Study and Analysis of Copy-move Forgery Detection with Local Binary Pattern Method

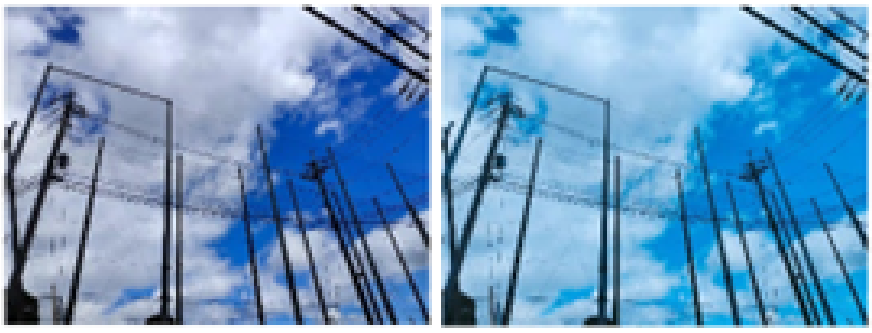
JINGJING RAO[1], Songpon TEERAKANOK[2], and TETSUTARO UEHARA[1]

[1]Ritsumeikan Daigaku
[2]Mahidol University

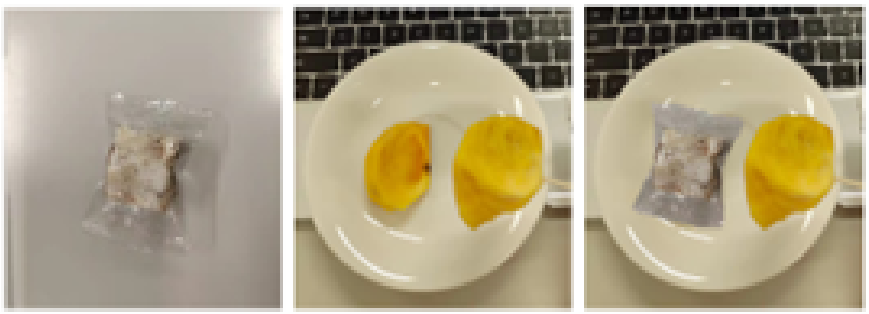
November 7, 2022

Abstract

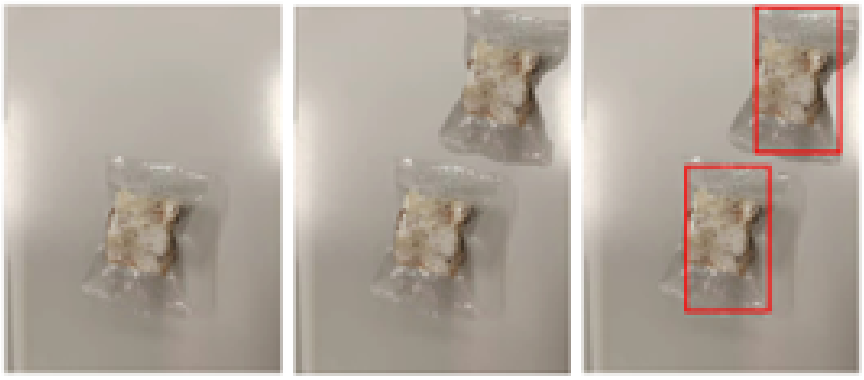
With the advancement of technology, new problems and challenges also follow, among which the more serious problem is media forgery. Forged media information brings a lot of inconvenience to life. It is difficult to distinguish the truth from the false. In this article, various types of forgery are listed and elaborated with a focus on the copy-move forgery category, the study and research involving copy-move forgery(CMF) detection techniques using the Local Binary Pattern (LBP) are presented. The technical review of recent state-of-the-art LBP-based is provided.



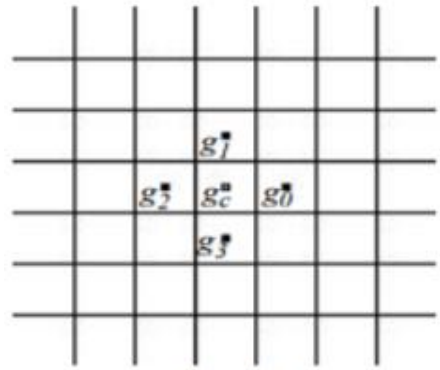
Retouching: Original image (a) **Forged image (b)**



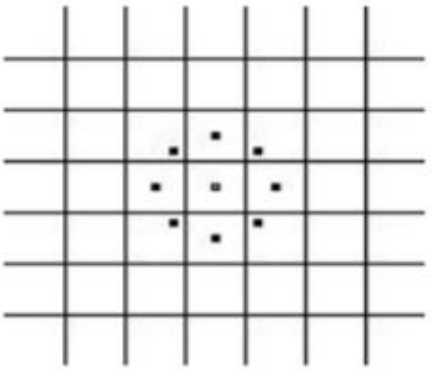
Splicing: Original image (a) **Original image (b)** **Forged image (c)**



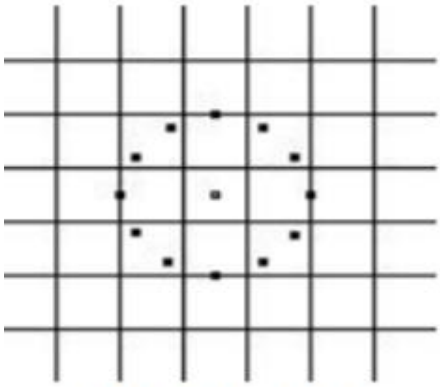
Copy-move: Original image (a) **Original image (b)** **Forged image (c)**



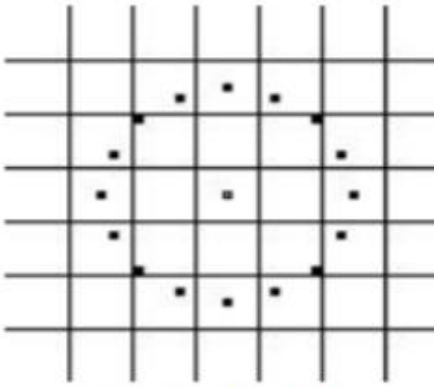
(P=4,R=1.0)



(P=8,R=1.0)



(P=12,R=1.5)



(P=16,R=2.0)

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.DOI

Study and Analysis of Copy-move Forgery Detection with Local Binary Pattern Method

JINGJING RAO [1], SONGPON TEERAKANOK[2], AND TETSUTARO.[3]

[1]Graduate School of Information Science and Engineering, Ritsumeikan University, Kusatsu 525-8577, Japan
[2]Faculty of Information and Communication Technology, Mahidol University, Nakhon Pathom, Thailand
[3]College of Information Science and Engineering, Ritsumeikan University, Kusatsu 525-8577, Japan

Corresponding author: Jingjing Rao (e-mail:raojingjing@cysec.cs.ritsumei.ac.jp).

ABSTRACT With the advancement of technology, new problems and challenges also follow, among which the more serious problem is media forgery. Forged media information brings a lot of inconvenience to life. It is difficult to distinguish the truth from the false. In this article, various types of forgery are listed and elaborated with a focus on the copy-move forgery category, the study and research involving copy-move forgery(CMF) detection techniques using the Local Binary Pattern (LBP) are presented. The technical review of recent state-of-the-art LBP-based is provided.

INDEX TERMS Copy-move, LBP, Keypoint-based, Block-based

I. INTRODUCTION

Advancement in today's technology bring forth new challenges and issues. One of the most serious issues is the problem of media forgery. Fake media forged with malicious intention can not only deceive/mislead people and cloud their judgements, but also cause a negative impact on the society. With the help of easy-to-use media manipulation tools and software, creating a realistic fake image or video is no longer a difficult task.

