Image Copy Move Forgery Detection using Block Representing Method

Rohini.A.Maind, Alka Khade, D.K.Chitre

Abstract- As one of the most successful applications of image analysis and understanding, digital image forgery detection has recently received significant attention, especially during the past few years. At least two trend account for this: the first accepting digital image as official document has become a common practice, and the second the availability of low cost technology in which the image could be easily manipulated. Even though there are many systems to detect the digital image forgery, their success is limited by the conditions imposed by many applications. Most existing techniques to detect such tampering are mainly at the cost of higher computational complexity. In this paper, we present an efficient and robust approach to detect such specific artifact. Firstly, the original image is divided into fixed-size blocks, and discrete cosine transform (DCT) is applied to each block, thus, the DCT coefficients represent each block. Secondly, each cosine transformed block is represented by a circle block and four features are extracted to reduce the dimension of each block. Finally, the feature vectors are lexicographically sorted, and duplicated image blocks will be matched by a preset threshold value. In order to make the algorithm more robust, some parameters are proposed to remove the wrong similar blocks. Experiment results show that our proposed scheme is not only robust to multiple copy-move forgery, but also to blurring or nosing adding and with low computational complexity.

Keywords- Didgital forencics copy-move forgery circle block duplicated region

I. INTRODUCTION

From the early days an image has generally been accepted as a proof of occurrence of the depicted event. Computer becoming more prevalent in business and other field, accepting digital image as official document has become a common practice. The availability of low-cost hardware and software tools, makes it easy to create, alter, and manipulated digital images with no obvious traces of having been subjected to any of these operations. As result we are rapidly reaching a situation where one can no longer take the integrity and authenticity of digital images for granted. This trend undermines the credibility of digital images presented as evidence in a court of law, as news items, as part of a medical records or as financial documents since it may no longer be possible to distinguish whether a given digital images is original or a modified version or even a depiction of a real-life occurrences and objects. Digital image forgery is a growing problem in criminal cases and in public course. Currently there are no established methodologies to verify the authenticity and integrity of digital images in an automatic manner. Detecting forgery in digital images is an emerging research field with important implications for ensuring the credibility of digital images [1].

In the recent past large amount of digital image manipulation could be seen in tabloid magazine, fashion Industry, Scientific Journals, Court rooms, main media outlet and photo hoaxes we receive in our email. Digital image forgery detection techniques are classified into active and passive approach [3]. In active approach, the digital image requires some pre-processing such as watermark embedding or signature generation at the time of creating the image, which would limit their application in practice. Moreover, there are millions of digital images in internet without digital signature or watermark. In such scenario active approach could not be used to find the authentication of the image. Unlike the watermark-based and signature-based methods; the passive technology does not need any digital signature generated or watermark embedded in advance [4]. There are three techniques widely used to manipulate digital images [3]. 1) Tampering – tampering is manipulation of an image to achieve a specific result. 2) Splicing (Compositing) - A common form of photographic manipulation in which the digital splicing of two or more images into a single composite 3) Cloning (Copy-Move).

A.C.Popescu et. al. [1] applied a principle component analysis (PCA) on small fixed-size image to yield a reduced dimension DCT block representation. Each block was represented as 16x16 and the coefficients in each block were vectorized and inserted in a matrix and the corresponding covariance matrix was constructed. The matrix constructed stores floating numbers. By finding the eigenvectors of the covariance matrix, a new linear basis was obtained. Duplicated regions are then detected by lexicographically sorting all of the image blocks. Their method was robust to compression up to JPEG quality. Li Jing et. Al. [2] proposed firstly analyzes and summarizes block matching technique, then introduces a copy-move forgery detecting method based on local invariant feature matching. It locates copied and pasted regions by matching feature points. It detects feature points and extracts local feature using Scale InvariantTransform algorithm. Vincent Christlein [3] In this, aim to answer whichcopy-move forgery detection algorithms and processing steps(e. g. , matching, filtering, outlier detection, affine transformation estimation) perform best in various post processing scenarios. Fridrich et al. [4] suggested the first method for detecting the copy-move forgery detection. In their method, first the image is segmented into overlapping small blocks followed by feature extraction. They employed discrete cosine transform (DCT) coefficients for this purpose. The DCT coefficients of the small blocks were lexicographically sorted to check whether the adjusted blocks are similar or not. In their paper, the method shown was robust to the retouching operations. However, the authors did not employ any other robustness tests.. S. Bayramet. Al. [5],proposed Fourier-Mellin transform (FMT) method to each block FMT values

