Comparative Study of Copy-Move Forgery Detection Techniques

Mohamed A. Elaskily and Heba K. Aslan

Department of Informatics, Electronics Research Institute, Cairo, Egypt

Fathi E. Abd El-Samie

Department of Electronics and Electrical Communications, Faculty of Electronic Engineering, Menoufia University, Menouf, 32952, Egypt

Osama A. Elshakankiry and Osama S. Faragallah

Department of Information Technology, College of Computers and Information Technology, Taif University, Al-Hawiya, 21974, Kingdom of Saudi Arabia

Mohamed M. Dessouky

Department of Computer Science and Engineering, Faculty of Electronic Engineering, Menoufia University, Menouf, 32952, Egypt

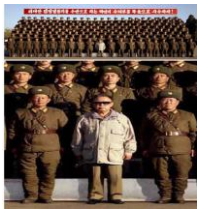
Abstract— **Digital images and their applications gained a huge interest around the world in several fields like newspapers, social media, defaming persons, and courts. There are two types of digital image authentication. The first type is active authentication, which uses digital signature and image watermarks. These techniques have certain constraints such as knowing the content of the digital image. They need special equipment like cameras and development software. The second type is passive authentication, which is used to detect digital image forgeries represented in image cloning, image splicing, image resampling, image retouching, and image morphing. Passive authentication has an advantage of not needing any previous knowledge of the image content to detect the forgery. Copy-move forgery is the most famous type, and it is widespread in all image forgeries. Copy-move forgery is easy to perform and the forged part has the same properties of the whole image that makes it difficult to detect. There are many algorithms used to detect copy-move forgery attacks depending on different techniques. This paper covers the directions of copy-move forgery detection and gives a wide coverage of earlier copy-move forgery detection algorithms and techniques.**

Index Terms - Digital image forgery, Image authentication, Copy-move forgery, Image splicing, Image morphing.

I. INTRODUCTION

The image is one of the most popular ways of communication today. Unlike other types of digital data, the image can easily carry any idea quickly and correctly between recipients. The wide range of image applications makes it mostly affected by tamper or fraud. Figure 1 represents different examples of image forgeries. To authenticate an image, there are two ways of authentication; active authentication and passive authentication [3].

Active authentication is classified into two methods; digital signature and watermarking. Each camera has its unique methodology to construct the digital image. Camera fingerprint, acquisition fingerprints, coding fingerprint, and editing fingerprint represent different types of digital signature extracted from an image [4]. A digital signature is embedded also by automatic camera software or post-application software as shown in figure 2. Watermarking embeds some information into the image without appearance degradation. Watermarking is tested by extracting this information at the receiver and examining if those watermark tampers or not [5]. When active authentication is not available, the passive or blind methods are the best solution to make decisions about the trustworthiness of image authentication. Active authentication requires knowing the content of the image, unlike passive authentication that does not need a previous knowledge of the image.



Forged image used from North Korea to obscure the rumors of Kim Jong-Il's death [1]

A boxer fights the shark and Drives it to the beach [2]

Photographer Brian Walski combines objects of the original first two photographs in a new altered image which appeared on the front page of the Los Angeles Times on 31 March, 2003.

Fig. 1. Examples of image forgeries.

Passive or blind forgery detection techniques became very important to overcome the problems of active techniques represented in:

a) Previous knowledge of image contents.

b) Processing time to embed a digital signature or watermark in an image in addition to the processing time lost at the receiver side to examine the authenticity [6].

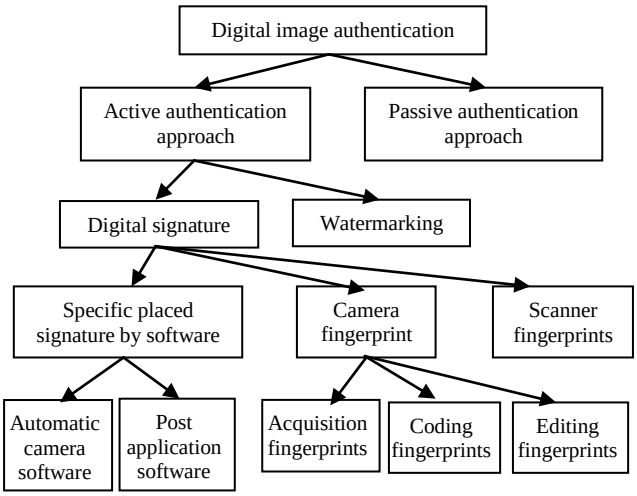


Fig. 2. Digital image authentication.

The rest of this paper is organized as follows. Section two defines digital image forgery types. Section three discusses copy-move forgery detection. Section four focuses on copy-move forgery detection algorithms and their classifications.

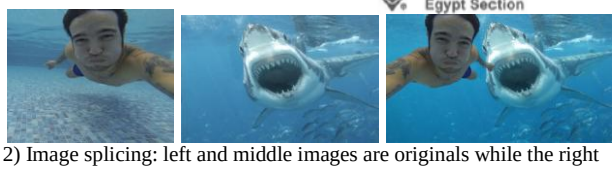
Finally, section five presents the conclusions and the future work.

II. TYPES OF DIGITAL FORGERY

Digital image forgery is represented in different shapes illustrated as follows:

1) *Copy-Move Forgery:* Copy-move forgery is the broader spread forgery, especially, in forgeries that use one image only to duplicate or hide one or more objects into the same image [7]. It is performed by copying a region from an image and pasting it into the same image to hide or duplicate specific objects in the image as illustrated in figure 3(A). The final forged image has homogenous features.
2) *Image Splicing:* Image splicing is the same idea of copy-move forgery but the used objects are collected from more than one image [8]. It is performed by copy one or more object from two or multiple images to combine these objects into a new tampered image as shown in figure 3(B). The effects of images splicing forgery may be cleared because it uses different regions from different images with different features to combine a new image.
3) *Image Resampling:* Image resampling depends on creating a new image with increasing/decreasing height/width of a specific object in an image or in all content of the image [9]. Figure 3(C) shows an example of image resampling. Resizing of an image means changing the dimensions of an object only to appear larger but not to improve the quality of that object.
4) *Image Retouching:* Image retouching forgery idea is enhancing an object or image to exhibit or hide a specific feature as coloring, lighting or background changing to attract attention or to divert attention about an object in an image [9]. Figure 3(D) shows an example of image retouching.
5) *Image Morphing:* In image morphing forgery, the shape of an image is gradually changed into another shape in another image and it must be applied to two images [10]. Figure 3(E) shows an example of image morphing.
6) *Image Created by Graphical Software:* An image is created by graphical software by using a computer and its applications to create a forged image not connected with reality by building its objects and features by the computer as shown in figure 3(F).

1) Copy- move forgery where left is the original image and right is the tampered one.



2) Image splicing: left and middle images are originals while the right image tampers.

3) Image resampling: left Image is the original and right image is resampled.

4) Examples of image retouching.