Recently, there is an increasing of cases reported regarding the use of tampered media in public channel. A classic yet an excellent example of using fake media to deceive the public is the use of fake photo during US presidential election in 2004. Figure 1 shows the picture of Bush that was transplanted to the target image to create counterfeit information. Although the fake image appeared in figure 1 is not very realistic, however, it serves as a very good example of how adversaries can interfere with decision making of people by providing false information.

There are several techniques used by attackers to create a realistic forged media. For digital image, the tampering techniques can be divided into three primary categories: retouching, splicing and copy-move forgery (CMF)

Retouching refers to the image manipulation techniques in which some features or small details within the target image are enhanced or concealed. In general, not only retouching can be used to conceal some information and convey falsified information, but it is also a commonly used technique to create images for advertisement and commercial purposes [1], [2].

FIGURE 1. The use of fake image during US presidential election in 2004.

Splicing [1], on the other hand, refers to the combining of parts of images from two (or more) different sources to create a forge image. Utilizing splicing technique, the attacker can create a counterfeit information or evidence to trick people, create misunderstanding or to avoid being suspected during criminal investigation. Lastly, copy-move forgery (CMF) [2] involves copying parts for images and then replace them onto the same image. This type of attack is good for emphasizing/exaggerating or hiding some details within the target picture. Figure 2 shows picture of image forgery using retouching (top), splicing (middle) and copy-move (bottom) techniques respectively.

To detect CMF, this type of forgery requires the detection methods that can find matching between original parts of the image and the tampered areas. Since the attacker may utilize some transformation techniques to remove traces and make the forged image looks more realistic, the detection mechanisms should robust against commonly used transformation techniques: i.e., blurring, scaling and rotation. Regarding techniques for CMF detection, local binary pattern (LBP) is a widely used feature extraction techniques in fields of image analysis, computer vision, and pattern recognition. The technique produces extracted features with high discriminating capability, while requiring low computational cost and complexity. Currently, there are several extension and variation of LBP-based techniques [3]–[10]. In this paper, the study and research involving CMF detection techniques using local binary pattern (LBP) is presented. The technical review of recent state-of-the-art LBP-based (from 2010 to 2022) is provided.

II. COPY MOVE FORGERY DETECTION (CMFD)

Copy-move forgery detection (CMFD) techniques can be roughly divided into two main categories: active and passive methods.

Active CMFD methods [11]–[13] rely on an additional piece of information embedded into the digital image at the time of creation. This information serves as a mean to verify the integrity of the image. Tampering any part of the target image protected using this method will corrupt the embedded data making it noticeable during verification process. In term of digital investigation, although this type of technique yields very high detection accuracy, the number of its application is very limited due to the need for additional information. Digital watermarking is the most common application in this category.

Passive approach, on the other hand, rely on nothing but the target image itself. Without additional information, most CMFD techniques search for inconsistencies and redundancies of some information which should not appear in typical digital image. These residual artifacts are the key to detect the manipulation in the suspect digital image and to locate the tampered areas inside. Since passive approaches do not require the use of additional data, this type of detection methods usually have wider range of application. In this paper, we will focus on the LBP-based passive CMFD techniques. The following subsections 2.1 and 2.2 present a classification of passive CMFD techniques and common processes for CMFD respectively.

A. TYPES OF CMFD TECHNIQUES

In this paper, we divided passive CMFD techniques into four subcategories: block-based, keypoint-based, segmentation-based, and deep learning-based approaches.

Block-based techniques refers to the detection method in which the target image is first divided into small overlapping (i.e., sliding windows) or non-overlapping blocks [14]. The shape of these blocks can be square, rectangular, circular or any shapes depending on the algorithm. From each block, feature vectors will be generated using feature extraction techniques. These feature vectors will be later used during the matching process to identify and locate the tampered area.

Instead of processing image information as blocks, keypoint-based approaches utilize algorithm to detect points of interest (so-called "keypoint") within the target image [15]. These keypoints represents objects within the image. Example of some commonly used keypoint detection algorithms include SIFT [16]–[18], SURF [19]–[21] and KAZE [21], [22]. By extracting features from each keypoint and matching these feature vectors, we can locate the tampered areas within the target digital image.

Segmentation-based approaches split the target image into several non-overlapping segments [23]. The segment division process depends on some key features (such as color, texture, and shape) to determine the size and border of each segment. Typically, areas of image containing similar features and located next to each other will be group as one segment. Each segment, however, should still show obvious differences between different segments. Next, feature extraction techniques, e.g., noise estimation and histogram, can be applied to create distinctive feature for each segment.

Currently, most traditional detection approaches mentioned earlier are designed to deal with only one type of tempering techniques. This limits their range of application and render them useless against some combination attacks in which the adversaries simultaneously use more than one type of tampering techniques to create a forge media.

Unlike traditional approaches, the successful application of deep learning technology in various fields (computer vision and image processing, for example) shows promising potentials for CMFD problem. Some research and studies also propose the use of deep learning for recognition of image tampering/modification [24]. Regarding the field of deep learning, the problem of passive image forensics can be viewed as the combination of object recognition and anomaly detection problems [25]–[27]. Figure 3 shows an overview and classification of state-of-the-art CMFD techniques.

B. CMFD PROCESS

Generally, CMFD process can be roughly divided into six primary steps. Given a target digital image, the process of CMFD starts by first applying pre-processing technique to the image. Color space conversion is considered one of the most popular techniques in this step. A digital image with RGB color space is often converted to other color spaces, such as Grayscale, LAB, YCrCb, HSV and CIE.

Next, a block division or keypoint detection algorithm is then applied to the target image resulting in a set of overlapping blocks or a set of keypoint information which will later be fed into feature extraction algorithm.

Step 3 covers the use of feature extraction techniques to generate feature vectors from a given set of blocks or keypoints information. A good feature extraction technique that is robust against various types of transformation (e.g., ro-

