Recent Trends in Copy Move Forgery Detection

Malti Puri, Vinay Chopra

Abstract- In today's era due to rapid growth in image capturing and image editing tools it has become very easy to manipulate any image. Whereas detecting whether image has undergone some changes or not has become very difficult. Any manipulation in an image is termed as digital image forgery. There are various kind of digital image forgeries among which most common is Copy-move forgery. The detection of copy-move forgery has become topic of interest of many researchers. Various researches has been done since 2007. In this paper we have discussed some recent techniques to detect copy move forgery in a digital image.

Index Terms: CMFD; Copy-Move forgery detection; Cloning; Tampering; Digital image forgery.

I. INTRODUCTION

In present era due to presence of inexpensive and high-quality digital cameras, there is large amount of digital images all over the world. Digital images play a very important role in various areas such as forensic investigation, surveillance systems, insurance processing, intelligence services, journalism, medical imaging etc. There are various easy to use photo editing tools, with the help of which it has become very easy to alter any image. Moreover, it is impossible to detect with an eye that image is forged or altered. So, there is a need of forgery detection tools. Because images are used widely in various areas. Any image manipulation can become a forgery, if it changes semantic of original image. [10]. It is necessary to check whether image is authentic or not [2].

A. Types of Digital Image forgery

There are many ways to categorize the digital image forgery. However it can be categorized into following main categories: Image Enhancing, Image Retouching, Splicing, Image Morphing and Copy-Move forgery [9]. Following is brief description of different types of digital image forgery are Image Enhancing, Image Retouching, Image splicing, Image morphing and copy move forgery.

Image enhancing involves enhancing an image with the help of Photoshop such as saturation, blur and tone etc. These enhancements don't affect image meaning or appearance. But somehow effects the interpretation of an image [22]. Enhancing involves changing the color of objects, changing time of day in which the image appears to have been taken, changing the weather conditions, Blurring out objects.

Image retouching is basically used to reduce certain feature of an image and enhances the image quality to capture the reader's attention. In this method, an image editor changes the background, fill some attractive colors, and work with hue saturation for toning [22].

In image splicing different elements from multiple images are pasted into a single image. At last, one image is obtained from content of different images.

Revised Version Manuscript Received on 25 January, 2019.

Malti Puri, Scholar, Department of Computer Science & Engineering, DAV Institute of Engineering. & Technology, Jalandhar (Punjab), India.

Dr. Vinay Chopra, Assistant Professor, Department of Computer Science & Engineering, DAV Institute of Engineering. & Technology, Jalandhar (Punjab), India.

Image morphing is defined as a digital technique that gradually transforms one image into another. Transformations are done using smooth transition between two images.

In copy-move forgery one region is copied from an image and pasted onto another region of the same image. Therefore, source and the destination both are same [9, 35]. Copy Move involves copying regions of the original image and pasting into other areas. The main intention of Copy-Move forgery is to hide some information from the original image. Since the copied area belongs to the same image, the properties of copied area like the color palette, noise components, dynamic range and the other properties too will be compatible with the rest of the image [9, 5]. So, the human eye usually has much more trouble detecting copy-move forgeries. Also forger may have used some sort of retouch or resample tools to the copied area so as it becomes even more difficult to detect copy-moved forgery. Retouching involves compressing the copied area, adding the noise to the copied area etc. and re-sampling may include scaling or rotating the image. For example: An image from the crime scene is taken. Figure 1.2 shows the original image and figure 1.1 shows the forged image. Forgery is done to hide some important evidences.

Fig. 1.1 Copy- Move Forged Image

Fig. 1.2 Original Image

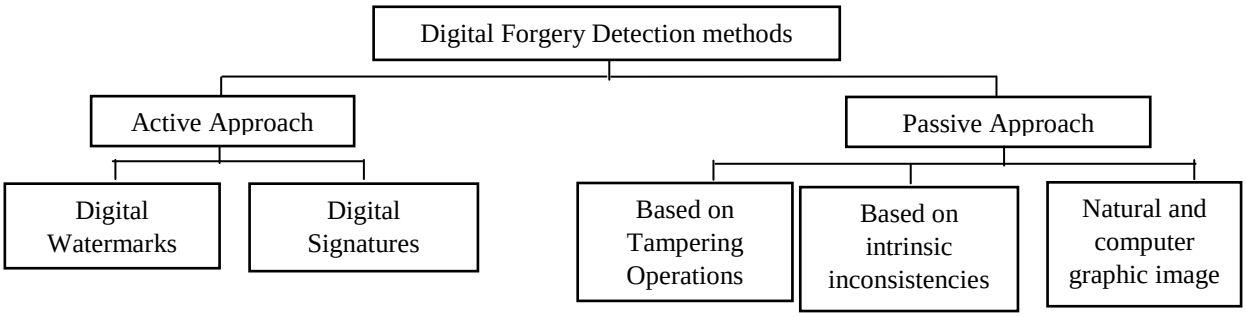


Fig. 1.3 Digital Image Forgery detection Methods [32]

With the availability of low cost and high quality digital cameras and easy methods of sharing the digital images, Digital images have become an integral part of almost every area. So, image authenticity and integrity is a major concern [11]. And there must be techniques to detect whether an image has been forged or not. Authenticity of images cannot be neglected, especially when in case of legal photographic evidence [10]. Digital images play a very important role in areas. Following are some important areas in which integrity and authentication of a digital image is very necessary:

- Medical images are used to prove illness or fitness of a person.
- In courtrooms digital images are used as evidence.
- In e- commerce sites images are essential so that buyer can see what they are buying.
- In class rooms for smart learning.

Digital image forgery detection techniques are mainly classified into two categories active approach and passive approach [2, 16]. Active approach requires a pre-processing step and suggests embedding of watermarks or digital signatures to images [16]. It relies on the presence of a watermark or signature and therefore require knowledge original image. So, it limits their operation. Algorithm/key used to embed the watermark or fingerprint. Any manipulation in the image will impact the watermark and further retrieval of the watermark and examination of its condition indicates whether tampering has occurred. On the other hand passive approach forgery detection does not required knowledge of original image and does not rely of presence of Digital watermark or Digital fingerprint. The passive approach is regarded as evolutionary developments in the area of tamper detection [16]. Digital image forgery detection methods classification is shown in figure 1.3.