Manuscript Received May 2014

Rohini.A.Maind, Department Computer, Terna Engineering College Nerul, Navi Mumbai, India

Alka Khade, Department Computer, Terna Engineering College Nerul, Navi Mumbai, India

D.K.Chitre, Department Computer, Terna Engineering College Nerul, Navi Mumbai, India

are finally projected to one dimension to form the feature vector. More recently Xunyu Pan et. al[6] suggested a method to detect duplicated regions with continuous rotation regions. As described in [6] the new method was based on the image SIFT features.First the SIFT features are collected from the image, and the image is segmented into non-overlapping examination blocks. The matches of SIFT keypoints in each non-overlapping pixel blocks are computed. After which the potential transform between the original and duplicated regions are estimated and the duplicated regions are identified using correlation map. Even though using SIFT keypoints guarantee geometric invariance and their method enables to detect rotated duplication, these methods still have a limitation on detection performance since it is only possible to extract the keypoints from peculiar points of the image. Frank Y. Shih et. Al.,[7], discuss the techniques of copy-cover image forgery and compare four detection methods for copy-cover forgery detection, which are based on PCA, DCT, spatial domain, and statistical domain. We investigate their effectiveness and sensitivity under the influences of Gaussian blurring and lossy JPEG compressions. Preeti Yadav, Yogesh Rathore[8],proposed an improved algorithm based on Discrete Wavelet Transform (DWT) is used to detect such cloning forgery. In this technique DWT (Discrete Wavelet Transform) is applied to the input image to yield a reduced dimensional representation.After that compressed image is divided into overlapping blocks. These blocks are then sorted and duplicated blocks are identified. Due to DWT usage, detection is first carried out on lowest level image representation so this Copy-Move detection process increases accuracy of detection process.

Chun Wang et.al.[9]More challenging situation for detection of copy-move forgery is to detect the duplicated region which is rotated some angle before it is pasted. The method presented by [9] to detect duplicated regions in limited rotation angles.

B.L.Shivakumar[10],In this a technique is presented to detect Copy-Move Forgery based on SURF and KD-Tree for multidimensional data matching. We demonstrate our method with high resolution images affected by copy-move forgery.

Recently, Bayram et. al [11] suggested a method by applying Fourier Mellin Transform (FMT) on the image block. They first obtained the Fourier transform representation of each block, re-sampled the resulting magnitude values into log-polar coordinates. Then they obtained a vector representation by projecting log-polar values onto 1-D and used these representations as our features. In their paper, the authors showed that their technique was robust to compression up to JPEG quality level 20 and rotation with 10 degree and scaling by 10%.

Yanjun Cao, Tiegang Gao [12], present an efficient and robust approach to detect such specific artifact. Firstly, the original image is divided into fixed-size blocks, and discrete cosine transform (DCT) is applied to each block, thus, the DCT coefficients represent each block.Secondly, each cosine transformed block is represented by a circle block and four features are extracted to reduce the dimension of each block. Finally, the feature vectors are lexicographically sorted, and duplicated image blocks will be matched by a preset threshold value. In order to make the algorithm more robust, some parameters are proposed to remove the wrong similar blocks.

II. COPY-MOVE FORGERY

Copy-Move is a specific type of image manipulation, where a part of the image itself is copied and pasted into another part of the same image (Fig 1).

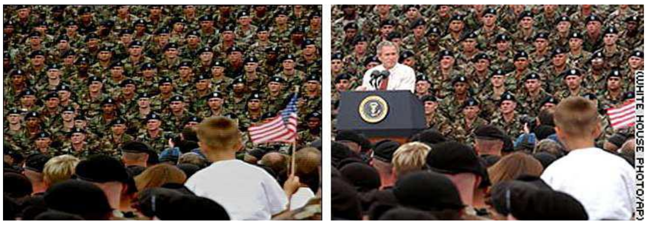


Fig 1. Is an example of copy-move forgery where a group of soldiers are duplicated to cover George Bush. Hence, the goal in detection of copy-move forgeries is to detect image areas that are same or extremely similar.