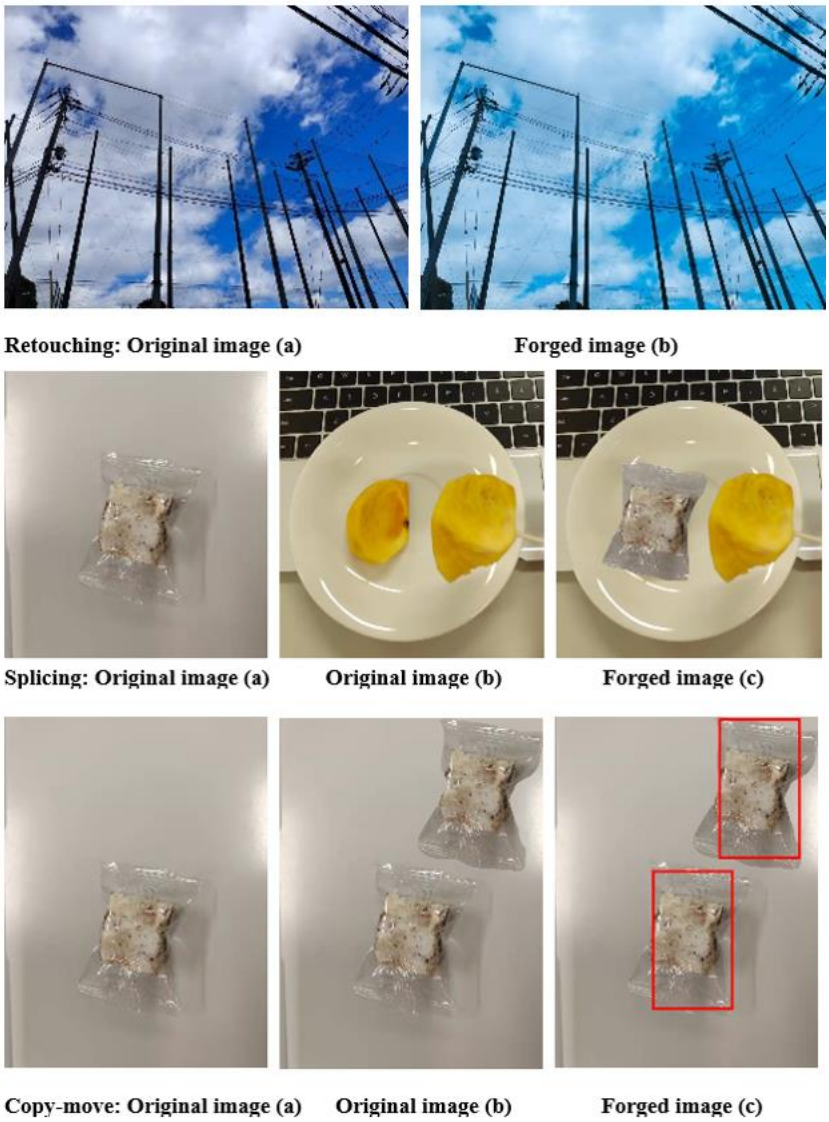


FIGURE 2. Type of tamping image (From up to down: retouching, splicing, and copy-move; First row: original image, tamping image; Second row: original image A, original image B, tamping image; Third row: original image, tamping image, detected result)

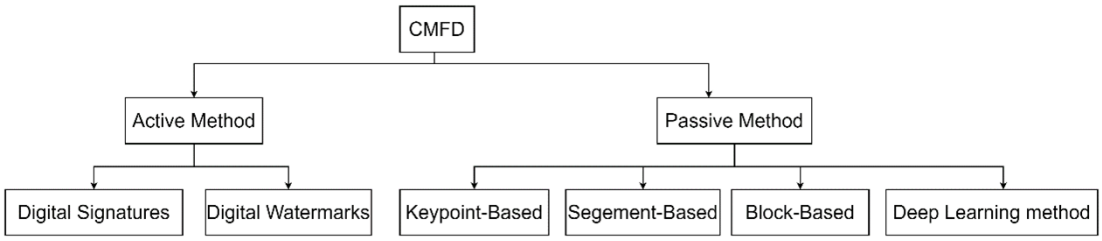


FIGURE 3. A classification of copy-move forgery detection techniques.

tation, scaling, etc.) is a key factor to make the whole CMFD process a success. There are several ways to extract feature from a block or a keypoint retrieved from the previous step. Among them, some commonly used techniques are discrete cosine transform (DCT) [28], discrete wavelet transform (DWT) [29], Fourier transform [30], principal component analysis (PAC) [31], moment-based approaches (for example, Hu [32], Zernike [33], Krawtchouk [34], or PCET moments

[35]), and local binary pattern (LBP).

After successfully extract feature vectors from the target image, the matching algorithm will then use this information to look for pairs of vectors containing similar values or patterns. Some measuring method, such as Euclidean or Manhattan distance [36], can be used to estimate the similarity between two feature vectors against a static (pre-defined) or dynamic threshold. Since this step of CMFD usually take long time, some research incorporates sorting algorithm to speed up the matching process.

Next, the post-processing techniques is applied to enhance the matching results obtained from the previous step. This step is optional that is usually used to eliminate false matches (false positive results) from the matching output. Random Sample Consensus (RANSAC) [37] is a commonly used technique in this step.

Lastly, localization is the step that is responsible for marking or locating the tampered region for better visualization of the output. During this step, the tampered areas within the target image will be highlighted, making it much easier for forensic practitioners to interpret and make a decision. The overall CMFD process is shown in figure 4.

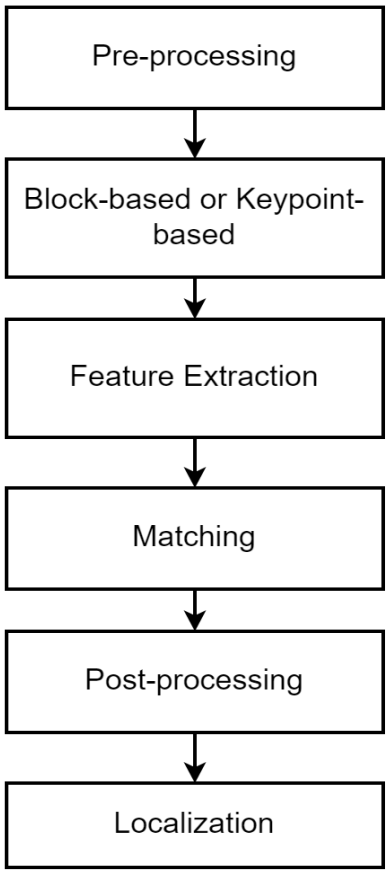


FIGURE 4. A flowchart demonstrating steps to perform Copy-move Forgery Detection

III. LOCAL BINARY PATTERN

Local binary pattern (LBP) is a visual descriptor used to represent local features within a digital image. This technique is a useful technique for classification problems in the field of machine vision. Proposed by T. Ojala, M. Pietikäinen, and D. Harwood [3] in 1994, LBP is a robust technique with its features provide significant advantages in term of both gray scale invariant and rotation invariant properties. Since the calculation of LBP feature is simple yet efficient, it has become of the most commonly used techniques in the field of machine vision with a wide range of applications. Advantages of LBP method can be summarized as follows.

1) Low computational complexity
2) No training/learning period required
3) Light invariance
4) Easy to implement

A. LOCAL BINARY PATTERN

The original LBP operator is defined over a square of 3x3 pixels containing a central and its surrounding pixels. Using the gray scale value of the center pixel as a threshold, each surrounding pixel is quantized. This quantization process produces a binary (0 or 1) output. If the pixel value is greater than the threshold (i.e., value of the center pixel), it will yield 1 as a result; otherwise, the quantization will result in 0.

The binary pattern is then formed by connecting binary value around the central pixel in a counterclockwise rotation starting from a pixel of the positive x-axis. This series of binary digits are converted into decimal to create the LBP value representing the center pixel. This LBP value will be used to represent the texture information of the area.

The LBP operations are defined as follow:

$$LBP(x_c, y_c) = \sum_{p=0}^{P-1} 2^p (i_p - i_c) \tag{1}$$

$$s(x) = \begin{cases} 1 & if \quad x \geq 0 \\ 2 & else \end{cases} \tag{2}$$

(x_c, y_c)represents coordinate of the center pixel, while i_c and i_p indicate brightness levels of the center pixel and each neighboring pixel respectively. Lastly, $s(x)$ represents a quantize function giving 1 as an output if i_p is greater than i_c,and 0 otherwise.

Although, the method of applying LBP operator on a 3×3 square pixels is appeared to be very simple, it, however, come with two significant disadvantages. First, the 3×3 pixels is very small making this approach is not an optimal choice for representing textures of larger scales. Another drawback involves to the use of rectangular shape matrix which is not suitable for producing rotation-invariant features.