B. Copy Move-Forgery Detection Techniques

Copy move forgery detection includes various steps which includes preprocessing, Feature extraction, feature matching, detection of copied regions and post-processing. Feature extraction is the most important step out of all steps. It requires great amount of attention. Following are some techniques for feature extraction during copy move forgery detection techniques [32]:

Moment based feature extraction:

It comes under block-based copy move forgery detection. In moment based feature extraction there are basically three different approaches which are: blur invariant moment, Hu moments (Hu) and Zernike moments (Zernike). In case of blur moments, k–d tree representation is used for feature matching. It can detect forged region with presence of blur and Gaussian noise. This method is also invariant against contrast changes. However its computational time is high. In case of Zernike moment's Euclidean distance is used for feature matching. Zernike moments are robust against JPEG compression and blurring [32, 35]. However, it is weak against forgeries based on scaling operation and affine transformation.

Dimensionality based feature extraction:

It comes under block-based copy move forgery detection. In dimensionality based feature extraction there are basically three different approaches which are: Principal Component Analysis (PCA), Kernel Principal Component Analysis (KPCA) and Singular value decomposition (SVD). PCA is basically a mathematical technique which divided image into coordinate systems, called Eigen vectors. Features are extracted and represented in the form of Eigen vectors. Thus, it reduces the dimensionality. PCA uses Row distance for feature matching. It works well even when noise is present [18, 35]. But it does not work well when blocks are of very small size and when Signal to noise ratio is low. In case of SVD kd-tree and, Euclidean distance both can be used for feature matching. Computational complexity is low as compared to other methods. Robust against various post image processing. However, it is not robust against JPEG compression. Also, it cannot specify that which part is copied and which is pasted. In case of KPCA, Lexicographical sorting is used for feature matching. Higher Precisions and Recalls as compare to PCA-based systems. But it does not work well in case of noiseless images.

Frequency based feature extraction:

Fourier–Mellin Transform (FMT) and Discrete Cosine Transform (DCT) comes under this category. But most commonly used method is DCT. DCT Transforms image into to frequency domain from spatial domain. In frequency domain it can be efficiently encoded. It discards high frequency sharp variations components and thus refines the details of the image. DCT Focuses on the low frequency "smooth variations", holds the base of an image. It also removes redundancy between neighboring pixels. It provides the best compression ratio.

Prepares image for quantization. Quantization is the step during which image is separated into the parts of different frequencies. Less important frequencies are discarded and most important frequencies that remain are used. Hence DCT can pack most information in fewest coefficients [7]. In the DCT algorithm the input image is divided into blocks of size 8x8 or 16x16, DCT coefficient is computed for each block, DCT are then quantized, then quantized coefficients are decoded and corresponding to each bock inverse (IDCT) is computed and at a last is stored as a single image [7]. It can detect the forgery even when the copied area is retouched and even when image is in saved in a lossy format.

Wavelet based feature extraction:

It comes under block-based copy move forgery detection. Discrete Wavelet Transform (DWT) is used. In this feature extraction is done using wavelet transformation. Wavelet transform is basically tool for texture discrimination. Wavelet Transforms are based on small waves called wavelets of varying frequency. Discrete Wavelet Transform is to reduce the size of image at each level. At each level, the image is decomposed into four sub images: LL, LH, HL and HH. LL corresponds to the coarse level coefficients [29]. LH corresponds to vertical, HL corresponds to horizontal and HH corresponds to diagonal components of the image. Usage of DWT for feature extraction reduces the time needed for the detection process. It is robust to common post processing operations. However, Duplicated regions with rotation and scaling cannot be detected.

Keypoint based Method

Unlike block-based method it doesn't work on pixel level, rather it sparsely covered by matched Keypoints. Detection is done on the basis of key points found in the image. These key points are the regions having. Features are extracted from Keypoints mainly using Mainly Scale-invariant feature transform (SIFT) and Speeded up robust features (SURF). Feature vectors are less and thus computational complexity is reduced [2, 10]. Key-point based method works on point level and gives information about single points that are part of the copy-pasted area. It is less accurate as compare to block-based method. Processing speed of key-point based method is faster and takes less computational load. It doesn't Work well in case of pure translation. Keypoint based methods works well in case of geometrical transformations. Keypoint-based methods are sensitive to low-contrast regions. It becomes poor in performance in detecting multiple regions [8].

However, broadly methods for detection of copy move forgery has been categorized into two major categories which are: Key Point Based detection and Block Based detection. In Block based method image is divided into several over lapping blocks. The blocks are compared against each other in order to see which blocks are matched. The regions of the image covered by the matching blocks are the copied and forged regions. In case of Key Point Based method no subdivision of image is done. Rather detection is done on the basis of key points found in the image. These key points are the regions with the high entropy. Both methods differ in only feature extraction rest steps are same.

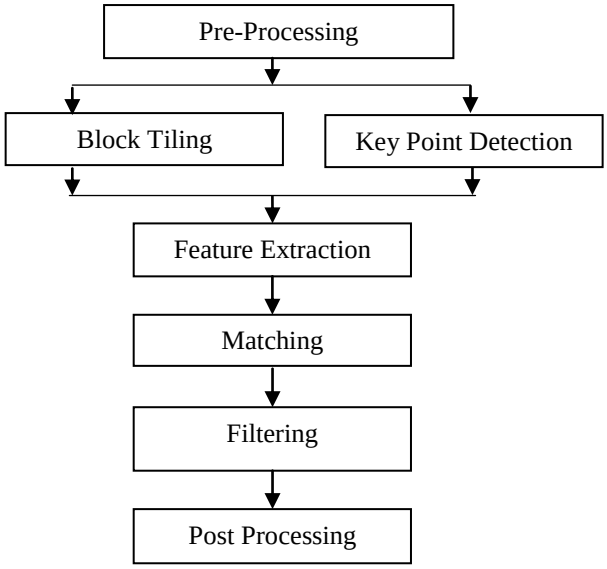


Fig. 1.4 Copy Move Forgery Detection Method [32]

Many researchers have done a lot of research in copy move forgery detection methods. Jessica Fridrich et.al (2003) studied the problem of detecting the copy-move forgery for the first time and presented an efficient copy-move forgery detection method. A DCT-based method was proposed i.e. features were extracted using DCT. The method was proved to be reliable and efficient. It can successfully detect the forged regions even if the copied area is enhanced or retouched [17].

Babak Mahdian et.al (2006) proposed a method based on blur moment invariants to detect copy-move forgery. Firstly image divided into overlapping blocks. Each block is represented using blur moment invariants. To reduce the dimension of the blocks representation principal component transformation (PCA) is applied. After feature extraction feature matching is performed using a k–d tree .After matching forged regions are marked. The experimental results show that proposed method is very efficient [4].

