Institución Universitaria SALAZAR Y HERRERA

QUID Nº28, pp. 78-92, enero-junio de 2017, ISSN: 1692-343X, Medellín-Colombia

IDENTIFICATION OF MANIPULATION IN DIGITAL IMAGES THROUGH HYBRID BLOCK-BASED AND KEY POINTS ALGORITHM

(Recibido el 16-01-2017. Aprobado el 11-04-2017)

MSc Mohammad Hossein Tirnaz
Islamic Azad university, *Faculty of Mechatronics Science and Research Branch of Alborz, Karaj, Iran*
Research@QIAU.ac.ir

PhD. Azam Bastan fard
Islamic Azad University, *Department of computer engineering Science and Research Branch of Alborz, Karaj, Iran*

Abstract: Nowadays, digital images in many legal centers are considered as a source of information and request to determine the authenticity of an image has increased dramatically. In this paper, an efficient algorithm to check and identify manipulation in which a combination of block-based methods and key points for the extraction of forged parts has been implemented. In the proposed algorithm, the input image is taken at First. After compliance with the test target which is based on database, it is recognized that whether the image has been manipulated or not. In case of observing a positive result, it is concluded that that forgery has been made. First, the input image is divided into irregular and non-overlapping blocks using simple clustering algorithm (SLIC)[1]. Then, feature points as the characteristics of the blocks are extracted using local binary method with several resolutions. Block attributes are adapted with each other to identify Areas suspected of forgery. In the second stage, for more accurate diagnosis of forging parts, characteristic points were replaced with small super-pixels as characteristic blocks and adjacent Features of blocks are replaced with the characteristics of positional color which are similar to feature blocks to produce consolidated areas. Finally, RANSAC[2] algorithm on integrated areas is used to remove false matches. Experimental results using a test database and forgery rotation methods, blurring, jpeg compression and etc., show that the proposed algorithm in the field of detection of copy-transfer forgery has reached to 97 percent and has also achieved recall rate of 98 percent.it has been improved 3 percent compared to other valid methods in terms of recalling and precision. This algorithm can even identify rotation methods, blur and jpeg compression by calculation which have less complexity.

Keywords: areas suspected of forgery, super pixel, block features, extraction of forged areas, the characteristic points, social networks

Citar, estilo APA: Bastan fard, A., & Hossein, M. (2017). IDENTIFICATION OF MANIPULATION IN DIGITAL IMAGES THROUGH HYBRID BLOCK-BASED AND KEY POINTS ALGORITHM. *Revista QUID (28)*, 78-92.

[1] **Simple Linear Iterative Clustering**
[2] **random sample consensus**

1. INTRODUCTION

Forgery of digital images has been very simple with the development of computer technology and image processing software. However, digital images are common sources of information. Therefore the reliability of digital images has become an important issue**.** In recent years, more and more researchers have focused on the issue of manipulating digital images. Among existing types of manipulation, copy-transfer forgery can be cited which means copying and then pasting the copied areas of an image in other parts of the same image. During copy-transfer operations, some of the image processing methods such as rotation, scaling, blurring, compression and addition of noise, are augmented to make forge acceptable for presenter, as copied and transferred parts, are copied from the same image. Noise component, characteristic of color and other key properties are compatible with the rest of the picture. Some of forgery detection methods which are based on specifications of related picture are not applicable in this case. During previous years, many counterfeit detection methods have been proposed to detect counterfeit copy-transfer like pixel-based method, techniques based on image format, camera-based approaches and etc.
Such methods are presented completely in figure 1.

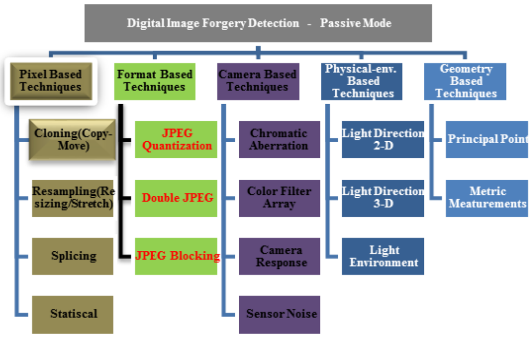


Fig 1. Categorization of identifying manipulated digital images

According to existing procedures, copy-transfer forgery detection methods can be divided into two categories: block-based algorithms and algorithms on the basis of key points. (Pun et al., 2011). In Forgery detection methods based on the blocks, the input image is divided to regular and overlapped blocks (circular - square - rectangular). Then, manipulated area can be obtained with compliance of blocks of the image pixels or transfer coefficients. These methods have three fundamental flaws. Firstly, the larger is the image size, the higher is the computational cost. Secondly, these methods are not able to identify geometric transformations accurately. Thirdly, the call rate is low.