5) Examples of image morphing.

E) Image morphing where the left and middle images are originals and the right image is morphed.

F) Images created by graphical software.

Fig. 3. Types of digital image forgery.

The different effects of digital image forgery are illustrated in figure 4. The effects of copy-move forgery are not debunked because the added objects have the same features of the other regions. The effects of image splicing are represented in edges and boundaries disturbances, inconsistency in chromatic aberration, and blurred splicing boundaries. Compared with other forgery type's effects, it is clear that copy-move forgery is the hardest type to detect.

III. PROPOSED METHOD

Copy-move forgery is the most difficult type of digital image forgeries to detect. It uses a region in the same image with the same properties and features of the other image regions to hide or duplicate some objects in the image. We will concentrate on copy-move forgery detection due to its widespread use and the difficulty of its detection.

There are two main goals of any forgery detection algorithm; firstly, reducing complexity represented in execution time, and Secondly, increasing the algorithm accuracy against different processing operations used in copy-move forgery.

There are main steps which any copy-move forgery detection algorithm performs. First, gray-scale conversion is applied by combining the red, green, and blue channels to operate in a form of a gray-scale image. The second division operation is performed based on two types of classification; pixel-based type and block-based type [11]. Third, image processing transformations are applied to extract the image features. A descriptor or classifier is used to calculate the feature vectors as noise distribution, color, light, shadow, resolutions, or edges. Finally, a lexographical representation is used as a map to examine the image feature vectors to compare values and match the identical ones. The block diagram in Figure 5 shows the copy-move operation methodology.

Copy-move forgery detection algorithms are divided into different families based on the image processing operation performed after division [3]. In the next section, we will discuss each family, and the earlier techniques used and compare between the best techniques in each family.

IV. Copy-Move Forgery Detection Algorithms

In this section, we try to draw a map for the huge number of researches that appeared in this area. The paper focuses on the earlier techniques by showing and comparing the advantage and disadvantages of each one.

A. Algorithms Based on DCT

The main idea of this family of algorithms is using Discrete Cosine Transform (DCT) to be applied to an image. The DCT coefficients are used as features and then compared to find the duplicated regions.

Fridrich et al. [12] presented the first algorithm that works with this technique. The algorithm steps begin by1) dividing the image into overlapping blocks. After that, the DCT is applied to the image and the DCT coefficients are extracted. The features are lexicographically ordered in a2) map. Finally, identical features mean that regions are similar and tampering happened. A shift vector S is used to calculate the difference between each two blocks as $S = (S_1, S_2) = (i_1 - j_1, i_2 - j_2)$, where, (i_1, j_1) is the position of the first block and (i_2, j_2) is the position of the second block. By using an exhaustive search, tampering is detected by calculating the distance between each two blocks.

The difference result is equal to zero if the two blocks are the same and in the same position. Therefore, not tampering is detected. If the result is equal to a value, the two blocks are the same and in different positions. This means that tampering has happened. The main advantage of this method is that it may successfully detect the forged part even when the copied area is enhanced or retouched. The main disadvantage is that uniform areas in images, such as the sky, may lead to false matches.

Kumar et al. [13] used DCT to represent the features of overlapping blocks after the division of blocks. An automated threshold is used for separating the mirage matches from the real matches. The advantages of Kumar's algorithm are the better execution time and performance for all block sizes. Another advantage is the robust success at different Signal-to-Noise Ratio (SNRs). The main disadvantage is the dependence of the detection algorithm upon the size of the copied region in the case of rotation and scaling. The robustness decreases with the decrease in the size of the copy-moved region.

Maind et al. [14] divide the image into fixed blocks and quantized these blocks by applying DCT on each one. The transformed circular block is represented with four features for each block to reduce the dimension of it. A Lexographically representation made and depends on a threshold value the duplicated blocks are detected. The algorithm shows robustness to repeated copy-move forgery and also robustness against blurring or nosing adding. Offers low computational complexity due to the lower dimensions of feature vectors. The main disadvantage is the high computational complexity in case of the large size of feature vectors.

Fadl et al. [15] depended on first dividing the image into fixed size overlapping blocks. Second, they applied DCT on each block to extract its features. They used fast K-means clustering technique over DCT to speed up the search by classifying features into different classes. They used zigzag scanning to reduce the length of block features. Finally, a Lexographically representation was used with radix sorting to reduce complexity. The advantage of this technique appears in reducing execution time up to 50% compared with the previous work. The main disadvantage is the low level of robustness against JPEG compression, blurring, rotating and scaling reprocessing, and the need to improve the response to geometric operations.

From the previous clarification, it is clear that the algorithms based on DCT use the methodology of extracting the feature vectors after any type of division. Then, we select a way to match these features. The difference between algorithms in robustness is obtained by:

a) The method that each algorithm tries to reduce the size of the feature vector and this has an effect on the computational complexity.

b) The algorithm able to detect different operations of image processing used by attackers to hide tampering.

B. Algorithms Using Invariant Image Moments

Image moments concept means a certain particular weighted average of image pixels intensities or functions. These moments are chosen to give a uniform interpretation of the image that helps in shape analysis. It is useful to describe image objects after segmentation or describe the total image intensity, central point, and information about objects orientation to detect rotation, translation, and scaling. Image moments technique connects regions in binary form to translate rotation and scaling in useful classification shape and part recognition as shown in figure 6.

Liu et al. [16] divided the image into circular blocks and then extracted the seven Hu moments. It is clear that they can handle rotation, blurring, noise addition and operations like JPEG compression. To decrease the processing time, the dimensions of search space must be decreased by 25% of the original dimensions using the Gaussian pyramid. They used only the first four Hu moments as features instead of all the seven moments to reduce time processing complexity. In addition, the features dimensions are also decreased. The main advantage of this method is the success in detection of post-processing operations and rotations. Also, it is more efficient compared with other algorithms. It has a small effect on increasing of false positive ratio. On the other hand, it cannot handle a way to Struggling scaling.