Er. Saiqa Khan et. al (2010) proposed a technique based on discrete wavelet transform (DWT) for detecting copied regions in copy move forgery. Firstly features are extracted by applying Discrete Wavelet Transform to the input image. Then block tiling is done to divide image into overlapping blocks. Feature matching is done using Phase Correlation and forged regions are detected. Experimental results prove that proposed approach has less computational time [13].

Seung-Jin Ryu et. al (2010) proposed a detection method of copy-move forgery using Zernike moments. Zernike moments' magnitude is invariant against rotation therefore proposed method is robust against rotation. It performs really well even in the presence of additive white Gaussian noise, JPEG compression, and blurring. However, does not work well if scaling operations or affine transformations are done in image [29].

Chao et al. (2012), present region duplication detection algorithm which depends on improved DCT and exhibits low computational complexity.

The profound difference between this method and the other DCT-based methods is that here the quantized block is characterized by a circle block. The circle block is then divided into a fixed number of parts, for which the feature vectors are calculated. Euclidean distance between adjacent pairs is calculated after lexicographic sorting of vectors. This method is capable of identifying multiple region duplications and is also robust against blurring and additive noise but it has poor performance with poor image quality [9].

Leida Li et. al (2013) presents a new method for detecting the copy-move forgery. Focus of authors is to solve a main problem that many existing schemes fails to solve and the problem is when the copied region is rotated or flipped before being pasted. They proposed method based on Local Binary Pattern (LBP). Firstly image is divided into circular overlapping blocks. Local binary pattern features are extracted from circular blocks. At last feature vectors are compared to detect forged regions. LBP is rotation invariant hence proposed method is robust against rotation. Experimental results demonstrate that proposed method is robust against JPEG compression, noise, blurring and flipping [21].

Gavin Lynch et. al(2013) proposed an efficient expanding block algorithm. They basically enhanced the existing block based method and named it as efficient expanding block algorithm. Experimental results demonstrates that proposed method accurately detect forged area. Moreover, it can detect forgery even when postprocessing operations like JPEG compression or Gaussian blurring are done on image. It is mainly good at identifying the shape and the location of forged areas [14].

Guzin Ulutas et. al (2013) proposed a method based on Color Coherence. Color Coherence Vector (CCV) is used to determine the similarity among blocks in this method. The vector will designate the coherence of the colors in a region. Experiments show that the method can detect forged regions even if the image is processed by Gaussian Blurring to hide forgery [15].

Chi-Man Pun et. al (2015) proposed a new copy-move forgery detection scheme using adaptive over segmentation and feature point matching. The proposed scheme merge both block-based and Keypoint-based forgery detection methods. First, the proposed algorithm divides the input image into non-overlapping and irregular blocks. After that, the feature points (key-points) are extracted from each block as block features. These the block features are matched with one another to locate forged areas. The experimental results shows that the proposed method can give better results as compare to existing copy move forgery detection methods [10].

Devanshi Chauhana et.al (2016) has done a survey on key-point based methods on the basis of various parameters. They concluded that SIFT is an efficient technique and can detect forgery in a single or multiple regions of an image. It gives goof results in case of both plain copy-move forgery and geometric transformation like scaling, rotation, translation. But SIFT is invariant to rotation, scaling and affine transformation. Also, SIFT give high computational efficiency compared to SURF. But SIFT accuracy is low compared to SURF [11].

Beste Ustubioglu et. al (2016) proposed a method to detect copy-move forgery that can calculate threshold automatically. Threshold is value that is used to compare similarity between feature vectors. Authors use DCT-phase terms to limit the range of the feature vector elements. Benford's generalized law is used to determine the compression history of the input. Unlike existing forgery detection methods the proposed method uses element-by-element equality between the feature vectors. Whereas other methods uses Euclidean distance or cross correlation. Experimental results show that the method can detect forged regions with higher accuracy ratios and lower false negative compared to existing methods [7].

II. RECENT ADVANCES IN AREA OF COPY-MOVE FOREGERY DETECTION

Junlin Ouyang et. al (2017) proposed a method based on convolutional neural network. The proposed method uses existing trained model from large database as ImageNet. Net structures are then slightly adjusted using small training samples. Test image may be identified by the trained model at last. Figure 2.1 shows the overall structure of convolutional neural network based copy move forgery detection method. Convolutional Neural Network is a well-known deep learning architecture, and is a great success in the task of image classification and recognition [18]. In this work authors used the pre-trained model proposed by Krizhevsky et al. from the Caffe CNN library. There are various layers and operators used. Important operators are Convolution, RELU, Normal and Drop out. The convolution layer can be defined as core of convolution neural Network. The kernel of convolution is a filter which can reduce the number of neuron because it is impractical to connect neurons to all neurons in the previous neural Network. RELU is an activation function which can be used by neurons. Pooling operator deals with individual feature channels nearby feature values into one. Thus it can reduce the number of neurons and computation complexity. Common pooling operators include max-pooling or sum-pooling. Max-pooling is defined in equation 1.

$$y_{ijk} = \max\{y_{i'j'k} : i < i' < i + p.j < j' < j + p\} \quad (1)$$

The Normal operator normalizes the feature channels vector of each spatial location and is defined in equation 2.

$$y_{ijk'} = \frac{x_{ijk}}{(k+\alpha \sum_{k \in G(k')} x_{ijk}^2)^{\beta}} \quad (2)$$

Dropout defines nodes that can be ignored and thus dropout from the list.