• Forgery detection methods based on a key point, in which key points are extracted, are matched together throughout the image to identify duplicated areas. Algorithms including SIFT[3] (Amerini et al., 2011) and SURF[4] (Bo et al., 2010) are used to extract features. Although these methods can locate adapted key points, most of them cannot locate forged areas well. Therefore, they are not able to achieve correct and satisfying detection as well as stable and high rate of recall. Examples of algorithms based on blocks and key points are shown in figure 2.

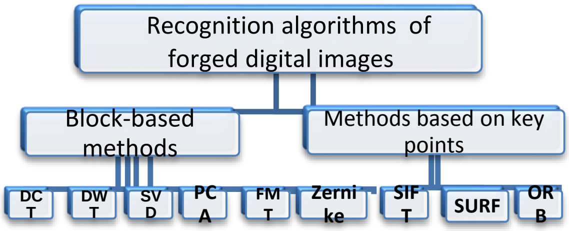

Recognition algorithms of forged digital images
Block-based methods
Methods based on key points
DCT
DWT
SVD
PCA
FMT
Zernike
SIFT
SURF
ORB

Fig 2. Methods and algorithms for identification of forged images

A new method to identify counterfeit copy-transfer using integration of forgery detection methods based on traditional block as well as forgery detection methods on the basis of key points is provided in order to address the above issues and solve earlier bugs.in this way, the rate of precision is raised and the percentage of error probabilities it declined. Moreover, rapid diagnosis of a variety of forging in the image is conducted in a way that can be a

[3] **Scale Invariant Feature Transform**

[4] **Speeded Up Robust Features**

presentable algorithm for authoritative institutions (courts, insurance, police, cyber police and etc.) and posted images on social networks which are considered one of the methods of criminals to destroy the reputations of natural and legal individuals can be trusted.

The rest of this article is organized as follows: Previous works are described in section 2; the proposed algorithm is presented in section 3, then, experimental obtained results are described in Section 4.comparison of the proposed method with the previous methods, was fully described this section. In Section 5, conclusions and an appropriate recommendations is provided to improve a method.