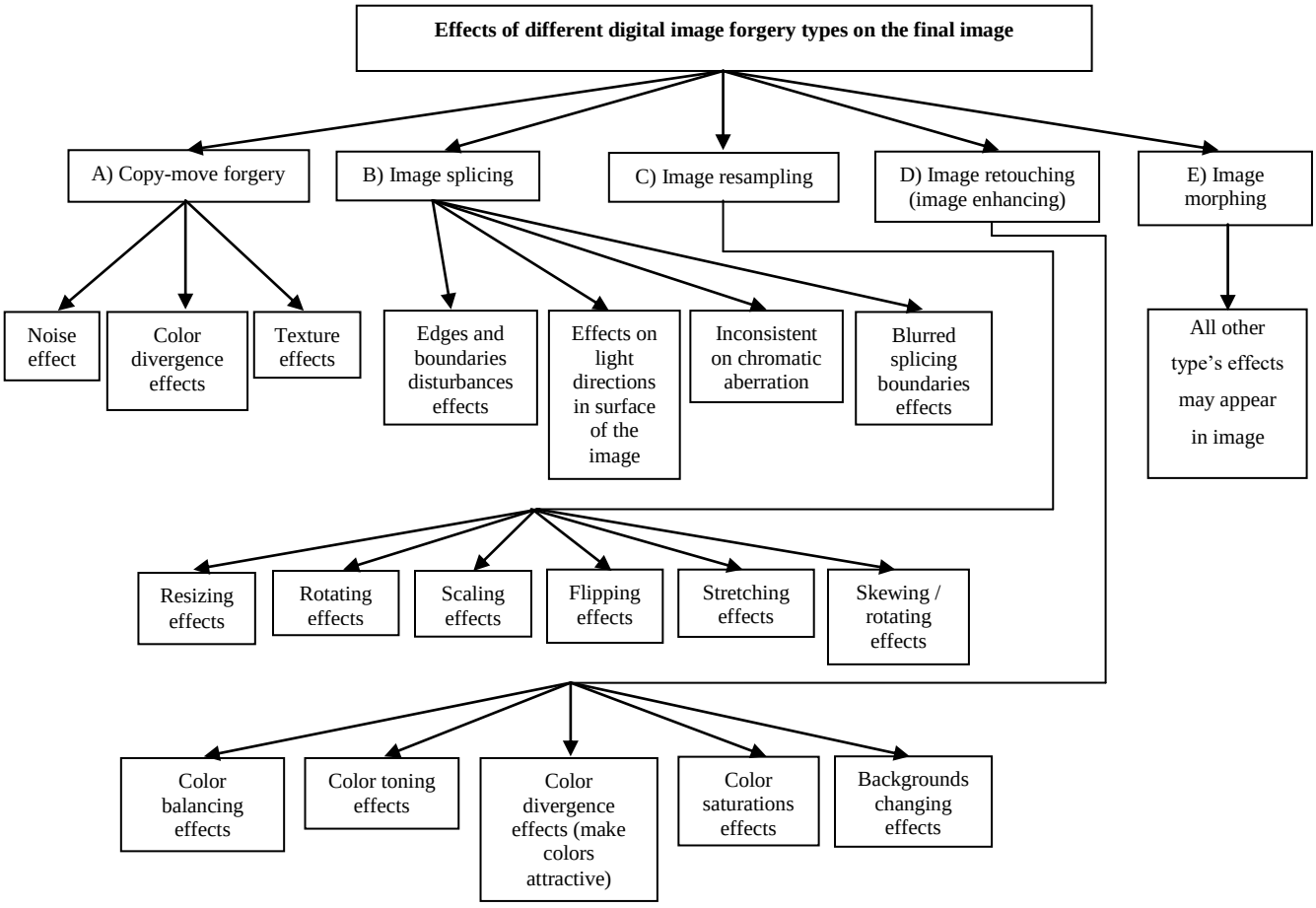


Fig. 4. Effects of different types of digital image forgery on the final image.

Accuracy Ratio (AR) is how often the detectors of the forgery have the ability to detect the actual forgery, which is explained by equation 1.

$$AR = (T_P + T_N)/(T_P + T_N + F_P + F_N) \quad (1)$$

where T_P is the true positive ratio, which reflects the forgery detection and existence. T_N is the true negative ratio, and it means that the algorithm does not detect any forgery and actually, the forgery does not exist. F_P is the false positive ratio, which means that the algorithm finds a forgery in the examined image, but actually it is a false alarm because forgery does not exist. F_N is the false negative ratio, and it means that the algorithm does not detect forgery, but actually the forgery is existing. Each algorithm has a precision ratio or true alarm rate that means how often a positive result of detecting forgery is actually an attack. True alarm rate is calculated by equation 2.

$$\text{True Alarm Rate} = T_P/(T_P + F_P) \quad (2)$$

Muhammad et al. [17] applied an un-decimated wavelet transform on the original image. They convert the image into a gray-scale image to produce a Lower Level (LL) resolution approximation image. A division process is applied on the LL image to produce 8×8 overlapped blocks. Zernike moments are extracted from each block to construct a feature vector for each one. They used a fixed threshold distance between each pair of blocks.

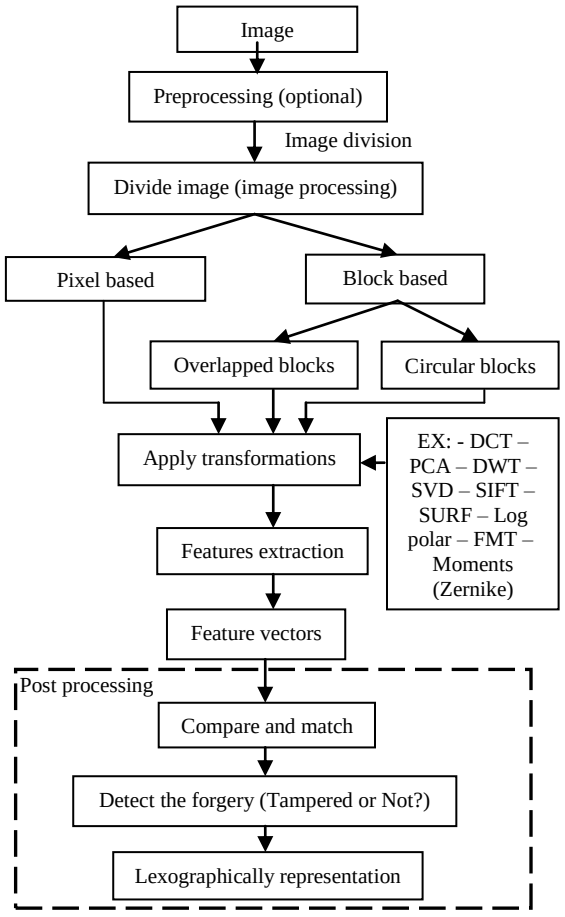


Fig. 5. Copy-move detection methodology.