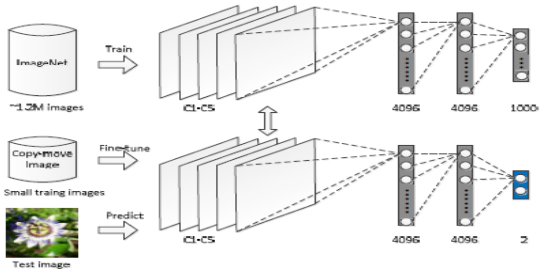


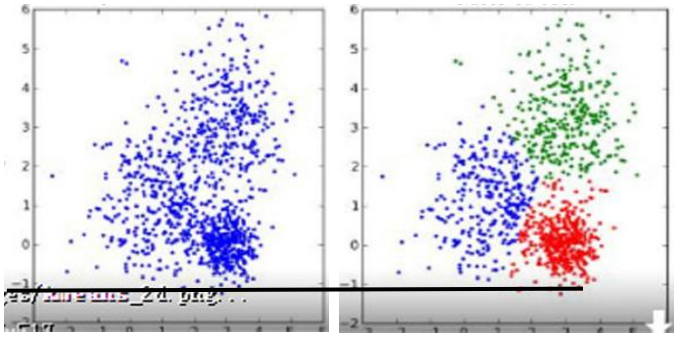
Figure 2.1 Copy-move forgery detection framework based deep convolutional neural network [18]

Algorithm for Copy-move forgery detection framework based deep convolutional neural network [18]:

Step 1: Build copy-move forgery image database. The rectangle block from the upper left corner to the center randomly. The specific process reference experimental section.
Step 2: The parameters of CNN based on Caffe architecture are initialized.
Step 3: Fine-tuning the CNN network.
Step 4: Identify image. If the training process has been completed from the upper fine-tuning step, the identification results.

Although it was a good attempt by researchers to propose such kind of method to detect copy move forgery. But the method does not proved be as efficient. A lot of improvement is needed to implement deep learning and CNN networks for detecting copy move forgeries.

Chao Xiong et. al (2018) proposed a method based on clustering technique. Main aim of study was to reduce detection time and to increase detection accuracy. First of all it uses k- mean clustering to cluster image blocks. Later, the same block, in each cluster is adopted locally sensitive hash matching (LSH) based on the Zernike moments approach. The copy move detection algorithm starts by dividing the image into overlapping blocks. Then, some features are extracted from the overlapped blocks. After extracting the first 12 ZMS forms of the overlapped blocks, the vector set Z [9]. The block diagram is shown in figure2.2.



(a) Unclustered data (b) Clustered Data
Figure 2.2 Clustering in Clustering based CMFD [9]

Algorithm for Clustering based CMFD [9]:

Step 1: Feature extraction using Principle component Analysis. New set of zirconium Zr is generated.
Step 2: Zr is divided into 8 clusters using of k- means clustering.
Step 3: For each subset of ZCI, LSH is used to detect block matching. At the end of this step we get a list of forged candidates.
Step 4: The actual distance between the candidate blocks is determined using equation 3.

M_distance (b_i, b_j) = V ((x_ (I) ^ 2 + (x_j) y_ (I) y_j) ^ 2) >d_1 (3)

If M_distance exceeds a predefined threshold of D1, the corresponding block is considered to be forged.
Step 5: After calculating distance there will be 8 matching lists L1 to L8 that indicates the possible duplicate blocks.
Step 6:RANSACis calculated using equation 4.

R_i = "_i" {scale}, corner _i = RANSAC (l_i) (4)

A list of R's 8 horns and 8 scales is formed at last of this step.
Step 7: Each row in listing R corresponds to a list of matching block li.
Step 8: The points in the two-dimensional space are clustered by clustering using the k-mean.
Step 9:A point that belongs to the pH value of a cluster, which has the largest number of pointscorresponding to the cluster containing the copied moving block, while the other list isdiscarded.

P= {p_h ("_a" scale, corner (_a), "_b" scale, corner, _b)... ("_x" scale, corner, _x)} (5)

Where a, B, and X are clusters that contain replicated moving blocks.
Step 10:All the matching blocks in the rest list are linked together from a list

Lf: L_t = l_a, l_b,..., l_x (6)

Where a, B, and X are clusters that contain replicated moving blocks.
Step 11: Remove the outlier from the list generated in previous step, d Ransac again generates the matching block, if the finalist.

Experiments conducted with the method tested show that the processing time is significantly reduced and the detection accuracy is improved.

V.Thirunavukkarasu et. al [2017] proposed a copy move forgery detection based on Discrete Stationary Wavelet Transform along with Multi Dimension Scaling. Author uses employs Discrete Stationary Wavelet Transform (DSWT) to divide forged image at various frequency bands such as LL, LH, HL and HH at level one. Out of four different bands LL is better for forgery detection as it contains all approximate coefficients of input image. Multi-Dimensional scaling is used to reduce diminishing dimension of feature descriptors. Matching is done using lexicographical sorting, At last forgery is detected [31].Block diagram of process is shown in figure 2.3.

Algorithm of DSWT based copy-move forgery detection method [31]

Step 1: Converting color image into intensity image using equation 7.

LC = 0:.99 R + 0.587G + 0.114 B (7)

Step 2: Applying DSWT to preprocessed image.
Step 3: Extract LL sub-band and divide it into overlapping blocks. For a given input image of size RXC, total blocks should be (R - BS + 1) (C - BS + 1). Where R and C indicate number of rows and columns respectively and BS represents block size and S is calculated using equation 8.

$S = ll\ i_1\text{-}j_1, i_2\text{-}j_2\ ll$ (8)

Step 4: Apply multi-dimensional scaling to decrease feature dimension.
Step 5: Match features vectors using lexicographical sorting.
Step 6: Localize the forged region.

Experimental results shows that this method takes very less computational time. At the same time accuracy is high and it is a reliable method to detect copy move forgery. Feature dimension is reduced to 8. Value of AR is almost 99% and value of FPR is close to 0.

Xiuli Bi et.al (2018) presented a fast Copy-Move Forgery Detection Using Local Bidirectional Coherency Error Refinement. The proposed algorithm can accurately and robustly detect regions of copy-move forgery. Work flow is displayed in figure 2.4.

Firstly a coherency sensitive hashing method is enhanced to establish the feature correspondences in input image. Then a local bidirectional coherency error is proposed to refine the feature correspondences. It is an iterative step Iteration stops when the variation in the local bidirectional coherency error of the host image is not larger than a specified threshold. Iteration stop indicates the stability of feature correspondences. Finally the copy-move forged regions are detected using the local bidirectional coherency error of each feature that we got as stable features at the end of iteration [36].

Algorithm: Local Bidirectional Coherency Error Refinement based CMFD [36].

Input: Image *I*; Feature set F= $\{f_i\}_{i=1}^{MXN}$

Output: feature correspondencesω^*, which indicate the copy-move forgeryregions.