B. ROTATION-INVARIANT LOCAL BINARY PATTERN

To reduce the impact of rotation within the target image, Ojala et al. [4] proposed a rotation-invariant texture classification technique using LBP. In this work, the rectangle of

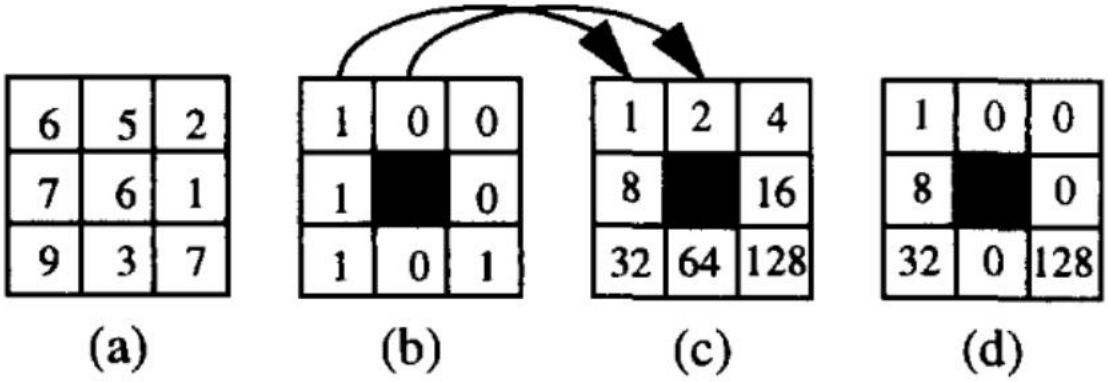


FIGURE 5. Example of calculating LBP descriptor representing a 3x3 pixel square [3]

3×3 pixels is replaced with a circular area of pixels of any size (with a radius, R). As a result, the circular LBP operator (denoted as $LBP_{P,R}$) containing P sampling points in a circular area with the radius of R is introduced.

Using the circular LBP, a rotation-invariant LBP value can be easily calculated. First, for all P samplings inside the given circular area of the image, the value of each sampling (i.e., an image pixel) is quantized into binary output 0 or 1. With all quantized pixel values, they will form a bit string (i.e., binary pattern) with the length of P.

Next, a rotation-invariant is derived from the binary pattern obtained from the previous step. By repeatedly performing right circular shift on this binary pattern, the pattern having minimum value will be used as the final LBP value that represents the entire circular area. Figure 7 illustrates the process of generating rotational-invariant LBP value. Also, a mathematical expression of the circular LBP technique is shown in (3).

$$LBP^{ri}_{P,R} = min\left\{ROR(LBP_{P,R}, i)|i = 0, 1, ..., P-1\right\} \tag{3}$$

According to (3), $ROR(x, i)$ represents a bitwise right circular shift on the binary string x by i positions.

C. UNIFORM LOCAL BINARY PATTERN

In order to further improve the rotation invariance performance of the LBP feature descriptor and further reduce its feature dimension, on the basis of the original LBP descriptor, rotation invariant LBP descriptor, and uniform LBP descriptor, Ojala et al. [4] proposed rotation invariance uniform LBP descriptor. Based on the rotation-invariant LBP descriptor, the rotation-invariant LBP mode is further divided into uniform rotation-invariant mode and non-uniform mode.

Due to the development of technology, the original LBP method is difficult to meet the current needs, so a variety of extended LBP methods have appeared. As shown in Table 1, not all are listed, only some common methods which used in copy-move forgery detection

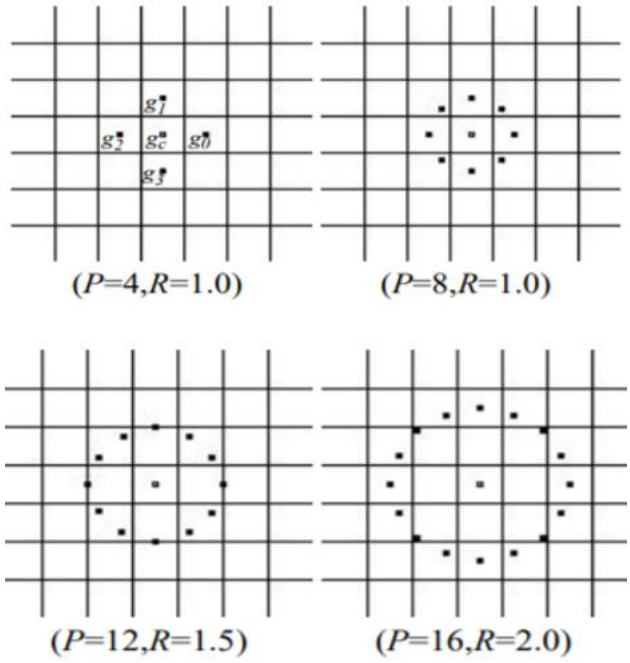


FIGURE 6. circular LBP (image source form [4])

IV. CMFD USING LBP

This section reviews and analyzes some copy-move forgery detection using local binary pattern or its extended mode. It is mainly divided into one type is the image passive method based on the traditional method, and the other type is the image passive method based on the deep learning method or machine learning.

A. TRADITIONAL METHODS

Since the local binary pattern has the above shortcomings and advantages, many researchers combined it with other methods to detect the forgery part.

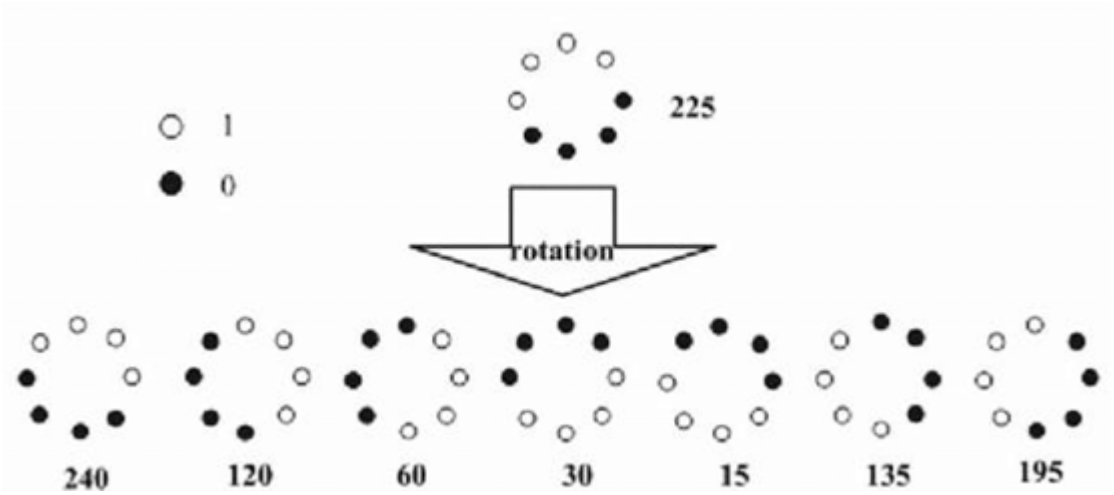


FIGURE 7. A diagram showing the use of right circular shift on the binary string to calculate rotation-invariant LBP feature (image source from [5]))

In Davarzani et al. [38] proposed a method called multiresolution local binary patterns(MLBP) which including basic form of LBP,$LBP_{P,R}$,rotation uniform LBP,$LBP^{ri}_{P,R}$,uniform LBP,$LBP^{u2}_{P,R}$, rotation invariant uniform LBP,$LBP^{riu2}_{P,R}$,and rotation invariant variance measures, $VAR_{P,R}$.First, the input image divided in overlapping blocks of B×B pixels. In the feature extraction step, they used MLBP features with two, three, and four types of LBP operators. In other words, a variety of LBP operators of varying parameters (P, R) are applied to every block to extract the features. So, for each block, there will be two, three, and four vectors-the number is based on the number of LBP operator types used. Then, for the obtained N-dimensional feature vector, they use lexicographical sorting and k-d tree at the same time to reduce more time and improve accuracy in the matching step. Finally, using Random Sample Consensus (RANSAC) algorithm to remove the false matches. The experimental results show that when no disturbance is added to the image, the size of the replicated area and the type and number of MLBP operators have very little effect on the average detection accuracy. However, for small-sized fake areas, DCT [8]'s results are slightly better than their proposed method and believe that the reason for this situation is that the use of the RANSAC algorithm to eliminate mismatch errors leads to a major error in the recall and accuracy of the small size fake areas. At the same time, because the proposed method uses multiple features to represent each image block, its average running time is longer than that of the SIFT [51] method, although the computational complexity of the LBP operator is lower.The author claims that the proposed method can detect repeated regions with common post-processing operations, including scaling, JPEG compression, Gaussian blur and AWGN, and can detect multiples of 90 degrees and different rotation angles, up to 208 degrees, However, it is not possible to detect repeated regions with arbitrary rotation angles, and this method is still time-consuming for forgery detection in high-resolution images.