2. CONDUCTED RESEARCH

Reliability to photos has a major role in some fields including forensic investigation, criminal investigation, surveillance systems, intelligence services, medical imaging and journalism. The art of creating fake image has a long time history but today's digital era, has made Easy change in the provided information in the picture without observation of any trace of manipulation, possible. Some ways have been created to identify manipulating regarding the evolution of digital information and issues related to multimedia security. Identification method based on filtration and search operations and the nearest neighborhood was presented by B.Dybala et al. (Dybala et al., 2007). A way of detecting copy – transfer forgery was proposed by J.Fridrich et al. using the discrete cosine transform related to blocks overlapping and displays the words (Fridrich et al., 2003). Identifying the connection of image in case of facing a problem of detecting photo manipulation is one of the principal tasks. It is assumed in the picture connection that cut and paste of areas of an image has been done to another image. A method based on support vector machine (SVM) was offered by Dong et al. to identify the connection of an image. Their feature was acquired by detachable correlation analysis of image pixels and coherence arising from connection (Dong et al., 2008). Identification of connection scheme based on the extracted features of the moment from the discrete cosine transform as well as qualitative features of image was provided by Zhang et al. (Zhang et al., 2008).Image model based on geometry was presented by Shih-Fu Chang et al. to identify Graphics which was inspired by process of physical image production to classify real photographic and computerized images (Ng et al.,2005), (Ng et al.,2006). Online systems were also developed for the detection of photography and computer images by researchers (Ng et al.,2006), (Ng et al.,2007).effective Differentiation of paintings and images were proposed by A.Leykin using the properties of edge features for (. Leykin & Cutzu, 2003). A framework to distinguish between computer graphics and real images based on the integration of other features and procedure of feature selection were offered by G.Sankar et al. (Sankar et al., 2009). In order to change the image normally, the image should be loaded to an image editing application, and it should also be saved again after applying the changes. Complex procedures which are capable of finding the compression history, can be useful in detecting forgery (Fan & Queiroz, 2003). A method was proposed by Z. Fan and R. Queiroz based on the issue that an image has been compressed or not. A way to identify created composites of JPEG images and the difference in their qualities was presented by HanyFarid. This method can recognize whether a part of image is compressed in lower quality than the rest of image primarily or not (Farid, 2009). A method was also provided by W.Luo et al. to identify re-compressed blocks of image based on the properties of blocking JPEG effects (Luo et al., 2007), (Luo et al., 2007), (Qu et al., 2008). Regular identification method according to correlation models of the second partial derivatives was presented by H. Cao and Alex C. Kot in which correlation of internal channel and demosaicing cross-channel was detected (Cao et al., 2008), (Cao et al., 2009). A method to find forgery in the digital images through estimating the color of the light was provided by Gholap and Bora (Farid & Bravo, 2010).Additive noise is usually used to cancel the effects of manipulating and Elimination of flaws of some active and passive ways of forgery identification. Noise often becomes contradictory by creation of forgery in a digital image Therefore, identification of different levels of noise in an image may indicate manipulation. A method based on three feature sets of statistical noise were offered by H. Gou et al.,so that their properties are based on algorithms to remove noise, wavelet analysis and prediction of neighbors (Gou et al., 2007). A simple technique was proposed by A.Dirik et al. for identification of chromatic aberration based on the Operations to promote and mutual information (Dirik et al., 2007). In case of changing in an image, a combination of image processing operations is often applied to them. Identification the effects of these operations can be helpful in identification of forgeries. A method was developed by I.Avcibas et al. to distinguish between the original and processed image (Avcibas et al., 2004). A set of different features for identification of various image processing operations was used by Avcibas et al. according to creation of a classifier using features and based on the sizes similar to binary ones, image quality criteria, statistics of higher order wavelet as well as feature selection methods (Bayram et al., 2005).Three techniques for identifying the effects of image processing operations in the scientific illustrations were presented by H.Farid. In particular, image segmentation technique is used to identify the removal, restoration and replication (Farid, 2006). Most of forged pictures are created by combining two or more images of sources. Therefore, finding different parts of the image with the different blur characteristics (blurring contradictions) can be useful in identifying forgery of image. Furthermore, blurring operation is one of the common methods to cancel the effects of manipulating .Local blurring estimator to measure blurring rate of pixels along the edges of the image was presented by G.Cao et al. (Cao et al., 2010). A way was provided for identifying sharpened images by the same authors. The mentioned method was based on the histogram of deviation slope (aberration) and criteria of ringing effects (Cao et al., 2009). Identification method of manipulating based on the estimation of blurring was presented by D.Hsiao et al. (Hsiao & Pei, 2005). A method based on local entropy gradient was also offered by Z. Li and J.Zheng (Li & Bin Zheng, 2008). A technique to identify the effects of blurring was proposed by Zheng and M.Liu.Their work was based on wavelet homonorphic filter and procedure of mathematical morphology (Zheng & Liu, 2008). Detector of image Connecting based on sharp boundaries was presented by Z. Qu et al.,. Method of detecting forgery on the basis of the regular properties of wavelet coefficients was proposed by Y.Sutcu et al. which could be used in estimation of Sharpness and blurring rate of the edges (Sutcu et al., 2007). A way of non-uniformity of image response regarding imaging sensors was analyzed by Fridrich et al. (Fridrich, 2009). Hu moments to extract features of block were employed in reference (Liu et al., 2011). Mentioned method is applied to adjust rotation of region and common signal processing operations. Operation of rotation and re-scaling was provided by Wei et al. This method applies periodicity in the interpolated image for identification of the rejection of re-scaling. A united method was developed inspired by Wei et al. to determine the parameters of re-scaling and rotation. The methods such as ones presented by Wei et al., Stamn and Liu for identifying manipulation of the image, are limited to identification one or two operations of the image. A detailed explanation about the re-sampling identification, sequential rotation and scaling identification was presented again using separate samples (Wei et al., 2010). Polar coordinates were implemented by Solario and Nandi to acquire the constant of one-dimensional descriptor for reflection, rotation and scaling to identify doubled areas (Solario & Nandi, 2009).

3. PROPOSED ALGORITHM

Framework of proposed scheme of image forgery detection is shown in figure 3. The mentioned scheme which has two stages attempts to detect forgery using the proposed algorithm including block-based method and based on key points. Input image is divided to irregular and non-overlapping blocks at first using simple clustering algorithm.