Step1: Create hash tables.
Step 2: Initialize feature correspondence sets ω.
Step 3: $\omega \rightarrow \emptyset$ the initial Local bidirectional coherency error of host image *Err* =0
Step 4: for each feature *if F* **do**
Step 5: obtain *Cands (fi)*via (8)
Step 6: optimize ω_i
Step 7: end for
Step 8: update $\{Err(f_i)\}_{i=1}^{MXN}$
Step 9: if Err/ $\sum_{i=1}^{MXN} \boldsymbol{Err(fi)} \ni [\mathbf{1}-\boldsymbol{th}, \mathbf{1}+\boldsymbol{th}]$
Step 10: Err=$\sum_{i=1}^{MXN} \boldsymbol{Err(fi)}$**,** and then go to step 4
Step 11: end if
Step 12: obtain ω
Step 13: apply morphological operations to ω*for the final detected regions.

The experimental results of Local Bidirectional Coherency Error Refinement based CMFD shows that it is very effective in real time. Moreover, it can achieve good detection rates in presence of various postprocessing as compared to other CMFD methods. The parameter values were F-image: 96.63%, F-pixel: 92.97% and time 74.17 sec.

Bin Yang1 et. al (2017)proposed a method based on novel feature using SIFT to detect copy-move forgery.Main aim was to improve detection in case of images having uniform texture. As existing methods does not perform well if image is having uniform texture. Key-points are detected by using a modified SIFT-based detector. A novel key-points distribution strategy is developed for detecting the key-points. At last, key-points are descripted by an improved SIFT descriptor which is enhanced for the CMFD. Experiments prove that proposed method is quite sufficient in detecting forgeries even if images have uniform texture **[5]**. Block diagram of the novel keypoint based CMFD is shown in figure 2.5.

Steps shown in flow chart are explained as following:

Step I First of all input image is converted into Greyscale from RGB usingstandard color space conversion. After that keypoints are detected.

Step II: Key point detection: SIFT key-points are found by searching for locations that are stable local extreme in the scale space. Keypoints are defined using equation 9.

$$P(x,y,z)=G(x,y,z)*K(x,y) \quad (9)$$

Where G(x,y,z) is a scale variable Gaussian function and is defined using equation 10.

$$G(x,y,z)=\frac{1}{2\pi\sigma^2}e^{-\frac{x^2+y^2}{2\sigma^2}} \quad (10)$$

(x, y) is a spatial coordinate

σis scale coordinate.

The sample point is compared to all its adjacent points. The local extreme point is selected as a key-point. Next, a gradient direction histogram is established. The direction is defined as equation 11 & 12.

$$r(x,y)=\sqrt{((P(x+1,y)-P(x-1,y)))^2+((P(x,y+1)-P(x,y-1)))^2} \quad (11)$$

$$\beta(x,y)=\alpha\tan2((P(x,y+1)-P(x,y-1))/P(x+1,y)-P(x1,y))) \quad (12)$$

Key-points are localized in scale by applying non-maximum suppression in a neighborhood. A fixed threshold λ to remove the low contrast key-points is used in the SIFT detector [5].Flow chart of determining the threshold is displayed in figure 2.6.

Step III Key-points distribution: A novel key-points distribution algorithm is then developed in this step. This step is very important. Because this step helps in ensuring that forgery could also be detected if input image is a texture less image or image having uniform texture. Keypoint distribution involves some steps which are shown in algorithm below:

Step 1: Select a sub-image Sij ($1 \le i \le \lceil M/n \rceil$, $1 \le j \le \lceil N/n \rceil$) from image I.

Step 2: Save keypoints from image I into a list as temp list Lt = {p1 , 1, p1 , 2, …, p2 , 1, p2 , 2,…}.

Step 3: The smallest q percent key-points from list in Lt are eliminated. Q is calculated using equation 13.

$$q=1-\frac{Number\ \ of desired\ \ output\ \ keypoints}{Number\ \ of\ \ total\ \ keypoints} \quad (13)$$

Step 4: After deleting keypoints remaining key-points of Lt are inserted into the output list Lo.
Step 5: Repeat Step 1 to 4 for all sub images.
Step 6: Output the result Lo.

Step IV Key-points description: An improved SIFT descriptor technique is used for keypoint description that uses circular blocks instead of rectangular blocks and thus is rotation invariant.

Step V Key-point matching and forgery detection: At last keypoints are matched to detect and mark forged regions. The ratio of the distance of the closestneighbor fi and the second-closest neighbor fi+1 is compared to a threshold λ.

If constraints given in equation 14 is satisfied the corresponding key-points are regarded matched. Thus forgery is detected.

$$f_i = f_{i+1} < \lambda;\ \lambda \in (0,1) \qquad (14)$$

Experiment results show the robustness of this method against various post processing operations such as rotation, flipping. Scaling etc. Value of TPR is 95.88% and value of FPR is 9.02% and these values very well show how efficient and reliable the method is.