Compared with the method of Davarzani et al. [38], the method proposed by Kaur et al. [39] is simpler. In Kaur et al. [39], firstly input image is divided into overlapping blocks. Features of the small blocks are extracted by making use of the Local binary pattern texture method. Further blocks are lexicographically sorted, and lastly duplicated blocks are identified utilizing the similarity criterion and Euclidean distance threshold. They claim that the main aid of this paper is that the given scheme is robust not only to the traditional signal processing operations but additionally to the rotation and flipping. A deficiency of the presented scheme is that when the region is rotated by general angles, it is arduous to detect the forgeries.

S. Sharma, et al. [40] proposed a copy-move forgery detection using center symmetric local binary pattern (CSLBP), CSLBP is a variant of LBP proposed by [7] to obtain a shorter LBP histogram and make LBP more stable to noise. For this method, the algorithm is developed for monochrome images only, therefore, at first, they converted input image into gray scale image, and the low pass Gaussian filter is used to extract low-frequency components of the image, then divided in overlapping blocks of $B \times B$ pixels. For feature extraction, they applied uniform rotational invariant $CSLBP_{N,R}$, to every block for getting features. The expression for the uniform rotation invariant CSLBP is given below:

1) CSLBP:

$$CSLBP(x_r, y_r) = \sum_{i=0}^{\frac{n}{2}-1} s(g_i - g_{i+\frac{n}{2}}) \quad (4)$$

$$s(z) = \begin{cases} 1 & \text{if } z \geq 0 \\ 0 & \text{Otherwise} \end{cases} \quad (5)$$

Where, the g_i represents the gray value of neighbor pixels.

2) Rotational invariant CSLBP:

$$CSLBP^{ri}_{N,R} = min\left(ROR\left(CSLBP_{N,P}, i\right)|i = (0, 1, ..., N)\right) \tag{6}$$

Where, function $ROR(z, i)$ represents circular bitwise rotation of sequence z by i steps.

3) Uniform rotation invariant CSLBP

$$CSLBP^{riu2}_{N,R} = \begin{cases} N+1 & \text{Otherwise} \\ \sum_{i=0}^{N-1} s(g_i - g_{i+\frac{n}{2}}) & U(CSLBP_{N,R}) \leq 2 \end{cases} \tag{7}$$

$U(CSLBP_{N,R})$ is the number of bitwise transitions.

They set two thresholds: frequency shift threshold and Euclidean distance threshold to obtain matching blocks, and finally, apply morphological openings to fill the holes in the marked area and remove isolated points. They claim that the proposed method can identify forged areas up to 12×12 pixels under the influence of AWGN and Gaussian blur, and all other mentioned technologies cannot detect these areas.

While D. M. Uliyan et al. [41] also used the CSLBP method, but they proposed a segmented-based method, combining Hessian features and a center-symmetric local binary pattern (CSLBP). To reduce computational complexity, the authors choose to segment the input image into different regions by normalized cut (Ncut) segmentation, for each segment, localizing the local interest points by Hessian method, and extracting CSLBP features, and combine these two methods together as a feature vector, calculate the Euclidean distance between features. They claim that the combined Hessian points and CSLBP make the features invariant to translation, scale, and illumination.

Local Binary Pattern Histogram Fourier Features using by Badal Soni et al. [42], in this paper, a block-based passive technique for copy-move tampering detection is given by extracting LBP-HF from each overlapping block. LBP-HF proposed by T. Ahonen et al. [9], is a rotation invariant descriptor based on uniform local binary pattern histograms. After feature extraction, matched blocks are obtained by calculating the Euclidean distances between the feature vectors of each block with the rest of the blocks and using the distance threshold as a decision parameter. According to their result, the computational time and accuracy are better than these three methods, Kulkarniet al. [43], Yang et al. [44], and Huang et al. [45]. And said that the proposed method is efficient and able to detect small-copied regions with the minimum false match.

While in Y. Wang et al. [46] choose different color space YCbCr, they proposed a novel passive image copy-move forgery detection technique based on Local Binary Pattern (LBP) and Singular Value Decomposition (SVD). Unlike other methods, this method uses YCbCr color space for preprocessing, and the test image is then divided into overlapping sub-blocks. Then LBP is followed to label the blocks. And they extracted the biggest N of SVD values on the LBP-labeled blocks. This N of SVD values plus average Y, Cb, Cr values constitute the feature vector for the block. Then the feature vectors are lexicographically sorted, and element-by-element similarity measurement is used to determine the forged blocks finally. Finally, the authors compared with the SVD based and LBP-DCT based methods, the result shows that the method has lower computational complexity and detects the copied and pasted regions with higher accuracy and has good performance on regular or non-regular copy-move forgery operations. D. K. Kalsi et al. [47] proposed a passive method Approximation image local binary pattern (AILBP) is being applied for feature extraction, which is a combination of wavelets decomposition along with the LBP method. In this approach, the input image divides into non-overlapping blocks at first, using wavelets applied to decompose the image into many different levels, selecting the lowest frequency components and the highest frequency components, and extracts the LBP features after the wavelet decomposition process. They claim that the proposed method is effective in terms of accuracy and it reduces time computation.

How to overcome rotation forged is still a problem in the current field. Li, L. et al. [48] proposed a method using rotation-invariant uniform local binary patterns to solute this problem. First, the image is converted to grayscale, and then the grayscale image is filtered through a low-pass filter. Secondly, the grayscale image is divided into overlapping circular blocks, and then the LBP of each block is calculated, and dictionary sorting is used to store all the feature vectors. The third step is to calculate the Euclidean distance of the feature vector to find the corresponding block. At last, reduce the false matches using a specially designed filter and morphological operations, producing the detection map. Rotation invariant uniform LBP method combines the advantages of Rotation invariant LBP and Uniform LBP. The proposed scheme is that it cannot only deal with traditional image processing operations but also geometric transforms, especially region rotation and/or flipping.

In Tralic, D. et al [49], the image is divided into small overlapping blocks. The center pixel of the block is used to define circles with different radii. Bilinear interpolation is used for sampling. The sampling points are used to form small neighborhoods. The simplified description of the point value of LBP is locally applied to each block in each neighborhood. Use this point value as the input of CA to get a binary array as a feature vector for matching. Due to the interpolation process, the proposed feature extraction process is inefficient, and the results show that the proposed method has limited robustness to noise and JPEG compression.

While in Gani, G. et al [50] also combine CA and LBP methods, but in their proposed scheme, the suspicious input image to be analyzed is first low pass filtered and converted into a local binary pattern (LBP) image. Then divide the LBP texture image into overlapping blocks. Next, a compact five-dimensional feature vector is extracted from each block by using threshold and cellular automata. This set of feature vectors is sorted in lexicographic order to make the copied and pasted blocks closer to each other. Finally, the feature

matching step is used to reveal duplicate blocks. They claim that the proposed method is effective for positioning, copying and moving forgery in uncompressed and compressed images and different image processing situations.

Table 2 shows the summary of the above papers, it shows that most researchers prefer to use the LBP method on block-based [38] [39] [40] [41] [42] [46] [48] [49] [50]. Also, the color space has some limitations, Gray and YCbCr are the first choices. D. K. Kalsi et al. [47] gave us a new method, which does not use any pre-processing method, directly divides into blocks, and uses Wavelet Decomposition to extract low-frequency parts as feature extraction blocks.

B. MACHINE LEARNING-BASED METHOD

In this kind of method, researchers think that image forgery detection is a binary classification problem (i.e., authentic vs. tampered), in this case the matching step name as classification.