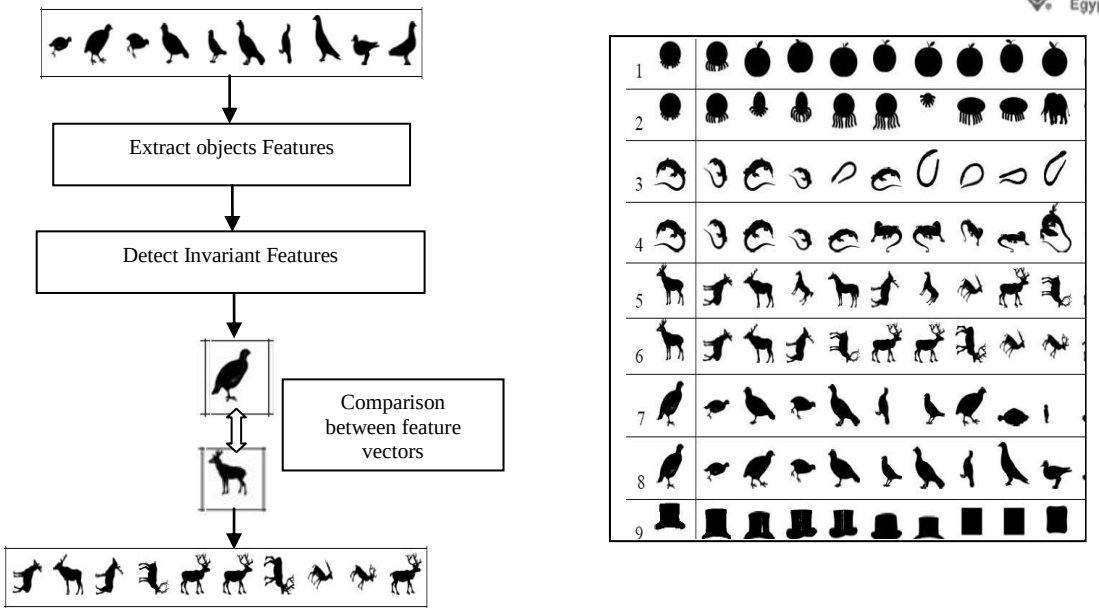


Fig. 6. Right diagram representing the operation of invariant image moments and the left one represents an example that describes each shape into one of the shape classes.

If the distances between some pairs of blocks are the same or below the threshold value, the pairs are forged blocks. It has a good performance up to 90% with low values of false positives.

YANG et al. [18] developed a new algorithm to overcome post-processing operations such as rotation, Gaussian noise, JPEG compression, and blurring. It is similar to Muhammad's algorithm [17], however, it applies dyadic wavelet transform. The image is converted to a gray-scale image and dyadic wavelet transform is applied to construct LL1 approximate image and HH1 near original image sub-bands. The upper left corner LL1 is divided into fixed $B \times B$ blocks. Zernike moments are computed for each block to produce a feature vector for each one and represent these features vectors in a lexicographic matrix as a map. If two neighboring blocks have features vectors V_i & V_{i+1} and the distance between them is less than a fixed threshold TH_1, the two blocks may be similar blocks or it is a false positive alarm. To reduce the ratio of false positive values, we resort to HH1 near the original image and calculate features vectors HV_i and, and then calculate the distance between them. If the distance is larger than a dissimilarity threshold TH_2, the two blocks are forged. This algorithm has a very good precision rate of detection compared with other algorithms. Also, it has a lower false positive rate of detection.

Ryu et al. [19] used Zernike moments to uncover duplicated regions with the ability to detect rotation in these regions. After that, the image is converted to a gray-scale image and divided into $M \times N$ blocks with $L \times L$ overlapping size. Zernike moments are used to extract feature vectors of each block and these feature vectors are representing the local image characteristics. A matching procedure is applied with Locality Sensitive Hashing (LSH) to match similarity feature vectors among all blocks. False matching appears when two or more blocks have similar magnitudes of Zernike moments. To increase the accuracy of matching and to reduce false matching of features, the space error-reduction procedure is used. It shows robustness against Additive White Gaussian Noise (AWGN), JPEG compression, and linear blurring but the main problem is the large load of processing complexity.

The previous discussion shows that this family of invariant image moments succeeds in solving and overcoming several problems of copy-move forgery. In addition, there are some other operations that make it easy to cover the forgery like rotation, scaling, and translation.

C. Algorithms Using Texture and Intensity Descriptors

The texture of an image refers to the structure of that image. This structure is inferred from intensity or colors changes appearing frequently in different patterns. Because of forgery changes, the statistics of the image may be invisible to a human. Invariant texture and intensity detection algorithms are methods used to analyze the relationship between pixels properties in a local area. Image texture reflects the spatial arrangement of color or intensities in an image or region. The image structure is analyzed by the characterization of the spatial relationship between objects in the image structure or by a statistical method. Statistical analysis of the image is accomplished by values arrangement of intensities in the whole image or region [20]. All invariant texture based algorithms use the rule that tampering harms the texture patterns of an image and texture descriptors can be employed to detect that tampering [25].

Zimba et al. [21] developed an algorithm to detect cloning forgery. Their goal was to reduce the processing complexity by reducing the image size itself approximately four times. They also reduced the feature vectors and selected the smallest feature vectors. First, DWT was applied on the color image to construct the four sub-bands (LL, LH, HL, and HH), and then they used the approximated image LL. Second, they divided this image into (bxb) overlapping blocks, and for each K blocks, they calculated a seven-feature vector (V1……V7). They sorted the features in a matrix with a fixed window, and then performed s slide over the sub-band pixel-by-pixel. Thirdly, they computed the shift vectors and calculated the distance between each feature vector and its shift. If it is greater than a threshold value T, therefore, there is no forgery, otherwise, the forgery exists. Unlike other algorithms, Zimba's algorithm used the radix sort instead of the lexicographical sort, and it used the seven-feature vectors to characterize each block. The algorithm has good detection accuracy with robustness against noise addition, JPEG

compression but it is not robust against all rotation angles and scaling.

Davarzani et al. [22] proposed a method that depends on dividing the image into overlapping blocks and then using Multi-resolution Local Binary Patterns (MLBP) to extract each block's feature vector. A lexographic map and a matching step are applied by using the k-d tree for more time reduction and to decrease feature dimensions. They used a Random Sample Consensus (RANSAC) algorithm to apply false match removal. The main advantage is the ability to precisely detect copy-moved regions even with scaling, rotation, blurring, JPEG compression, and noise addition. It cannot detect duplicated regions with different rotation angles.

Mushtaq et al. [23] developed a new algorithm that depends on if the local or statistical properties of an image are stable, slightly changeable or approximately frequent. So, the image has constant or homogenous texture. It uses Gray Level Run Length Matrix (GLRLM) based on reference pixels to analyze the image by intensity, length, and direction of the run. Features are extracted, and a linear Support Vector Machine (SVM) classifier is used to classify the extracted features. The algorithm is effective in copy-move forgery detection and image splicing. It suffers from a large percentage of true negative ratio.

Sharma et al. [26] presented a new algorithm to detect copy-move forgery for forged regions up to size 12x12. The algorithm used only the monochrome images. If the examined image is a colored or RGB image, it must be converted to monochrome image first. After monochrome conversion, the image is divided into overlapping blocks of size (BxB), and then Center Symmetric Local Binary Patterns (CSLBP) is applied to extract features. Taking a pixel as a reference in position (X, Y), which has N equally-spaced surrounding pixels placed as a circle with radius R. The CSLBP produces $2^{N/2}$ binary patterns. Before comparing and matching of blocks, a lexicographic sorting is used with the extracted feature vector. To get the matched blocks, two thresholds have to be set; shift frequency threshold T_{shift} and Euclidian distance threshold (dist). By applying the algorithm on medical images, it resulted in a good robustness even with post-processing operations such as additive JPEG compression, Gaussian blurring, Gaussian noise, or mixed operation.