Then, Local Binary Patterns (LBP) with several resolutions is applied in each block to extract feature points as characteristics of block. Subsequently, features of block are matched together. The feature points that have been fitted successfully together are determined as labeled feature points and are able to identify areas suspected of forgery.

In order to recognize areas of forgery more precisely in the second stage, the characteristic points are substituted with the small super-pixels as characteristic block and adjacent feature blocks are replaced with the characteristics of the local color which are similar to feature blocks to produce areas of integration.

Eventually, RANSAC algorithm is used to delete false matched ones on integrated areas. The rest of this section is organized as follows: In section 3.1, the proposed method of erratic blocking is introduced. Different Steps of extracting feature points of block are defined in section 3.2.

Feature Compliance process of block is explained in Section 3.3. Then, in Section 3.4, algorithm of extracting forged areas is presented and the database used in the experiments is described in section 3-5.

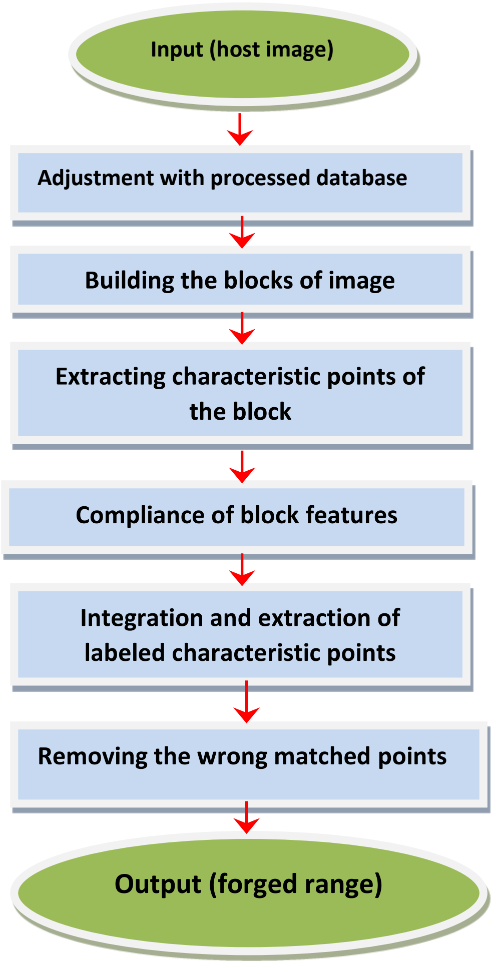

Input (host image)
Adjustment with processed database
Building the blocks of image
Extracting characteristic points of the block
Compliance of block features
Integration and extraction of labeled characteristic points
Removing the wrong matched points
Output (forged range)

Fig 3. Framework of proposed plan about copy-transfer forgery detection

3.1 algorithm of irregular block-making

For the detection of forgery in this stage, a block-matching algorithm is provided at first which can divide host image into irregular and non-overlapping blocks. Then, forged areas can be identified by complying irregular and non-overlapping areas. Since the image should be divided to non-overlapping areas of irregular shape, simple clustering algorithm (SLIC) is used in the implemented algorithm to divide image to meaningful and irregular super-pixels (Achanta et al.,). Non-overlapping blocking compared with the overlapping blocking can reduce the computational output using blocking of simple clustering; In addition, in most cases, significant and irregular areas can present forged areas better than regular blocks. A new method of block matching is presented in this algorithm which is able to determine the initial size of the Super pixels adaptively and based on the texture or design of host image. When the image texture is smooth, the initial size of the super pixels can be determined relatively large. Bigger super pixels imply a smaller number of blocks, so that when the blocks are matched, the computational cost is reduced. In contrast, when the texture of image includes more details, the initial size of the super pixels can be considered relatively small to be ensured completely of obtained results for forgery detection.

In the proposed method, dyadic wavelet transform is used to analyze the frequency distribution of the host image. Approximately, when the low-frequency component forms majority of the frequency component of the image, Host image will be smooth. If the low-frequency component only forms a small part of the frequency components of the image, Host image is a picture with detail.