Copy-Move forgery is performed with the intention to make an object “disappear” from the image by covering it with a small block copied from another part of the same image. Since the copied segments come from the same image, the color palette, noise components, dynamic range and the other properties will be compatible with the rest of the image, thus it is very difficult for a human eye to detect. Sometimes, even it makes harder for technology to detect the forgery, if the image is retouched with the tools that are available.

III. PROPOSED SCHEME

The goal in copy-move forgery detection is detecting duplicated image regions, even if they are slightly different from each other. A copy-move forgery is created by copying and pasting content within the same image, and potentially post processing it. Typical motivations are either to hide an element in the image, or to emphasize particular objects.

The entire architecture of the proposed method(block representing based on improved DCT) for copy-move forgery detection is given in figure II:

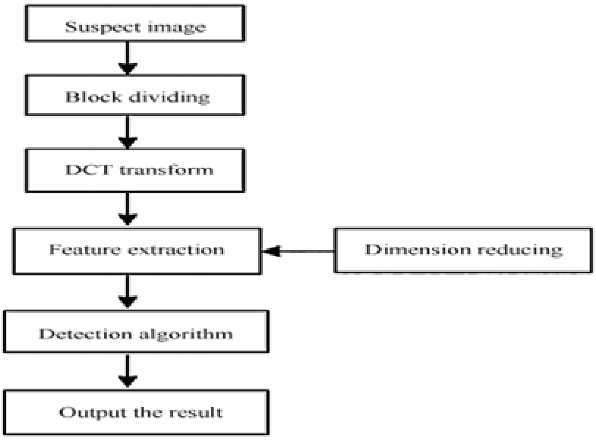


Fig.2: Architecture of the detection algorithm

The steps involved in proposed method are as follows:

1. Dividing the suspicious image into fixed-size blocks.
2. DCT is applied to each block to generate the quantized coefficients.
3. Representing each quantized block by a circle block andextracting appropriate features from each circle block.

4. Searching similar block pairs.
5. Finding correct blocks and output them.

Step 1. Take 2 images.Divide it into the fixed size blocks such as, M*N grayscale image first split up into overlapping blocks of B*B pixels:

$$Bij(x, y) = f(x + j, y + i)$$

Where,

$$x, y \in \{o,....B-1\}$$
$$i \in \{1,....M-B+1\}$$
$$j \in \{1,....N-B+1\}$$

We able to obtain Nblocks of overlapped subblocks from suspicious image:

$$N_{blocks} = (M-B+1)\times(N-B+1) \quad \text{…………...} \quad \text{-(1)}$$

Step 2. For each block DCT is applied, after that DCT coefficients matrix with same size as the block is exploited .which can represent the corresponding block.

Step 3. Assume the size of the block Bi is 8*8,the coefficient matrix is also 8*8.The nature of DCT that the energy only focuses on the low frequency coefficients.

If the image block undergoes DCT transform, we can use four part energy to represent the whole image while without losing any important information. For this basic motivation, we use a circle block to represent the coefficients matrix and divide it into four parts: C1, C2,C3,C4 is shown in image figureIII.

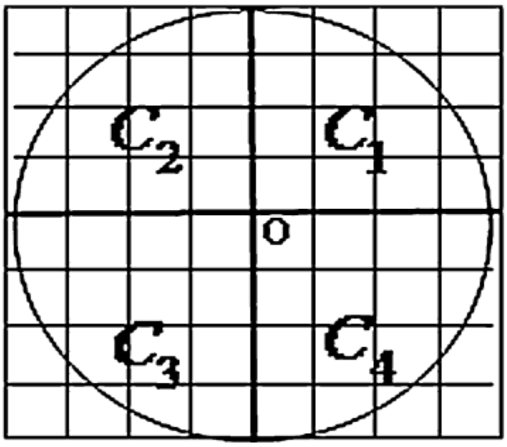


Fig.3. Feature Extraction

Using a circle block instead of a square block does not affect the detection efficient, on the contrary, it can decrease the computational complexity.

To obtain the matching features, denote v1,v2,v3,v4 as the feature of c1,c2,c3,c4. We can get $Vi\,(i=1,2,3,4)$ though equation:

$$Vi = \frac{\sum f(x,y)}{C\_area} \quad (f(x,y) \in C\_areai, \;\; i = 1,2,3,4) \quad \text{.. (2)}$$

Vi = mean of coefficients value corresponding to each Ci.