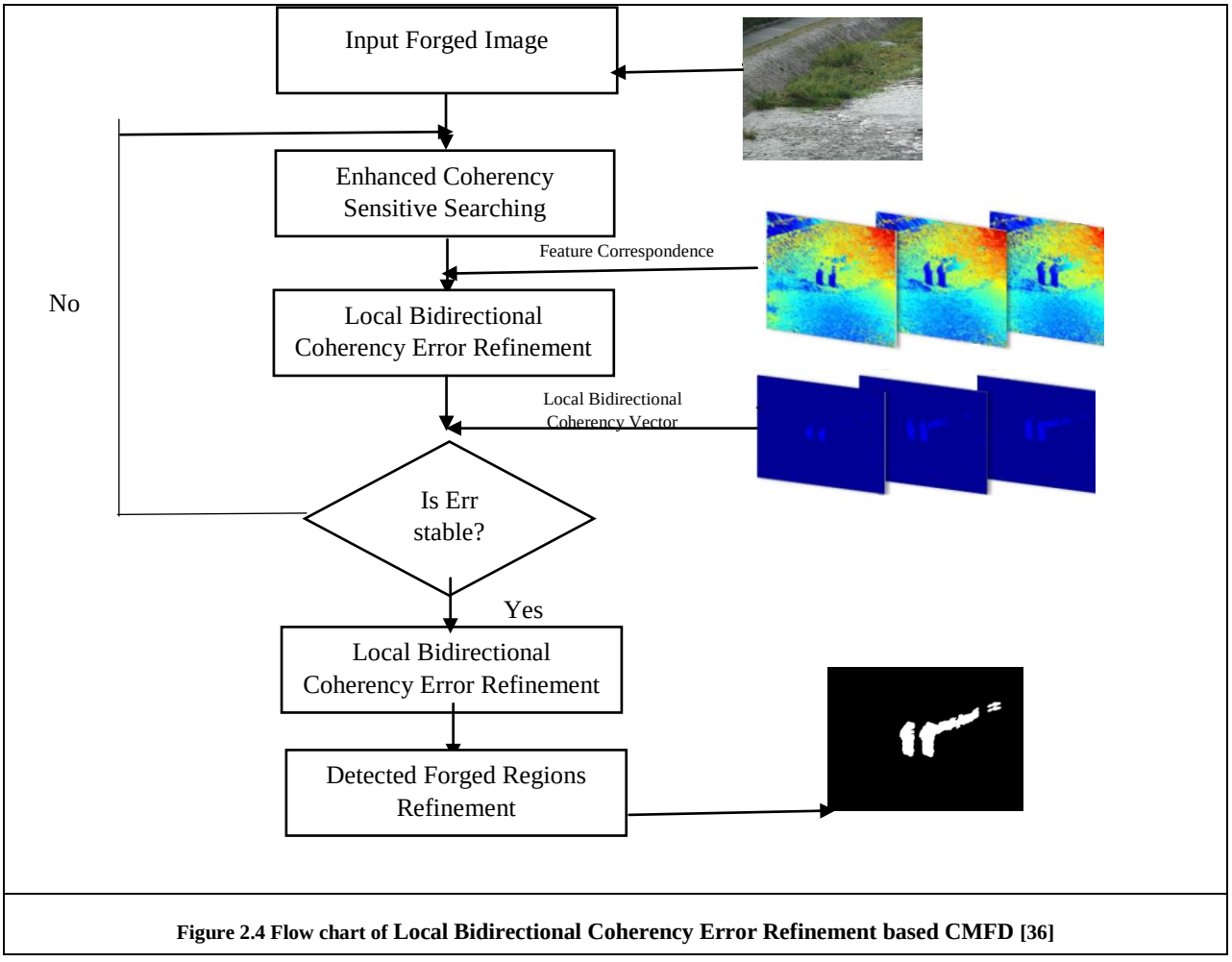


Figure 2.4 Flow chart of Local Bidirectional Coherency Error Refinement based CMFD [36]

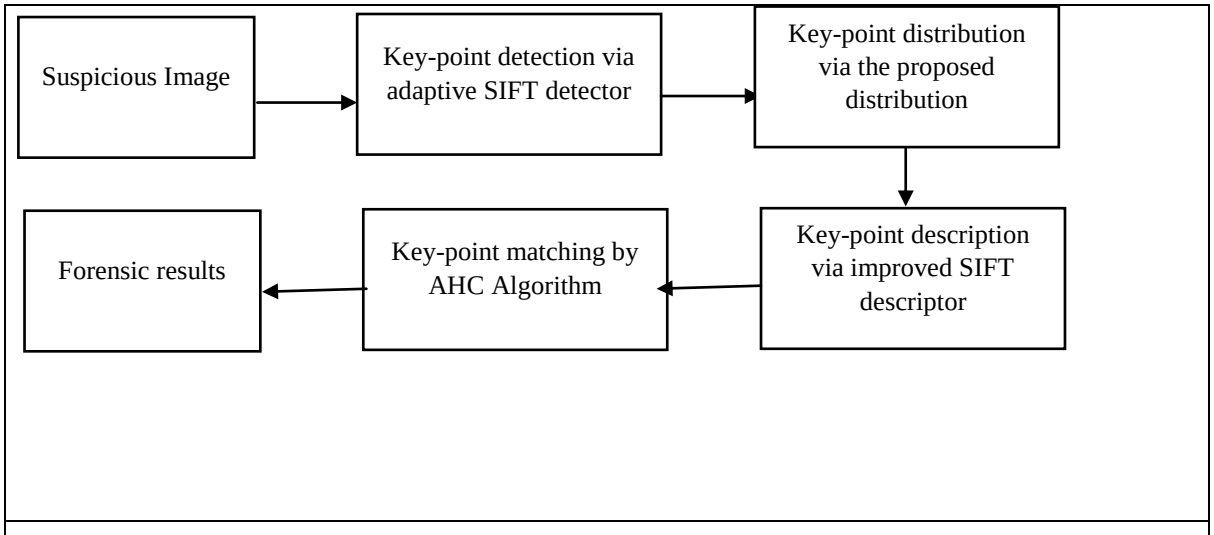


Figure 2.5 Novel keypoint based CMFD [5]