The previous explanations show that the algorithms based on invariant texture and intensity descriptors work with a good robustness and good processing time. These algorithms using the exploited texture, structure of the image, and the homogeneity. These properties represent the most important properties in the original image. In addition to image properties like colors, pixels coherence and general texture are used to detect image tampering.

D. Algorithms Using Invariant Key Points

In this family of algorithms, the algorithms don't divide the image into any type of block division. It is classified as non-block based algorithms. Invariant keypoints algorithms are based on extracting image features from all parts of the image to perform matching between different points of view of an object. These features are used also in object recognition. This technique is famous for its robustness with object rotation, scaling and is slightly invariant with changes in image illumination. There are a large number of local features that can be extracted from an image, and these features are extracted in four stages [27]. First, searches are performed over all image locations to identify points of interest, and at the same time invariant to rotation and scaling. Second, based on stability, the keypoints are selected and their locations are determined. Third, based on image gradient directions, each keypoint location is directed by one or more orientations. The next step is using the region around each keypoint to compute the average value of the keypoint gradient to face local shape distortion and illumination changes. A 128-dimensional feature vector f1×128 is generated for each keypoint. The feature vector consists of a row, column, scale, and orientation. This process is known as Scale Invariant Feature Transform (SIFT), and the same idea is applied to Speed up Robust Features (SURF).

Liu et al. [28] proposed a two-stage detection algorithm, which is developed to deal with copy-move attack. The algorithm combines two methods first use SIFT descriptor to local features extraction and eliminates false matched points by threshold distance. Second color and texture features are used by revised Gabor texture feature to determine the remainder false matched pairs. The two stages are applied in four steps. SIFT feature extraction and keypoint matching, neighboring keypoints removing, block color feature inspection and finally block texture feature examination. The algorithm shows a good performance in forgery detection even with very small duplicated regions that do not exceed 0.1% of the whole image. It shows robustness against geometrical changes as rotation, scaling and illumination changes reach to 60% darkness. It is not clear how its computational complexity is in large picture containing a huge number of keypoints.

Zhang et al. [29] developed a new method based on a combination between SIFT and bi-coherence method. The algorithm is applied in 4 steps. First, it extracts SIFT keypoints and applies matching. Second, based on a three-Point Center Clustering (3PCC) algorithm, it divides all matched keypoints into two clusters K1 and K2. Third, it uses RANSAC algorithm to improve the geometrical transform parameters between clusters K1 and K2 and removes the mismatched keypoints. Finally, reliable detection can be obtained by bi-coherence phase histogram. The algorithm verifies the accuracy rate or False Positive Rate and the detection performance is measured by the True Positive Rate. The bi-coherence phase feature is measured in terms of the True Classifying Rate (TCR). Results show the effectiveness of bi-coherence feature for decreasing the FPR and a good balance between ratios of mismatched keypoints and matching accuracy. It needs performance improvement to decrease the FPR and increase both the TPR and TCR.

Chihaoui et al. [30] innovated a new method based on hybridizing SIFT method to extract features and Singular Value Decomposition (SVD) method to match features. Firstly, the input image is examined by SIFT to produce SIFT keypoints. Secondly, a matching process is applied on it according to two parameters:

1) Similarity matrix which consists of values of the Euclidean distance calculated by equation 3, where D_x & D_y are two different descriptor vectors and x, y are two SIFT features that may be matched.

$$Dist_{x,y} = \sqrt{\sum_{x,y}^{n} (D_x - D_y)} \quad (3)$$

2) Proximity $m \times m$ matrix is factorized by SVD using equation 4.

$$G = USV^T \quad (4)$$

3) Feature points are matched by using a fixed threshold T_c to use between every two SIFT descriptors.

Thirdly, duplicated region detection is performed by comparing row, column, scale, and orientation of each pair of SIFT. Results show that the algorithm is robust to geometrical operations, but it needs improvement by reducing false matching rate.

Pandey et al. [31] developed a new algorithm which applies both SURF and SIFT. To speed up the examination of copy-move forgery detection, SURF is applied first. SURF keypoints are computed as 64-dimensional descriptors for each keypoint. The best ten matched keypoints are chosen. The g^{2NN} matching is applied to generalize 2 nearest neighbors by using a dynamic threshold. The process is applied again, but by using SIFTS keypoints. The algorithm computes the 128-dimensional keypoint descriptors, and then the best ten matches are chosen. The g^{2NN} matching is applied to generalize the 2 nearest neighbors by using dynamic thresholding. The results show that the algorithm offers both fast and robust copy-move forgery detection, and offers a good accuracy, and precision. It offers mall processing time, especially with dynamic thresholding which helps in removing outliers and generating accurate results. The algorithm needs to show how to improve the detection process for multiple copied objects, especially with a highly uniform texture that is not recovered by SURF or SIFT. More studies need to be done about the effects of using a dynamic threshold on processing complexity.

Other techniques attack SIFT keypoints used by SIFT-based algorithms to hide the copy-move attack effects. This enlarges the SIFT keypoints removal effects on the final perceptual quality of the image. Amerini et al. [32] evaluated a new technique that works on a perceptual image quality metrics to hide the distortion of the image quality affected by SIFT keypoints removal.

Costanzo et al. [33] studied SIFT keypoints removal and SIFT keypoints injection problem. They used three new detectors for image identification for which SIFT keypoints have been removed. The algorithm is based on consistencies in keypoints just like consistencies in image texture. The new detectors are responsible for searching about inconsistencies in keypoints distributions to detect SIFT keypoints removed. In addition, it detects the injected fake keypoints. The three detectors are keypoints to corner ratio detector, CHI square distance detector, and Support Vector Machine (SVM) detector. Keypoints to the corner ratio detector are based on two notifications. The first is SIFT keypoints locations, which are close to corners and to regions where two edges intersect. The second is the ability of removal attacks to hide keypoints removing process by copying of small regions to save the image content. The keypoints to corner ratio is detailed in equation 5.

$$KCR = \log_{10}(N_{Keypoints} / N_{corners}) \le T_1 \quad (5)$$

where $N_{corners}$ is the number of corners in a square region and $N_{Keypoints}$ is the total number of keypoints falling into such region. The KCR value of the tampered image should be smaller than the value of the authentic image. The CHI square distance detector is based on the fact that keypoints are centered in image regions by high variance and that SIFT discards keypoints that have low contrast. The CHI square distance detector is applied as follows:

A) The image is converted to gray-scale levels by dividing it into 32x32 non-overlapping blocks, and then SIFT keypoints are detected. Classification is made for each block according to the variance of low, medium, and high classes.

B) Compute the percentage, where each block contains a number of keypoints and classify the output percentage to h_l, h_m and h_h.

C) Attack the image by Classification Based Attack (CLBA) and repeat steps 1 and 2 on the tampered image to show the difference between the percentage of the original image and tampered image by the histogram. The histogram shows that the difference in variance at the authentic image is larger than the difference in variance in tampered images.