After that 4 features are gotten, which can be combined to feature vector with the size of 1*4 denote as: *V*=[v1,v2,v3,v4].

Step 4. The feature vector are extracted and arranged to a matrix:

$$A = \begin{bmatrix} V1 \\ . \\ . \\ . \\ V(M-B+1)(N-B+1) \end{bmatrix}$$

A is then lexographically sorted. meantime ,take all left corner's coordinate of each block which represented by circle block.

Each element of A is vector

Sorted set is defined as $\hat{A}$

Based on $\hat{A}$ Euclidean distance m_match = $(A\hat{i}, Ai\hat{j})$ between adjusent pairs of $\hat{A}$ is calculated using following equation:

m_match $(A\hat{i}, Ai\hat{j})$=

$$\sqrt{\sum_{k=1}^{4}(Vi^{k} - Vi + j^{k})^{2}} \langle \; similarity\ threshold$$

we calculate the actual distance between two similar blocks as follows:

m_distance $(Vi, Vi + j)$=

$$\sqrt{(xi - xi + j^{2}) + (yi - yi + j)^{2}} \rangle \; distance\ threshold$$

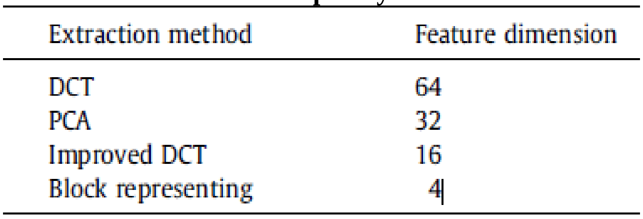
Step 5. Morphological operation is used and output the final result.

The use of DCT to detect forgery is better for jpeg images than using a predefined method PCA. We have further tried in this approach to make the program efficient by applying DCT instead of PCA. Since the PCA does not detect the forgeries for jpeg image efficiently, we apply DCT so that we detect forgery on jpeg image too. After that we compare both the approaches and find out the results and compare the results. Truncation of the PCA basis typically reduces the dimension from 64 to 32. This technique works by first applying a principal component analysis (PCA) on small fixed size image blocks to yield a reduced dimension representation.

IV. EXPERIMENTAL RESULTS

A key problem in the detection algorithm is the computational complexity, which is caused by the amount of the matching blocks and the dimension of the feature vector. There are some researchers use different methods to reduce the computational complexity, for example, use DCT-based, Improved DCT-based, and PCA method respectively.In this paper, our algorithm focuses on the dimension of feature vector. We use a circle block to represent each block which is quantized by DCT, and then four features are extracted, compared with both method, the amount of the dividing blocks are same, however, the feature vector's dimension of ours is lower, which implies our method has a lower computational complexity and TABLE.I. also makes a comparison with them.

Table.1.comparison of time complexity



Extraction method	Feature dimension
DCT	64
PCA	32
Improved DCT	16
Block representing	4

In our experiment we take different size of images respectively and calculate the complexity.

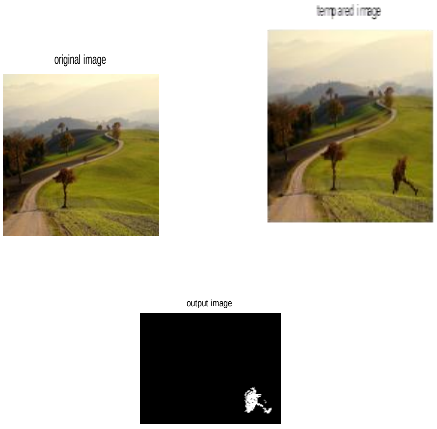


Fig 4(a): image of size 240*161

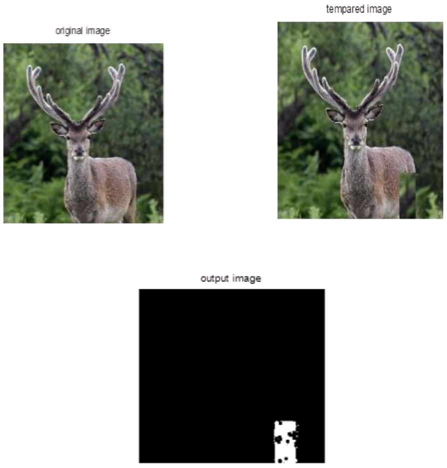
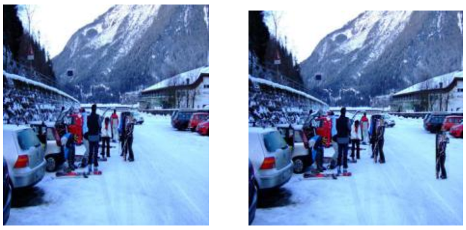