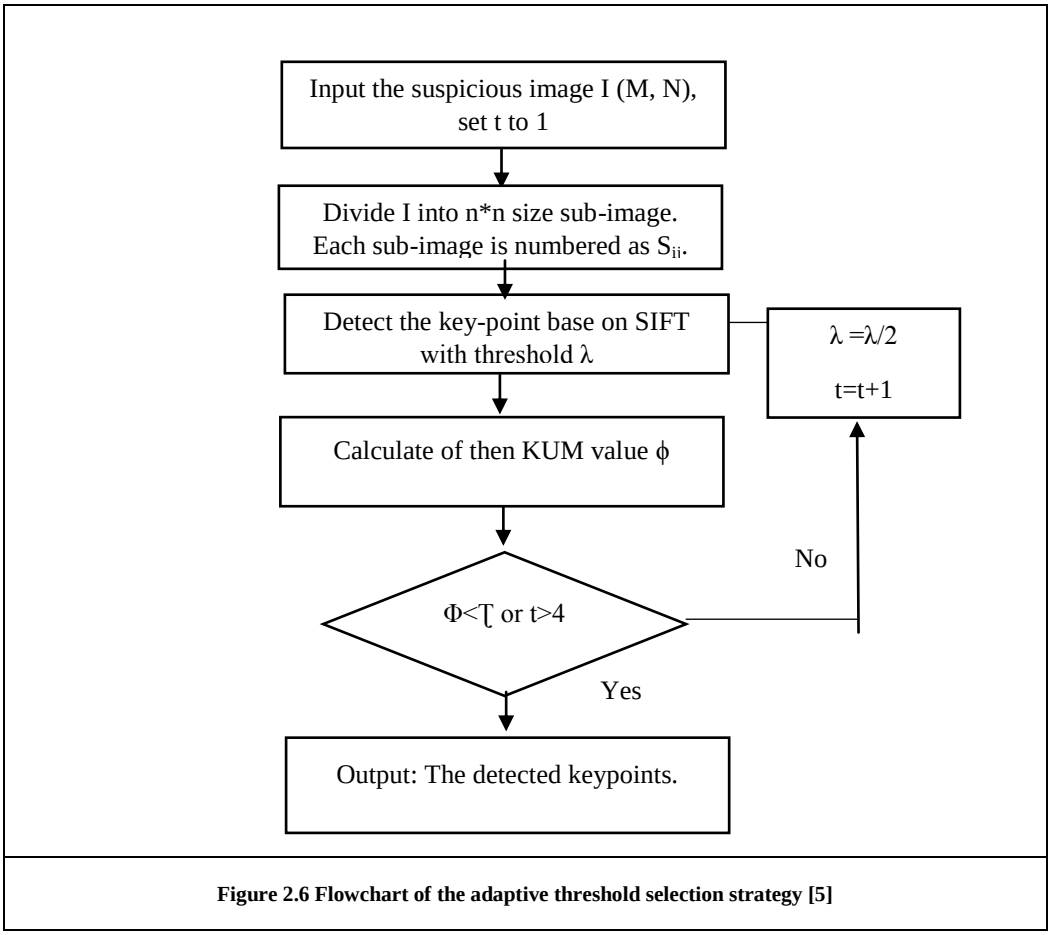


Figure 2.6 Flowchart of the adaptive threshold selection strategy [5]

III. COMPARISON AND KEY FINDINGS

Merits and demerits of existing and recent methods for copy move forgery detection is contrasted in following table.

Paper	Feature Extraction Method	Feature Matching Method	Pros	Cons
[17]	DCT	Autocorrelation	Can detect the forged part even if enhancement or retouching is done in image.	Uniform areas lead to false matches. Does not work well in case of noisy images.
[21]	LBP	Euclidean distance	Robust against blurring, rotation and flipping.	Difficult to detect forgery when the region is rotated at random angles.
[13]	DWT	Phase correlation	Reduces the time needed for the detection and detect exact copied regions.	Does not perform well if postprocessing operations have been done.
[1]	PCA	Row distance	Works well even when noise is present.	Doesn't work well for small sized blocks or low quality images or if Signal to noise ratio is low.
[4]	BLUR	k-d tree representation	Can detect forged region in presence of blur and Gaussian noise. Invariant against contrast changes.	Computational time is high.
[16]	SIFT	Nearest neighbor	Robust against Noise and rotation.	Not capable of detecting forgeries ofsmall-sized regions.
[8]	SURF	g2NN	Efficient in dealing with multiple forged regions.	Does not work well in case of highly textured area.

[29]	Zernike	Euclidean distance	Robust against AWGN, JPEG compression and blurring.	Weak against scaling and other Affine transform postprocessing operations.
[15]	CCV	Euclidean distance	Robust against Gaussian Blurring.	Cannot detect forgery if postprocessing is done.
[7]	DCT- Phase	Element by element equality	Robust against JPEG compression, Gaussian Blurring and AWGN. Calculate threshold value automatically. Higher accuracy ratios and lower false negatives.	Comparatively high processing time.
[36]	Local Bidirectional Coherency Error Refinement	Coherence error	Achieves real-time Effectiveness, good detection results.	---
[31]	DSWT	Reduced feature dimension	Decreased computational Complexity, Higher accuracy, Zero false negatives. Robust against blurred, brightness altered regions.	---
[18]	Deep Learning	CNN Network	Good performance to the Computer generated forged images build using simple copy-move operation.	Time consuming. Is not robust to the copy-move forgery image of real scenario.
[5]	SIFT	Euclidian distance	Robustness against postprocessing operations. Higher accuracy. Improves the invariance to mirror transformation and rotation.	Does not perform in case when regions are undergone nonaffine transformations.
[9]	PCA and clustering	Euclidean distance	Processing time is less. Accuracy is higher.	---

IV. CONCLUSION

Digital images have become integral part of day to day life and are used to present important information. Digital image forgery is very common these days with the availability of editing tools. So, authenticity of image has become major concern. Copy-move forgery is the most common type of forgery these days and has become hot topic for many researchers. A number of detection methods have been proposed since 2007 by researchers. In this paper we have surveyed various researches done in this field and some recent methods for detection of copy- move forgery in the digital images.

REFRENCES

1. Alin C Popescu and Hany Farid, “Exposing digital forgeries by detecting duplicated image regions,”Department of Computer Science, Dartmouth College,Tech. Rep. TR2004-515, 2004, pp. 1-11.
2. Anil Dada Warbhe , R.V. Dharaskar , V.M. Thakare " A Survey on Keypoint Based Copy-paste Forgery Detection Techniques ",Elsevier-1st International Conference on Information Security & Privacy ,2015, Volume 78, pp. 61-67.
3. Ashima Gupta, Nisheeth Saxena, S.K Vasistha, "Detecting Copy move Forgery using DCT", International Journal of Scientific and Research Publications, Volume 3, Issue 5, May 2013,pp. 1 – 4.
4. Babak Mahdian , Stanislav Saic," Detection of copy–move forgery using a method based on blur moment invariants", Forensic Science International, an international journal dedicated to the applications of medicine and science in the administration of justice, Vol.171 No.2-3 , Sep.2007, pp. 181-189.
5. Bin Yang, Xingming Sun, Honglei Guo1, Zhihua Xia, Xianyi Chen, "A copy-move forgery detection method based on CMFD-SIFT", Springer:Multimed Tools Appl, 2017.
6. B.L.Shivakumar, Dr. S.Santhosh Baboo, "Detecting Copy-Move Forgery in Digital Images:A Survey and Analysis of Current Methods", Global Journal of Computer Science and Technology, Vol. 10 Issue 7, September 2010, pp. 61-65.
7. Beste Ustubioglu, Guzin Ulutas , Mustafa Ulutas, Vasif V. Nabiyev," A new copy move forgery detection technique with automatic threshold determination”, Elsevier - International Journal of Electronics and Communications Volume 70, Issue 8, August 2016, pp. 1076–1087.
8. Bo X, Junwen W, Guangjie L and Yuewei D, " Image copy-move forgery detection based on SURF", International Conference on Multimedia Information Networking and Security, 2010.
9. Chao Xiong, Ju Zhu, Yuan Li, Ruxi Xiang,"Image-based forgery detection using big data clustering, Springer: Multimed Tools Appl, 2018.
10. Chi-Man Pun, Xiao-Chen Yuanand Xiu-Li Bi, "Image Forgery Detection Using Adaptive Over-Segmentation and Feature Point Matching", IEEE Transactions on Information Forensics and Security, Volume 10 , Issue 8, Aug. 2015, pp. 1705 – 1716.
11. Devanshi Chauhana, Dipali Kasatb, Sanjeev Jainc, Vilas Thakared, "Survey On Keypoint Based Copy-move Forgery Detection Methods On Image", Elsevier -International Conference on Computational Modeling and Security (CMS 2016), pp. 206 – 212.
12. E. Ardizzone, A. Bruno, and G. Mazzola” Copy-Move Forgery Detection by Matching Triangles of Keypoints”, IEEE Transactions on Information Forensics and Security ,Volume 10 , Issue 10 , Oct. 2015,pp 2084 – 2094.
13. Er. Saiqa Khan, Er. Arun Kulkarni," An Efficient Method for Detection of Copy-Move Forgery Using Discrete Wavelet Transform", International Journal on Computer Science and Engineering, Vol. 02, No. 05, 2010,pp.1801-1806.