In G. Muhammad et al. [52] an improved algorithm based on SPT and LBP is proposed to detect copy movement and tampering in digital images. The image is first converted into multiple subbands of different scales and directions through SPT. Then extract the LBP normalized histogram from each subband and use it as a feature vector. Two feature selection methods are used to reduce the dimensionality of the data set. Support vector machine (SVM) is applied to detect forged images. In this method, SPT is respectively applied to the two components of YCrCb, Cr and Cb, and it is found that the chrominance channels are better than luminance channel or grayscale in the detection of image forgery.

In Alahmadi A. et al. [53] a novel passive image forgery detection method is proposed based on local binary pattern (LBP) and discrete cosine transform (DCT) to detect copy-move and splicing forgeries. First, from the chrominance component of the input image, discriminative localized features are extracted by applying 2D DCT in LBP space. After that, the standard deviation of each DCT coefficient of all blocks is computed and used as features. Then, a support vector machine is used for detection. Figure 8 shows the detail of the process of modeling the tampering traces. According to its experimental results, the method has good robustness to rotation invariance, and the detection accuracy is the highest in the case of rotation, deformation, and resized form.

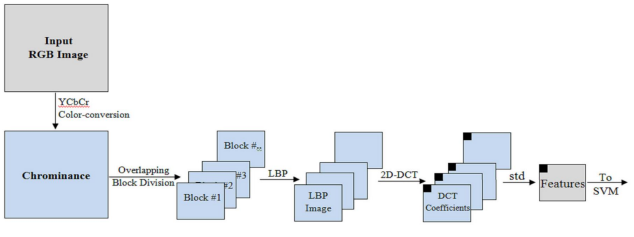


FIGURE 8. the detail of the process of [53]. (Image resource from [53]

Also using LBP, DCT and SVM, M. F. Jwaid et al. [54] made some improvements and added other methods. First, change the picture from RGB to YCbCr by applying preprocessing. Secondly, apply discrete wavelet transform on top of the image for compression. Guess that the subgraph contains the low-repetition part with the most extreme data. The LL subgraph is divided into overlay squares. Third, execute local binary mode. Fourth, use principal component analysis to match between matching blocks as feature matching. The latest step is support vector machine (SVM) classification to choose which slice is fake.

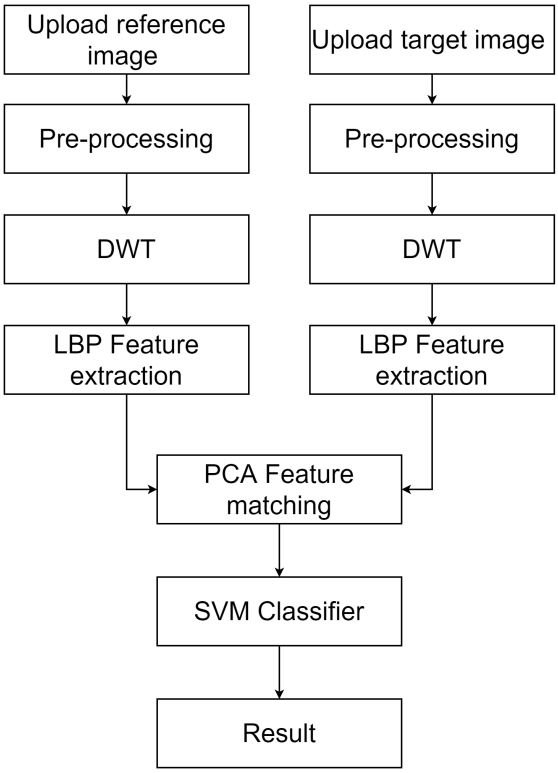


FIGURE 9. the detail of the process of [54].

Like Alahmadi A. et al. [53], M. M. Islam [55] also proposed a passive (blind) image tampering recognition method based on discrete cosine transform (DCT) and local binary pattern (LBP). But they choose like that, first, the chrominance components of the image are divided into fixed-size non-overlapping blocks, and the 2D block DCT is applied to identify the changes caused by the forgery in the local frequency distribution of the image. Then the texture descriptor LBP is applied to the amplitude component of the 2D-DCT array to enhance the artifacts introduced by the tampering operation. The resulting LBP image is again divided into non-overlapping blocks. Finally, calculate the sum of the corresponding inter-cell values of all LBP blocks and arrange them as feature vectors. These features are input into a support vector machine (SVM) with a radial basis function (RBF) as the kernel to distinguish fake images from real images. According to their results, the proposed method is superior to

existing methods on different well-known publicly available benchmark data sets for image forgery detection.

Table 3 show the summary of above methods, in the feature extraction step, we can clearly understand the different between the two methods, Alahmadi, A. et al. [53] using LBP first and then using DCT, while M. F. Jwaid et al. [54] using DCT first and then using LBP, beside this, M. F. Jwaid et al. [54] using PCA before SVM, the purpose of this step is to determine whether it is necessary to perform SVM classification. The PCA method compares the values of two images (reference image and target image). If there is any difference between the values of the referenced input image, it means it is forged and will continue to the next stage. If there is no difference in the values, it means that the input image is original and will stop at this stage.

V. CONCLUSION

In this paper, briefly summarizes several methods of using local binary patterns in copy move forgery detection. Some common LBP extension methods are listed. As a long-established method, LBP has many advantages and disadvantages. With the increase of its expansion method, its calculation amount is also increasing, and the complexity of the algorithm becomes higher. When used as a feature vector, the dimensionality is higher. This is the current problem. However, compared with other methods, the calculation efficiency of LBP and its extension method is still lower than other methods.

REFERENCES

[1] Meena, Kunj Bihari, and Vipin Tyagi. "Image Splicing Forgery Detection Techniques: A Review." In *International Conference on Advances in Computing and Data Sciences*, pp. 364-388. Springer, Cham, 2021.

[2] Kaur, Amandeep, and Jyoti Rani. "Digital Image Forgery and Techniques of Forgery Detection: A brief review."

[3] Ojala T, Pietikinen M, Harwood D. A comparative study of texture measures with classification based on feature distributions [J]. Pattern Recognition, 1996, 29(1): 51-59.

[4] Ojala, Timo, Matti Pietikainen, and Topi Maenpaa. "Multiresolution gray-scale and rotation invariant texture classification with local binary patterns." *IEEE Transactions on pattern analysis and machine intelligence* 24, no. 7 (2002): 971-987.

[5] Liao, Shengcai, Xiangxin Zhu, Zhen Lei, Lun Zhang, and Stan Z. Li. "Learning multi-scale block local binary patterns for face recognition." In *International conference on biometrics*, pp. 828-837. Springer, Berlin, Heidelberg, 2007.

[6] Zhao, Sanqiang, Yongsheng Gao, and Baochang Zhang. "Sobel-lbp." In *2008 15th IEEE International Conference on Image Processing*, pp. 2144-2147. IEEE, 2008.

[7] Heikkilä, Marko, Matti Pietikäinen, and Cordelia Schmid. "Description of interest regions with local binary patterns." *Pattern recognition* 42, no. 3 (2009): 425-436.

[8] Liao, Shu, Max WK Law, and Albert CS Chung. "Dominant local binary patterns for texture classification." *IEEE transactions on image processing* 18, no. 5 (2009): 1107-1118.

[9] Ahonen, Timo, Jiří Matas, Chu He, and Matti Pietikäinen. "Rotation invariant image description with local binary pattern histogram fourier features." In *Scandinavian conference on image analysis*, pp. 61-70. Springer, Berlin, Heidelberg, 2009.

[10] Louis, Wael, and Konstantinos N. Plataniotis. "Co-occurrence of local binary patterns features for frontal face detection in surveillance applications." *EURASIP Journal on Image and Video Processing 2011* (2011): 1-17.