Fig 4(b): Image of size 235*235



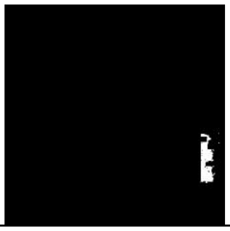


Fig 4(c): Image of size 335*335

From above figures we analyse that less time required for small size of image.and in PCA method large size of image does not detect because PCA detect only small size of image.

Table 2.running time of three detection methods

Images	Our method	Improved DCT	PCA
Image(a)	47.05 s	175.20 s	297.47 s
Image(b)	536.00 s	406.90 s	84.82 s
Image(c)	338.95 s	1178.58 s	-

Again to tast method we take 32*32 and 64*64 duplicated region of images and calculate accuracy of each images, again we add nose in image and blurred also and we analyse that the accuracy of our block representing method is better than other methods even after some post processing like noise adding and blurring.

Table 3.accuracy of detection results of 64*64 duplicated region

Images	Our method	Improved DCT	PCA
deer	71.10	67.17	68.58
Disconnected_shift	53.56	46.91	40.52
Dscf	68.79	39.33	-
Extension	42.16	25.54	40.25
Red_tower	81.27	55.49	70.16
Tree	64.69	61.02	57.91
Truck	58.13	57.64	55.53
CRW	29.55	20.81	24.00

There are also tampered images with post processing operation,such as noise adding and blurring.we currepted the tempered image with some noise adding and blur the same.The following table shows the detection accuracy of our methods which gives better results than other methods with less computational time.

Table 4.accuracy of blurring detection results

Images	Our method	Improved DCT	PCA
Deer	70.01	44.02	69.51
Disconnected_shift	45.02	43.02	42.42
Dscf	72.50	70.50	-
Extension	38.62	35.50	34.68
Red_tower	58.33	52.82	50.23
Tree	51.82	46.87	48.03
Truck	56.20	13.95	23.43
CRW	26.45	59.02	53.14

Above table.4. shows that accuracy of detection results after blurring is also good than other methods.

Table 4.accuracy of noise adding detection results

Images	Our method	Improved DCT	PCA
Deer	68.02	59.48	67.17
Disconnected_shift	61.12	70.71	47.31
Dscf	64.95	3.99	-
Extension	37.59	20.52	30.50
Red_tower	79.24	68.23	75.30
Tree	63.83	59.82	55.93
Truck	62.83	52.51	52.22
CRW	25.49	21.04	23.36

Above table 5. Shows accuracy of noise adding results which is also good than other methods.

Following curves prove that DAR of our method is also increased as compare with other metods. Fig 5(a) shows that DAR of forged image will increased. And Fig 5(b) shows that DAR of forged image which currepted by noise will also increased as compare with other methods.

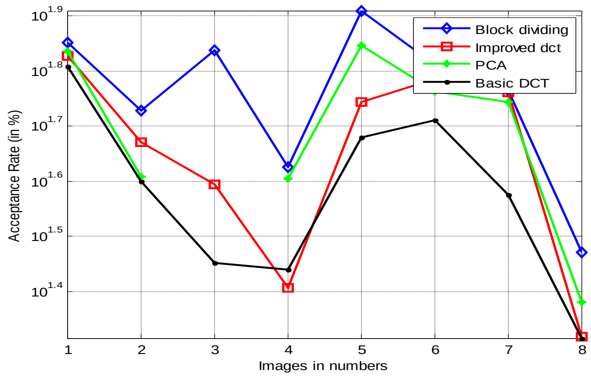


Fig 5(a). DAR.curves for four methods when duplicated region is 64*64 pixels

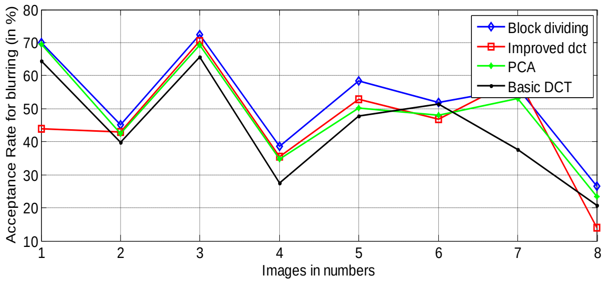


Fig 5(b). DAR.curves blurring for four methods when duplicated region is 64*64 pixels.