The Support Vector Machine (SVM) detector is performed to an image to assign as tampered if SVM output is higher than a certain threshold value. The algorithm tests its new detectors by testing the increase of complexity in two cases. The first case is when only the keypoints are removed and the second is when fake keypoints are injected into the image. The experimental results show that the new detectors are effective against both keypoints removal and fake keypoints injection which are applied to hide copy-move forgery.

This family is offering heavy duty algorithms overcome copy-move attack based on SIFT features and prove higher performance than any other techniques.

E. Algorithms Based on Mutual Information

The first time that mutual information idea was proposed was by Soleimani et al. [34]. Image template matching indicates the dependency between two random variables. The authors tried to estimate the joint probability matrix of two regions or random variables by mutual information. Mutual information is at its maximum value, when two regions or random variables are dependants (one of them is a function of the other). In this case, the joint probability matrix is diagonal, and in the case of independent regions or variables, the mutual information equals zero. Entropy function offers a good way to represent random variable as in Equation 6. The joint entropy between two random variables A and B is defined by Equation 7. The mutual information between A and B is defined by Equation 8. The two random variables A and B are independent, when $P(A,B) = P(A) \cdot P(B)$, and the mutual information equals zero. If they are dependant, the joint probability matrix gives a diagonal

value, where $H(A)$ the entropy of point A is and $P(A)$ is the position of point A.

$$H(A) = \sum P(A)\log(1/P(A)) \quad (6)$$

$$H(A,B) = \sum P(A,B)\log(1/P(A,B)) \quad (7)$$

$$H(A,B) = \sum_{A,B} P(A,B)\log(P(A,B)/P(A,B)) \quad (8)$$

Chakraborty [35] proposed a new technique based on the method of Soleimani et al. [34]. It detects copy-move forgery based on mutual information search for duplicated regions without extracting any features of the image. The steps of the algorithm are:

1) For the input image I with size M x N, divide the image into non-overlapping blocks of size m x n.
2) For each block Bi and embedded image region Rj, two matrices are represented.
3) Calculate the joint probability distribution using a histogram of the two regions represented by two matrices.
4) Calculate the mutual information between them as in equation 8. If the regions are not duplicated, the mutual information value equals zero. On the other hand, if the regions are duplicated, the mutual information gives a diagonal matrix. The mutual information threshold w is used.

The value of the mutual information exceeds a certain threshold, and this means a false rejection, and a lower threshold means false duplication detection probability.

The main advantage of this technique is its simplicity and its high speed. It does not extract any features from the image, it depends only on a mathematical way, and also it gives quite robustness against illumination changes. However, it needs more examinations about large illumination changes and other post-processing operations.

F. Algorithms Using SVD

Singular Value Decomposition (SVD) is an effective numerical analysis method to analyze matrices. An image is represented in an array of the non-negative scalar matrix which can be broken down into three orthogonal matrices, a diagonal Matrix, and a transpose of the orthogonal matrix. The SVD is a good way to extract geometric features from an image. The SVD is represented by Equation 9, where A is the original non-negative matrix or square image [36].

$$A = USV^T \quad (9)$$

Li Kang et al. [37] proposed a block-based algorithm, which divides the image into blocks. The SVD is applied to each block to the extract feature vectors for each one. After that, a lexicographical representation is built. A matching search with a coefficient threshold is performed to obtain the duplicated regions. Results show that the algorithm has low complexity with good detection ability, but it not robust against geometric operations.

Bhosale et al. [38] employed both SVD and wavelet transform for tampering detection without knowing the original image. The algorithm firstly embeds a pseudo-random bit sequence as a watermark in the revised image by using DCT coefficients. Secondly, for the image X , it applies a wavelet transform then obtains the inverse image $\overline{X}$ and compares if the watermark is changed or not. The SVD is employed to retrieve the content of the original image. The results show that the algorithm has the ability to detect forgery due to wavelet transform and retrieve the original image due to SVD. The SVD provides the location of the tampered regions in the image, but it needs more improvements in error concealment and recovering the tampered data. In addition, a comprehensive study is needed for the effects of geometric operations and robustness.

Zhao et al. [39] proposed a new algorithm, which uses the DCT and SVD to decrease the computational time complexity. It reduces the size of the checked region by dividing the image into two levels of sub-blocks. The algorithm steps are defined as:

1) Convert the suspicious image from color level into RGB gray-scale level.
2) Divide the image into fixed size $b \times b$ overlapping blocks.
3) Perform 2D-DCT for each block to get the quantized DCT coefficients.
4) To reduce the computational time, the quantized blocks are divided into non-overlapping sub-blocks.
5) Apply the SVD on each quantized sub-block to extract the feature vectors for each one and a lexicographical representation is built.
6) By using a predefining shift frequency threshold T_{shift} , matching of similar pairs of blocks and detecting the forgery are performed. The previous steps are applied according to equations 10-12.

$$S = (s_1, S_2) = (i_1 - i_2, j_1 - j_2) \quad (10)$$

$$C(s_1, s_2) = C(s_1, s_2) + 1 \quad (11)$$

$$C(S_n) > T_{shift} \quad (12)$$

where S is the shift vector and all normalized shift vectors are $S_1, S_2, \ldots\ldots, S_n$. C is the shift vector counter. Results show that the algorithm is more robust than all previous algorithms, where it can effectively detect multiple duplicated regions. In addition, it detects the locations of duplicated regions. The algorithm is robust against post-processing operations like Gaussian blurring, Gaussian noise, JPEG compression and AWGN with a large value of precision. This family offers medium performance level, especially when SVD is used only, but the performance gets enhanced when other transformations are applied with SVD.

V. CONCLUSION

This paper illustrated the meaning of digital image forensics and its aspects in general. It also focused on copy-move forgery, especially. The paper is divided into two parts; the first part discussed types of digital image forgery and how this forgery is implemented. In addition, the effects of different forgery types on the final tampered image have been discussed. The second part focused on families of copy-move detection algorithms and the latest algorithms under each family. All algorithms have been classified by two aspects. Firstly, the computational complexity inferred from run time complexity under different resources has been studied. This complexity makes the algorithm fast and easy to perform or slow and complicated.