[11] Zhou, Guojuan, and Dianji Lv. "An overview of digital watermarking in image forensics." In *2011 Fourth International Joint Conference on Computational Sciences and Optimization*, pp. 332-335. IEEE, 2011.

[12] Huo, Yaoran, Hongjie He, and Fan Chen. "A semi-fragile image watermarking algorithm with two-stage detection." *Multimedia tools and applications* 72, no. 1 (2014): 123-149.

[13] C. Singh and S. K. Ranade, "Geometrically invariant and high-capacity image watermarking scheme using accurate radial transform," *Optics Laser Technology*, vol. 54, pp. 176-184, 2013.

[14] İmamoğlu, Mustafa Bilgehan, Güzin Ulutaş, and Mustafa Ulutaş. "Detection of copy-move forgery using krawtchouk moment." In *2013 8th international conference on electrical and electronics engineering (ELECO)*, pp. 311-314. IEEE, 2013.

[15] Chauhan, Devanshi, Dipali Kasat, Sanjeev Jain, and Vilas Thakare. "Survey on keypoint based copy-move forgery detection methods on image." *Procedia Computer Science* 85 (2016): 206-212.

[16] Sharma, Aditi, Nishtha Adhao, and Anju Mishra. "A survey: Static and dynamic ranking." *International Journal of Computer Applications* 70, no. 14 (2013): 7-12.

[17] Jin, Guonian, and Xiaoxia Wan. "An improved method for SIFT-based copy–move forgery detection using non-maximum value suppression and optimized J-Linkage." *Signal Processing: Image Communication* 57 (2017): 113-125.

[18] Prakash, Choudhary Shyam, et al. "Detection of copy-move forgery using AKAZE and SIFT keypoint extraction." *Multimedia Tools and Applications* 78.16 (2019): 23535-23558.

[19] Manu, V. T., and Babu M. Mehtre. "Detection of copy-move forgery in images using segmentation and SURF." In *Advances in signal processing and intelligent recognition systems*, pp. 645-654. Springer, Cham, 2016.

[20] Gong, Jiachang, and Jichang Guo. "Image copy-move forgery detection using SURF in opponent color space." *Transactions of Tianjin University* 22, no. 2 (2016): 151-157.

[21] Wang, Chengyou, Zhi Zhang, and Xiao Zhou. "An image copy-move forgery detection scheme based on A-KAZE and SURF features." *Symmetry* 10, no. 12 (2018): 706.

[22] Yang, Fan, Jingwei Li, Wei Lu, and Jian Weng. "Copy-move forgery detection based on hybrid features." *Engineering Applications of Artificial Intelligence* 59 (2017): 73-83.

[23] Li, Jian, Xiaolong Li, Bin Yang, and Xingming Sun. "Segmentation-based image copy-move forgery detection scheme." *IEEE transactions on information forensics and security* 10, no. 3 (2014): 507-518.

[24] Elaskily, Mohamed A., Heba A. Elnemr, Ahmed Sedik, Mohamed M. Dessouky, Ghada M. El Banby, Osama A. Elshakankiry, Ashraf AM Khalaf et al. "A novel deep learning framework for copy-moveforgery detection in images." *Multimedia Tools and Applications* 79, no. 27 (2020): 19167-19192.

[25] Ouyang, Junlin, Yizhi Liu, and Miao Liao. "Copy-move forgery detection based on deep learning." In *2017 10th international congress on image and signal processing, biomedical engineering and informatics* (CISP-BMEI), pp. 1-5. IEEE, 2017.

[26] Abidin, Arfa Binti Zainal, et al. "Copy-move image forgery detection using deep learning methods: a review." *2019 6th International Conference on Research and Innovation in Information Systems* (ICRIIS). IEEE, 2019.

[27] Jaiswal, Ankit Kumar, and Rajeev Srivastava. "Detection of copy-move forgery in digital image using multi-scale, multi-stage deep learning model." *Neural Processing Letters* 54, no. 1 (2022): 75-100.

[28] Huang, Yanping, Wei Lu, Wei Sun, and Dongyang Long. "Improved DCT-based detection of copy-move forgery in images." *Forensic science international* 206, no. 1-3 (2011): 178-184.

[29] Hilal, Alaa, Taghreed Hamzeh, and Samer Chantaf. "Copy-move forgery detection using principal component analysis and discrete cosine transform." In *2017 Sensors Networks Smart and Emerging Technologies* (SENSET), pp. 1-4. IEEE, 2017.

[30] Thayyil, Jamshida, and K. Edet Bijoy. "Digital Image Forgery Detection using Graph Fourier Transform." In *2020 International Conference on Futuristic Technologies in Control Systems and Renewable Energy (ICFCR)*, pp. 1-5. IEEE, 2020.

[31] Sharma, B. Vaishali, and Amit Garg. "Detection of Tampered Images via Stationary Wavelet Transform and Principal Component Analysis." *International Journal of Science, Engineering and Technology Research* (IJSETR) Volume 8.

[32] Tejas, K., C. Swathi, and M. Rajesh Kumar. "Copy Move Forgery using Hu's Invariant Moments and Log-Polar Transformations." In *2018 3rd IEEE International Conference on Recent Trends in Electronics, Infor-*

mation and Communication Technology (RTEICT), pp. 1229-1233. IEEE, 2018.

[33] Ouyang, Junlin, Yizhi Liu, and Miao Liao. "Robust copy-move forgery detection method using pyramid model and Zernike moments." *Multimedia Tools and Applications* 78, no. 8 (2019): 10207-10225.

[34] M. B. İmamoğlu, G. Ulutaş and M. Ulutaş, "Detection of copy-move forgery using Krawtchouk moment," *2013 8th International Conference on Electrical and Electronics Engineering*(ELECO), 2013, pp. 311-314.

[35] Hosny, Khalid M., Hanaa M. Hamza, and Nabil A. Lashin. "Copy-move forgery detection of duplicated objects using accurate PCET moments and morphological operators." The Imaging Science Journal 66, no. 6 (2018): 330-345.

[36] Malkauthekar, M. D. "Analysis of Euclidean distance and Manhattan distance measure in Face recognition." In *Third International Conference on Computational Intelligence and Information Technology* (CIIT 2013), pp. 503-507. IET, 2013.

[37] Fischler, Martin A., and Robert C. Bolles. "Random sample consensus: a paradigm for model fitting with applications to image analysis and automated cartography." *Communications of the ACM* 24, no. 6 (1981): 381-395.

[38] Davarzani, Reza, Khashayar Yaghmaie, Saeed Mozaffari, and Meysam Tapak. "Copy-move forgery detection using multiresolution local binary patterns." *Forensic science international* 231, no. 1-3 (2013): 61-72.

[39] Kaur, Ramandeep. "Copy-Move Forgery Detection Utilizing Local Binary Patterns." (2013).

[40] Sharma, Shikha, and C. Rama Krishna. "An efficient distributed group key management using hierarchical approach with elliptic curve cryptography." In *2015 IEEE International Conference on Computational Intelligence and Communication Technology*, pp. 687-693. IEEE, 2015.

[41] Uliyan, Diaa M., Hamid A. Jalab, and Ainuddin W. Abdul Wahab. "Copy move image forgery detection using Hessian and center symmetric local binary pattern." In *2015 IEEE conference on open systems* (ICOS), pp. 7-11. IEEE, 2015.

[42] Soni, Badal, Pradip K. Das, and Dalton Meitei Thounaojam. "Copy-move tampering detection based on local binary pattern histogram fourier feature." In *Proceedings of the 7th International Conference on Computer and Communication Technology*, pp. 78-83. 2017.

[43] Khan, Er Saiqa, and Er Arun Kulkarni. "An efficient method for detection of copy-move forgery using discrete wavelet transform." *International Journal on Computer Science and Engineering* 2, no. 5 (1801): 2010.