Dyadic wavelet transform (DyWT) on the host image is used for determination and specification of the relationship between frequency distribution of host images and initial size of super-pixels in order to discover forgery (Cao et al., 2012), (Muhammad et al, 2012). Then, the low-frequency component (LL) and high-frequency component (HH) can be calculated using equations 1 and 2. Distribution Percentage of low-frequency P_{LL} can be obtained by using Equation 3, with these two components. Based on that, the initial size of S from super pixels can be defined like Equation 4.

$$C^{j+1}[n]=\sum_k h[k]c^j[n+2^j k] \quad \text{(LL)} \qquad (1)$$

$$d^{j+1}[n]=\sum_k g[k]c^j[n+2^j k]\text{(HH)} \qquad (2)$$

$$P_{LL}= \text{(LL/LL+HH).100\%} \qquad (3)$$

$$S=\begin{cases}\sqrt{0.02*M*N}P_{LL} > 50\% \\ \sqrt{0.01*M*N}P_{LL} \leq 50\%\end{cases} \qquad (4)$$

Briefly, the flowchart of the proposed method (Non-overlapping block-matching) is shown in Figure 4.

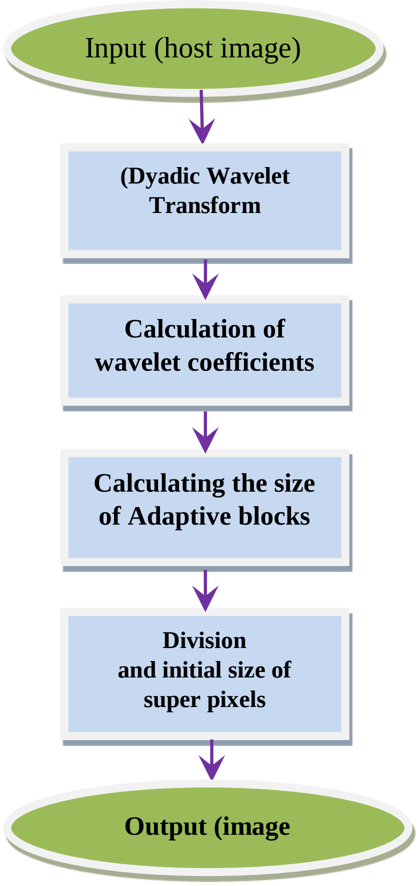


Fig 4. Steps of the matching method of non-overlapping and irregular blocks

As it was mentioned, the proposed method can achieve better results compared to conventional methods of forgery detection .Because it divides the host images to the fixed-size blocks and at the same time, decreases computing costs compared with most of forgery detection methods.

3.2 Algorithm of extracting characteristic points of block:

In this stage, features of block are extracted from the image blocks. Local binary patterns (LBP) are one of the most famous and most powerful descriptors of characteristic (Davarzani et al, 2013). This method has attracted the attention of scientists and has been applied in several analysis of images so far, as it has low computational complexity and it is fixed relative to changes of uniform gray scale .moreover it has the capability of describing the texture . In practice, LBP operator can combine statistical characteristics and analysis of texture structure together. The idea of LBP was proposed first by Ojala et al. for classifying tissue (ojala et al., 1996). Then, it has been developed for using in other applications of image analysis such as face recognition, investigating face, identification facial expressions, evaluation of moving objects, image retrieval, etc.

LBP also can easily extend to all points of its neighborhood with any number of pixels. Other trends of extension have been displayed in recent works, so that LBP can be used to determine the change of scalability and rotation as well. To extract the characteristics and attributes, desired images were divided based on irregular blocks. Then, filtering operation was done on the image blocks. This is usually conducted for images degraded by added noise or the blurring process. The results showed that this type of filtering can improve the efficiency of examination and Identification. After filtering, LBP should be obtained for each performed block to characteristics. As a result, LBP as a method of extracting feature points is selected in the proposed algorithm; so that the feature points are extracted from each image block and the feature each block are described by the block attribute that that has been extracted from the same block. Therefore, the feature of each block contains irregular information of block as well as extracted feature points by LBP.

3.3 Compliance of feature block

Matching blocks is used to find a similar pair of blocks by estimating the Euclidean distance of feature vectors. Imagine S_i and S_j represent the i-th and j-th rows of S, then the Euclidean distance are calculated as follows:

$$D(i,j)=\sqrt{\sum_{k=1}^{l}[S_i(k)-S_j(k)]^2} \qquad (5)$$

So that L is the feature vector. Block matching begins from the first row of the matrix S. Distances with the following features related to R_{lim} for S_i are calculated and thus the minimum distance can be achieved:

$$D(i,i+k)=\min\{D(i,i+1), D(i,i+2),. D(i,i+R_{lim})\} \qquad (6)$$

In above mentioned relation, (i + k) is a row with the minimum distance of S_i .To determine whether two feature are properly matched or not, a similarity threshold is accepted which is shown as T_s. If D (i, i + k) D is smaller than T_s, *i- th* and (i + K)- *th* blocks are successfully complied. Then Their Indices are stored in a set of Ω. Otherwise, no match is found for S_i and it is not removed from S . This process is repeated for all the features in S . Finally, the entire pairs of matching blocks are recorded in Ω which leads to the extraction of areas suspected to be forged.