TABLE I
A COMPARISON BETWEEN COPY-MOVE DETECTION FAMILIES

Performing Steps		Families and Algorithms					
		DCT **Maind et al. [14]**	**Invariant Image Moments** **Ryu et al. [19]**	**Texture and Intensity Descriptors** **Sharma et al. [26]**	**Invariant Keypoints** **Costanzo et al. [33]**	**Mutual Information** **Chakraborty [35]**	**SVD** **Zhao et al. [39]**
Pre-processing	**- Grayscale conversions:**	-Yes	-Yes	-Yes	-Yes	-No	-Yes -N0
	- Resizing :	-No	-No	-No	-No	-N0	
Block division	**- Division :**	-Overlapping circular blocks.	-Overlapping blocks.	-Overlapping blocks.	- Non-overlapping blocks.	- Non-overlapping blocks.	- Overlapping blocks then non-overlapping sub-blocks.
	- Block size :	-Fixed size 8x8 pixels.	- fixed size *(B x B)*.	- fixed size *(B x B)*.	-fixed size 32 x 32	-fixed size m x n.	- Fixed size b x b.
Features Extraction	**-Method :**	- Apply DCT on each circular block to extract DCT coefficients.	-Use Zernike moments to extract feature vectors of each block.	- Apply (CSLBP) to each block and Feature of a block representing by a row in the feature matrix.	Extracts SIFT features and use KCR, CHI square distance detector and SVM detector.	----------	- Gets DCT coefficients for each block then, apply SVD on each sub-block to extract the features vector.
	-Numbers :	- Four features vector (V1, V2, V3 and V4).	- 12 moments used as feature vectors.	- 2^ (N/2) binary patterns where N is the number of surrounding pixels.	-Depends on SIFT keypoints.	----------	- Depends on sub-blocks numbers.
Matching	**- Sorting :**	- Lexicographically representation.	- Lexicographically representation.	- Lexicographically representation.	- Lexicographically representation.	----------	- Lexicographically representation.
	-Matching Methodology:	- Using Euclidean distance between vectors of two pairs blocks.	-Using locality Sensitive Hashing (LSH) to match similarities between Features vectors among all blocks.	- CSLBP produces 2^(N/2) binary patterns with circular radius R used as features.	- classify the output keypoints to *h1*,*hm* and *hh* then, use CLBA to detects the difference in variance between tested image and CLBA tampered image.	- By histogram, calculate two matrices represents the joint probability distribution of two regions block *B(i)* & embedded image *R(j)* with test threshold.	- Using a threshold *T(shift)* to match similar pairs of blocks with user-specified parameter Td and Euclidian distance threshold *(dist)*.
Verification Test		Threshold distance and morphological operation is used.	Use set of SATs thresholds for minimum Euclidean distance in addition to Space Error Reduction procedure (ERP).	Using shift frequency threshold *T(shift)* and Euclidian distance threshold *(dist)*.	**KCR** value should be smaller than its value in the authentic image. If **SVM** output is higher than a certain threshold value the image is tampered	Using mutual information value, if the regions are not duplicated its mutual information value equal zero otherwise it gives a diagonal value.	The morphologically open operation is applied to fill the holes in marked regions and remove the isolated blocks.
Computational Complexity		Low computational complexity due to low dimension size of features vectors and block size.	Medium computational complexity because it performs two matching procedure LSH and ERP.	Low computational complexity.	High computational complexity due to large number of its iteration with large number of detectors and features	Low complexity because it not needs to extract features or apply matching procedure.	Low computational complexity due to reducing the size of the checked region by divide the image into two sub-blocks levels.

TABLE II
A COMPARISON BETWEEN ALGORITHMS ROBUSTNESS AGAINST DIFFERENT PROCESSING OPERATIONS

Families and algorithms		Number of thresholds	Robustness against intermediate processes				Robustness against post-processing operations			Estimate the affine transform
			Reflection	Rotation	Scaling	Illumination changes	JPEG compression	Blurring	Gaussian white noise	
DCT	Maind et al. [14]	2	No	No	No	No	Yes	Yes	Yes	No
Invariant Image Moments	Ryu et al. [19]	4	Yes	Yes	No	No	Yes	Yes	Yes	Yes
Texture and intensity	Sharma et al. [26]	2	No	No	No	No	Yes	Yes	Yes	No
Invariant Keypoints	Costanzo et al. [33]	3	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes
Mutual Information	Chakraborty [35]	1	No	No	No	Yes	No	No	No	No
SVD	Zhao et al. [39]	3	No	No	No	No	Yes	Yes	Yes	No

Secondly, the algorithm robustness to different processes applied on digital forged images to hide forgery has been studied. The paper also offered two comparisons. The first comparison discussed in Table I showed the best algorithms in each family. The second compression discussed in Table II shows the robustness of each algorithm against processes applied on the forged image to distract about manipulation in the image.

From the two tables, it is clear that algorithms that achieve the first goal are [14], [26], [35] and [39], while the algorithm in [19] offers medium complexity and the algorithm in [33] offers high complexity. The second goal has been achieved by the algorithm in [33] and particularly by the algorithm in [19] under families of invariant key points and invariant image moments, respectively. To achieve robustness, we might sacrifice the goal of low complexity because algorithms need to perform complex operations in addition to transformations on a large number of features and detectors. So, there are disparities between the different algorithms about the percentage that each algorithm reaches the two goals.

REFERENCES

[1] Eric Kee, Hany Farid, "Exposing Digital Forgeries from 3-D Lighting Environments", IEEE WIFS'2010, 978-1-4244-9080-6/10, Seattle, USA, WA December 12-15, 2010.

[2] Eric Kee, James F. O'Brien, Berkeley and Hany Farid, "Exposing Photo Manipulation from Shading and Shadows", ACM Transactions on Graphics, V (N): 1–21, SIGGRAPH 2014.

[3] Osamah M. Al-Qershi , Bee Ee Khoo, "Passive detection of copy-move forgery in digital images: State-of-the-art ", Forensic Science International, 284–295, 3 July 2013.

[4] Alessandro Piva, "An Overview on Image Forensics", ISRN Signal Processing, Volume 2013, Article ID 496701, 2013.

[5] Christian Rey, Jean-Luc Dugelay, "A survey of watermarking algorithms for image authentication", EURASIP Journal on Applied Signal Processing, 613–621, 2002.

[6] Gajanan K. Birajdar, Vijay H. Mankar, "Digital image forgery detection using passive techniques: A survey", Digital Investigation, 226–245, 10 (2013).

[7] Judith A. Redi, Wiem Taktak, Jean-Luc Dugelay, "Digital image forensics: a booklet for beginners", Multimedia Tools Appl. 51, 133–162, (1) (2011).

[8] SALAM A.THAJEEL, GHAZALI SULONG, "A SURVEY OF COPY-MOVE FORGERY DETECTION TECHNIQUES", Journal of Theoretical and Applied Information Technology, Vol.70 No.1, 10th December 2014.

[9] M. Ali Qureshi, M.Deriche, "A Review on Copy-moveImage Forgery Detection Techniques", Multi-Conference on Systems, Signals & Devices (SSD), 11-14 February 2014.

[10] http://www.wikipedia.org/wiki/morphing.

[11] Tu K.Huynh, Thuong Le-Tien, Khoa V.Huynh, Sy C.Nguyen, "A Survey on Image Forgery Detection Techniques", The 2015 IEEE RIVF International Conference on Computing & Communication Technologies Research, Innovation, and Vision for Future (RIVF), 71-76, 25-28 Jan. 2015.

[12] J. Fridrich, D. Soukal, J. Luka´ s, "Detection of copy-move forgery in digital images", Proceedings of DFRWS 2003, Cleveland, USA, 2003.

