Tampered Regions Using Singular Value Decomposition in Digital Image Forensics," International Conference on Computer Science and Software Engineering, pp. 926-930,2008

[25] B.Mahdian and S. Saic, "Detection of copy-move forgery using a method based on blur moment invariants.," Elsevier Forensic Science International, vol. 171, no. 2-3, pp. 180-189 Sep. 2007.

[26] S.-jinRyu, M.-jeong Lee, and H.-kyu Lee, "Detection of Copy-Rotate- Move Forgery Using Zernike Moments," IH , LNCS 6387, vol. 1, pp. 51-65, 2010.