14. Gavin Lynch, Frank Y. Shih, Hong-Yuan Mark Liao, "An efficient expanding block algorithm for image copy-move forgery detection",Elsevier:Information Sciences 239, 2013, pp. 253–265.
15. Guzin Ulutas, Mustafa Ulutas, "Image forgery detection using Color Coherence Vector", Electronics, Computer and Computation (ICECCO), Nov. 2013, pp. 107 – 110.
16. Irene Amerini, Lamberto Ballan, Roberto Caldelli, Alberto Del Bimbo,Giuseppe Serra,"A SIFT-Based Forensic Method for Copy–Move Attack Detection and Transformation Recovery", IEEE Transaction on information forensics and security, Vol.. 6, No. 3, Sep.2011, pp.1099-1110.
17. Jessica Fridrich, David Soukal and Jan Lukas, "Detection of copy–move forgery in digital images", Proceedings of Digital Forensic Research Workshop, IEEE Computer Society, August 2003, pp. 55–61.
18. Junlin Ouyang, Yizhi Liu, Miao Liao," Copy-Move Forgery Detection Based on Deep Learning, 10th International Congress on Image and Signal Processing, Biomedical Engineering and Informatics" CISP-BMEI 2017.
19. Kumar Sunil, Desai Jagan, Mukherjee Shaktidev, "DCT-PCA Based Method for Copy-Move Forgery Detection",Advances in Intelligent Systems and Computing Volume 249, 2014, pp 577-583.
20. Kusam, Pawanesh Abrol, Devanand,"Digital Tampering Detection Techniques: A Review", BVICAM's International Journal of Information Technology, Vol. 1 No. 2, 2009, pp.125-132.
21. Leida Li, Shushang Li, Hancheng Zhu,"An Efficient Scheme for Detecting Copy-move Forged Images by Local Binary Patterns",Journal of Information Hiding and Multimedia Signal Processing,Volume 4, Number 1 ,January 2013, pp46-56.
22. M. Buvana Ranjani, R. Poovendran, "Image Duplication Copy Move Forgery Detection Using Discrete Cosine Transforms Method", International Journal of Applied Engineering Research ISSN 0973-4562, Volume 11, Number 4 , 2016, pp. 2671-2674.
23. Minati Mishra, Flt. Lt. Dr. M. C. Adhikary," Digital Image Tamper Detection Techniques - A Comprehensive Study", International Journal of Computer Science and Business Informatics, Vol. 2, No. 1, Jun 2013, pp. 1-12.
24. Mohsen Zandi, Ahmad Mahmoudi-Aznaveh, and Alireza Talebpour, "Iterative Copy -Move Forgery Detection Based on a New Interest Point Detector",IEEE Transactions on Information Forensics and Security,2016, pp.1-14.
25. Ms.Kavita V.Hulmukhe, Prof. Dr.S.S.Sane, Ms. Alpana A. Borse,"Exploring Duplicated Regions in Natural Images",International Journal of Computer Applications, 2011.
26. Osamah M. Al-Qershi and Khoo Bee Ee,"Passive Detection of Copy-Move Forgery in Digital Images: State-of-the-art" Forensic Science International, Volume 231, Issue 1, Sep 2013, pp. 284-295.
27. Pameli Mukherjee, Saurabh Mitra"A Review on Copy-Move Forgery Detection Techniques Based on DCT and DWT", International Journal of Computer Science and Mobile Computing IJCSMC, Vol. 4, Issue. 3, March 2015, pp.702 – 708.
28. Rahul Dixit and Ruchira Naskar,DyWT based Copy-Move Forgery Detection with Improved Detection Accuracy",2016 3rd International Conference on Signal Processing and Integrated Networks (SPIN), pp. 133-138.
29. Seung-Jin Ryu, Min-Jeong Lee, and Heung-Kyu Lee"Detection of Copy-Rotate-Move Forgery Using Zernike Moments",Springer Proc. Int. Workshop Information Hiding, 2010, pp. 51–65.
30. Shi Wenchang, Zhao Fei, Qin Bo, Liang Bin, "Improving image copy-move forgery detection with particle swarm optimization techniques", China Communications, Volume 13, Issue, 1, Jan 2016, pp. 139 – 149.
31. Thirunavukkarasu, J. Satheesh Kumar, Gyoo Soo Chae, J. KishorKumar," Springer: Non-intrusive Forensic Detection Method Using DSWT with Reduced Feature Set for Copy-Move Image Tampering", Wireless Pers Commun, July 2017.
32. Vincent Christlein, Johannes Jordan "An Evaluation of Popular Copy-Move Forgery Detection Approaches", IEEE Transactions on information forensics and security, 2012, pp. 1-26.
33. Vivek Kumar Singh and R.C. Tripathi, "Fast and Efficient Region Duplication Detection in Digital Images Using Sub-Blocking Method", International Journal of Advanced Science and Technology, Vol. 35, October 2011, pp. 93-102.
34. Weihai Li and Nenghai Yu, "ROTATION ROBUST DETECTION OF COPY-MOVE FORGERY", Proceedings of 2010 IEEE 17th International Conference on Image Processing, 2010, pp.2113-2116.
35. Xiaomei Quan, Hongbin Zhang, "Copy-Move Forgery Detection in Digital Images Based on Local Dimension Estimation" Cyber Security, Cyber Warfare and Digital Forensic (CyberSec) International Conference, June 2012, pp.180-185.
36. Xiuli Bi, Chi-Man Pun, "Fast Copy-Move Forgery Detection Using Local Bidirectional Coherency Error Refinement", Elsevier: Pattern Recognition, March 2018.