[44] Wo, Yan, Kemin Yang, Guoqiang Han, Haichao Chen, and Wenbo Wu. "Copy–move forgery detection based on multi-radius PCET." *IET Image Processing* 11, no. 2 (2017): 99-108.

[45] Huang, Yanping, Wei Lu, Wei Sun, and Dongyang Long. "Improved DCT-based detection of copy-move forgery in images." *Forensic science international* 206, no. 1-3 (2011): 178-184.

[46] Wang, Yuan, Lihua Tian, and Chen Li. "LBP-SVD based copy move forgery detection algorithm." In *2017 IEEE international symposium on multimedia* (ISM), pp. 553-556. IEEE, 2017.

[47] Parmar, Gagan, Sagar Lakhani, and Manju K. Chattopadhyay. "An IoT based low cost air pollution monitoring system." In *2017 International Conference on Recent Innovations in Signal processing and Embedded Systems* (RISE), pp. 524-528. IEEE, 2017.

[48] Li, Leida, Shushang Li, Hancheng Zhu, Shu-Chuan Chu, John F. Roddick, and Jeng-Shyang Pan. "An Efficient Scheme for Detecting Copy-move Forged Images by Local Binary Patterns." J. Inf. Hiding Multim. *Signal Process*. 4, no. 1 (2013): 46-56.

[49] Tralic, Dijana, Sonja Grgic, Xianfang Sun, and Paul L. Rosin. "Combining cellular automata and local binary patterns for copy-move forgery detection." *Multimedia tools and applications* 75, no. 24 (2016): 16881-16903.

[50] Hussain, M., G. Muhammad, S. Q. Saleh, A. M. Mirza, and G. Bebis. "Image forgery detection using multi-resolution Weber local descriptors, Eurocon, July 2013." 1570-1577.

[51] Huang, Hailing, Weiqiang Guo, and Yu Zhang. "Detection of copy-move forgery in digital images using SIFT algorithm." In *2008 IEEE Pacific-Asia Workshop on Computational Intelligence and Industrial Application*, vol. 2, pp. 272-276. IEEE, 2008.

[52] Muhammad, Ghulam, Muneer H. Al-Hammadi, Muhammad Hussain, Anwar M. Mirza, and George Bebis. "Copy move image forgery detection method using steerable pyramid transform and texture descriptor." In *Eurocon* 2013, pp. 1586-1592. IEEE, 2013.

[53] Alahmadi, Amani, Muhammad Hussain, Hatim Aboalsamh, Ghulam Muhammad, George Bebis, and Hassan Mathkour. "Passive detection of image forgery using DCT and local binary pattern." *Signal, Image and Video Processing* 11, no. 1 (2017): 81-88.

[54] Jwaid, Mohanad Fadhil, and Trupti N. Baraskar. "Detection of copy-move image forgery using local binary pattern with discrete wavelet transform and principle component analysis." In *2017 International Conference on Computing, Communication, Control and Automation* (ICCUBEA), pp. 1-6. IEEE, 2017.

[55] Islam, Mohammad Manzurul, Gour Karmakar, Joarder Kamruzzaman, and Manzur Murshed. "A robust forgery detection method for copy–move and splicing attacks in images." *Electronics* 9, no. 9 (2020): 1500.

TABLE 1. List of extension LBP method

Name	Short Name	Year	Advantages	Disadvantages
Local Binary pattern [3]	LBP	1996	1.Easy to computation 2.Gray scale invariant	1. Large number of eigenvectors dimensions 2. Fix area
Circular LBP [4]	$LBP_{P,R}$	2002	1. Adapted to texture features of different scales 2. Random area	-
Rotation Invariant LBP [4]	$LBP^{ri}_{P,R}$	2002	1. Rotation invariant	1.Large number of eigenvectors dimensions
Rotation Invariant Uniform LBP [4]	$LBP^{riu2}_{P,R}$	2002	1. Rotation invariant 2. Low feature dimensions	-
Multi-block LBP [5]	$MB-LBP$	2007	1. Dimensionality reduction	-
Sobel-LBP [6]	$Sobel-LBP$	2008	1. Significant effect on the change of different lighting. 2. Good on edge detection	-
Center Symmetric LBP [7]	$CSLBP$	2009	1. Tolerance to illumination changes 2. Robustness on flat image areas 3. Computational efficiency	-
Dominant LBP [8]	$DLBP$	2009	1. Robustness to image rotation and noisy images.	-
LBP Histogram Fourier [9]	$LBP-HF$	2009	1. Rotation invariant 2. Highly discriminative	-
Co-occurrence of LBP [10]	$CoLBP$	2011	1. Computationally efficient Produces a high-performance rate.	-

TABLE 2. survey summary

Paper	Pre-processing	Block/Segmented/Keypoint-based	Feature Extraction	Matching	Post-processing
Davarzani et al. [38]	RGB-GRAY	Block-based		K-d tree	RANSAC
Kaur et al. [39]	RGB-GRAY	Block-based	LBP	ED	-
S. Sharma, et al. [40]	RGB-GRAY	Block-based	CSLBP	ED	-
D. M. Uliyan et al. [41]	Ncut segmentation	Segmented based	Hessian interest points, LBP	ED	-
Badal Soni et al. [42]	RGB-GRAY	Block-based	LBP-HF	ED	-
Y. Wang et al. [46]	RGB-YCbCr	Block-based	SVD, LBP	Element-by-element similarity measurement	-
D. K. Kalsi et al. [47]	-	Block-based	Wavelet Decomposition, LBP	-	-
Li, L. et al. [48]	RGB-GRAY	Circular block-based	Rotation-invariant uniform LBP	ED	-
Tralic, D. et al [49]	RGB-GRAY	Block-based	CA, LBP	ED	-
Gani, G. et al [50]	RGB-GRAY	Block-based	CA, LBP	ED	-

TABLE 3. survey summary

Paper	Pre-processing	Block/Segmented/Keypoint-based	Feature Extraction	Classification
G. Muhammad et al. [52]	RGB-YCbCr	-	SPT+LBP	SVM
Alahmadi, A. et al. [53]	RGB-YCbCr	block-based	LBP+DCT	SVM
M. F. Jwaid et al. [54]	RGB-YCbCr	block-based	DCT+LBP	PCA+SVM
Islam MM et al. [55]	RGB-YCbCr	block-based	DCT+LBP	SVM

JINGJING RAO received the B.E. degree in software engineering from the Dalian Neusoft University of Information, in 2016, and the M.E. Eng. degree in information science and engineering from Ritsumeikan University, in 2022, where she is currently pursuing the Ph.D. degree in information science and engineering. Her research interests include digital forensics, and computer vision.

SONGPON TEERAKANOK received his B.E. from Prince of Songkla University, Thailand in 2013, and M.E. and D.Eng. degrees in Information Science and Engineering from Ritsumeikan University in 2016 and 2019, respectively. He was a former assistant professor at Ritsumeikan University before joining the Faculty of ICT, Mahidol University, Thailand in May 2021. His research interest covers Cryptography, Privacy, Location-based Service (LBS), and Digital Forensics.

TETSUTARO UEHARA received the B.E., M.E., and D.Eng. degrees from Kyoto University, in 1990, 1992, and 1996, respectively. He was an Assistant Professor with the Faculty of Systems Engineering, Wakayama University, from 1996 to 2003. From 2003 to 2005, he was an Associate Professor with the Center for Information Technology, Graduate School of Engineering, Kyoto University. From 2006 to 2011, he was an Associate Professor with the Academic Center for Computing and Media Studies, Kyoto University. From 2011 to 2013, he was the Deputy Director of the Standardization Division in the Ministry of Internal Affairs and Communication, Japan. He has been a Professor with the College of Information Science and Engineering, Ritsumeikan University, since 2013. He has also been the Vice-President of the Institute of Digital Forensics, since 2017. His research interests include systems security, digital forensics, privacy, education in information ethics, and information system management in local government.