[13] Sunil Kumar, Jagannath Desai, Shaktidev Mukherjee, "A Fast DCT Based Method for Copy-moveForgery Detection", IEEE Second International Conference on Image Information Processing (ICIIP), 649 – 654, 9-11 Dec. 2013.

[14] Rohini.A.Maind, Alka Khade, D.K.Chitre, "Image Copy-moveForgery Detection using Block Representing Method", International Journal of Soft Computing and Engineering (IJSCE), 2231-2307, Volume-4, Issue-2, May 2014.

[15] Sondos M.Fadl, Noura A.Semary, "A Proposed Accelerated Image Copy-Move Forgery Detection", Visual Communications and Image Processing Conference, IEEE, 253 – 257, 7-10 Dec. 2014.

[16] Guangjie Liua, Junwen Wanga, Shiguo Lianb, Zhiquan Wanga, "A passive image authentication scheme for detecting region-duplication forgery with rotation", Journal of Network and Computer Applications , Volume 34, Issue 5, 1557–1565, 2010.

[17] Ghulam Muhammad, Muhammad Hussain, "Passive Detection of Copy-Move Image Forgery using Undecimated Wavelets and Zernike Moments", Information Journal, Vol.16, No.5, 2957-2964, May 2013.

[18] Jiyun YANG, Pei RAN, Di XIAO, Jinyong TAN,"Digital Image Forgery Forensics by Using Undecimated Dyadic Wavelet Transform and Zernike Moments", Journal of Computational Information Systems, 6399–6408, 15 August, 2013.

[19] Seung-Jin Ryu, Matthias Kirchner, Min-Jeong Lee, and Heung-Kyu Lee, "Rotation Invariant Localization of Duplicated Image Regions Based on Zernike Moments", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 8, NO. 8, 1355 – 1370, AUGUST 2013.

[20] Linda G. Shapiro and George C. Stockman, Computer Vision, Upper Saddle River: Prentice–Hall, 2001.

[21] Michael Zimba, Sun Xingming, "Fast and Robust Image Cloning Detection using Block Characteristics of DWT Coefficients", International Journal of Digital Content Technology and its Applications. Volume 5, Number 7, July 2011.

[22] Reza Davarzani, Khashayar Yaghmaie, Saeed Mozaffari, Meysam Tapak, "Copy-move forgery detection using multiresolution local binary patterns", Forensic Science International 231, 61-72, 2013.

[23] Saba Mushtaq, Ajaz Hussain Mir," Forgery Detection Using Statistical Features", International Conference on Innovative Applications of Computational Intelligence on Power, Energy and Controls with their Impact on Humanity (CIPECH14) 28 & 29 November 2014.

[24] Guzin Ulutas, Mustafa Ulutas, "IMAGE FORGERY DETECTION USING COLOR COHERENCE VECTOR", International Conference on Electronics, Computer and Computation (ICECCO), 107 – 110, Ankara, 7-9 Nov. 2013.

[25] Muhammad Hussain, Sahar Q. Saleh, Hatim Aboalsamh, Ghulam Muhammad, George Bebis, "Comparison between WLD and LBP Descriptors for Non-intrusive Image Forgery Detection", IEEE International Symposium on Innovations in Intelligent Systems and Applications (INISTA) Proceedings, 197-204, Alberobello, 23-25 June 2014.

[26] Surbhi Sharma, Umesh Ghanekar, "A rotationally invariant texture descriptor to detect copy-moveforgery in medical images", IEEE International Conference on Computational Intelligence & Communication Technology, 795-798, Ghaziabad, 13-14 Feb. 2015.

[27] David G. Lowe, "Distinctive Image Features from Scale-Invariant Keypoints", international Journal of Computer Vision, Volume 60, Issue 2, pp 91-110, November 2004.
[28] Bo Liu, Chi-Man Pun, "A SIFT and Local Features Based Integrated Method for Copy-Move Attack Detection in Digital Image", IEEE International Conference on Information and Automation (ICIA), 865 - 869, Yinchuan, 26-28 Aug. 2013.
[29] Ju zhang, Qiuqi ruan,Yi jin, "COMBINED SIFT AND BI-COHERENCE FEATURES TO DETECT IMAGE FORGERY", International Conference on Signal Processing (ICSP), 1859 - 1863, Hangzhou, 19-23 Oct. 2014.
[30] Takwa Chihaoui, Sami Bourouis, and Kamel Hamrouni, " COPY-MOVE IMAGE FORGERY DETECTION BASED ON SIFT DESCRIPTORS AND SVD-MATCHING", 1st International Conference on Advanced Technologies for Signal and Image Processing – ATSIP, 125 - 129, Sousse, Tunisia, 17-19 March, 2014.
[31] Ramesh Chand Pandey, Sanjay Kumar Singh, K. K. Shukla and Rishabh Agrawal, "Fast and Robust Passive Copy-Move Forgery Detection Using SURF and SIFT Image Features", 9th International Systems Conference on Industrial and Information (ICIIS), 1 - 6, Gwalior, 15-17 Dec. 2014.
[32] I. Amerini, F. Battisti, R. Caldelli, M. Carli, A. Costanzo, " EXPLOITING PERCEPTUAL QUALITY ISSUES IN COUNTERING SIFT-BASED FORENSIC METHODS", IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2664 - 2668, Florence, 4-9 May 2014.
[33] Andrea Costanzo, Irene Amerini, Roberto Caldelli, Mauro Barni, " Forensic Analysis of SIFT Keypoint Removal and Injection", IEEE Transactions on Information Forensics and Security, Volume: 9, Issue: 9, 1450 - 1464, Sept. 2014.
[34] Hussein Soleimani, Mohammadali Khosravifard, "Mutual Information-Based Image Template Matching with Small Template Size", 7th Iranian Machine Vision and Image Processing (MVIP), 1 - 5, Tehran, 16-17 Nov. 2011.
[35] Somnath Chakraborty, "Copy-moveImage Forgery Detection Using Mutual Information", Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT), 1 - 4, Tiruchengode, 4-6 July 2013.
[36] V. Klema, A. J. Laub, "The singular value decomposition: Its computation and some application", IEEE Transactions on Automatic Control, Volume: 25, Issue: 2, 164 - 176, Apr 1980.
[37] Li Kang, Xiao-ping Cheng, "Copy-move forgery detection in digital image", 3rd International Congress on Image and Signal Processing (CISP), Volume: 5, 2419 - 2421, Yantai, 16-18 Oct. 2010.
[38] S arika Bhosale, Ganesh Thube, Pooja Jangam, Rushikesh Borse, " Employing SVD and Wavelets for Digital Image Forensics and Tampering Detection", International Conference on Advances in Mobile Network, Communication and its Applications (MNCAPPS), 135 - 138, Bangalore, 1-2 Aug. 2012.
[39] Jie Zhao, Jichang Guo, "Passive forensics for copy-move image forgery using a method based on DCT and SVD", Forensic Science International 233, 158 - 166, September 2013.