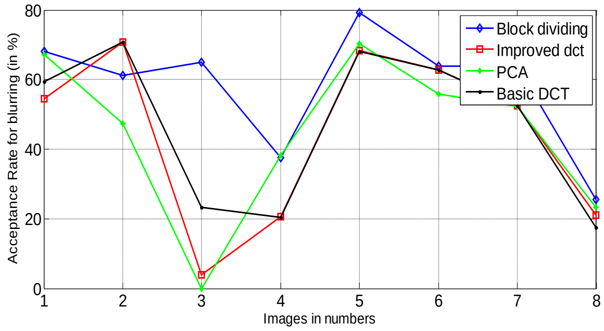


Fig 5(c). DAR.curves noise adding for four methods when duplicated region is 64*64 pixels.

V. CONCLUSION

The copy-move forgery detection is one of the emerging problems in the field of digital image forensics. Many techniques have been proposed to address this problem. One of the biggest issues these techniques had to deal with was, being able to detect the duplicated image regions without getting affected by the common image processing operations, e.g. noise adding and blurring. The other challenge was computational time, which becomes important considering the large databases; these techniques would be used on. An automatic and efficient detection algorithm for copy-move forgery detection is proposed here. It can work without any digital watermarks or signatures information. Compared with previous works, this approach will use less features to represent each block.and improve accuracy with less computational time, again it is robust to various attacks such as multiple copy move forgery,noise adding and blurring.

REFERENCES

1. A. Fridrich, et al., Detection of Copy-move Forgery in Digital Images, 2003.
2. Y. Huang, et al., Improved DCT-based detection of copy-move forgery in images,Forensic Science International 206 (1–3) (2011) 178–184.
3. A. Popescu and H. Farid, Exposing digital forgeries by detecting duplicate image regions, Dept. Computer. Sci. Dartmouth College, Tech.Rep. TR2004 515, 2004.
4. B. Mahdian, S. Saic, Detection of copy-move forgery using a method based on blur moment invariants, Forensic Science International 171 (2007) 180–189.
5. Li Jing, and Chao Shao,” Image Copy-Move Forgery Detecting Based on Local Invariant Feature Journal Of Multimedia,Vol.7,No.1, February 2012.
6. Vincent Christlein,” An Evaluation of Popular Copy-Move ForgeryDetection Approaches”, IEEE Transactions On Information Forensics And Security, 2011.
7. S. Bayram, H.T. Sencar, N. Memon,” An efficient and robust method for detecting copy-move forgery”, in: IEEE International Conference on Acoustics, Speech and Signal Processing, IEEE Press, New York, 2009.
8. X. Pan, S. Lyu,” Detecting image region duplication using SIFTfeatures”, in: IEEE International Conference on Acoustics Speech and Signal Processing (ICASSP),2010, 2010, 1706–1709.
9. Frank Y. Shih and Yuan Yuan,”A Comparison Study on Copy-Cover Image Forgery Detection”,The Open Artificial Intelligence Journal, 2010, 4, 49-54.
10. Preeti Yadav, YogeshRathore, Aarti Yadav,” DWT Based Copy-Move Image Forgery Detection”, International Journal of Advanced Research in Computer Science an Electronics Engineering Volume 1, Issue 5, July 2012
11. Hwel-Jen Lin, Chun-We Wang,” Fast Copy-Move Forgery Detection”, WSEASTransactions on SIGNAL PROCESSING, May 2009.
12. B.L.Shivakumar1 and Lt. Dr. S.SanthoshBaboo,” Detection of Region Duplication Forgery in Digital Images Using SURF”, IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 4, No 1, July 2011.
13. Sevinc Bayram, Taha Sencar, and Nasir Memon, “An efficient and robust method for detecting copy-move forgery,” in Proceedings of
14. Yanjun Cao a,*, TieqangGao,” A robust detection algorithm for copy-move forgery in digital images”,Forensic Science International 214 2012.