3.4. Algorithm of extracting forged areas

Even though, labeled feature points were extracted in the previous steps which were the only positions are forgery areas, forgery areas should be also located.

With the regard to the issue that super pixels can divide host image well, a method is proposed in which labeled feature points are replaced with small super pixels for Identification of areas suspected of forgery, and it is a combination of labeled super-small pixels.

In addition, local color feature of super pixels which are adjacent to areas suspected of forgery should be measured to improved precision and results of calls. If their color features are similar to the color feature of areas suspected to forgery, super pixels which are adjacent areas are merged in corresponding suspected areas. In this way, integrated areas are produced.

Finally, a deletion operation of false matched ones is applied on the combined areas to detect copy-transfer forgery areas. Figure 5 shows the flowchart of algorithm for extracting forged areas which is described in detail in the following.

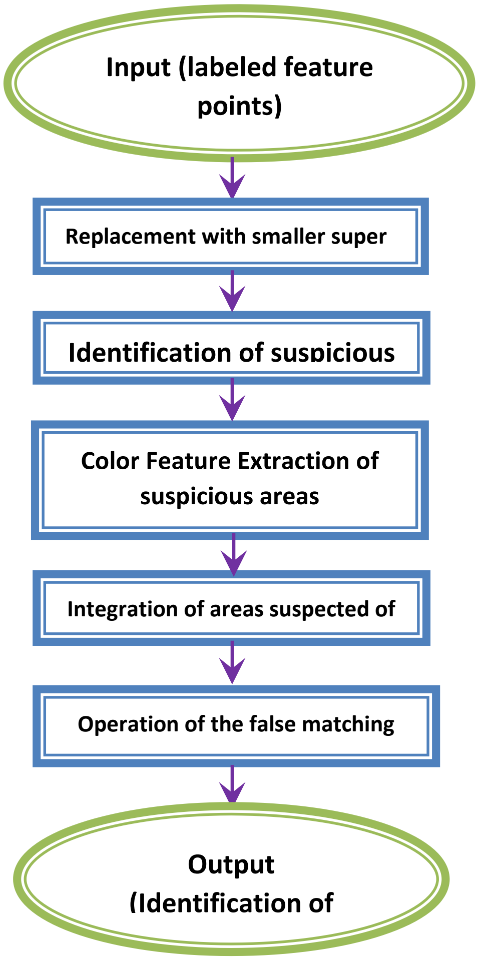

Input (labeled feature points)
Replacement with smaller super
Identification of suspicious
Color Feature Extraction of suspicious areas
Integration of areas suspected of
Operation of the false matching
Output (Identification of

Fig 5. Flowchart of the algorithm of extracting forged area

3.4.1. Different steps of extracting forged areas

Labeled feature points are as the input of this stage of the implemented algorithm. Identified forged areas are also specified in output. The basic steps of this process are as follows:

Step 1. Labeled feature points are loaded. Then, the simple clustering algorithm is applied with the initial size of S on the image to divide it into small super pixels (as blocks of feature). Each labeled feature point is replaced with the corresponding feature block to identify areas suspected to be counterfeit.

Step 2: localized color feature of super pixels adjacent to suspected areas (adjacent blocks) are measured. When their color feature becomes similar to the suspected areas, adjacent blocks are integrated in their corresponding suspected areas and thus the new integrated areas are arisen.

Step 3: Removal operation of false matched ones is applied in integrated areas in a way that finally identified fake areas are produced.

In step 1, it is assumed that LPF=$\{\langle LP_1.\overline{LP_1}\rangle.\langle LP_2.\overline{LP_2}\rangle.\cdots\ .\ \overline{P_n}\rangle\}$ .in the equation, $\langle LP_i;\overline{LP_i}\rangle$ shows a pair of matched feature point. *i* means *i-th* pair of point feature is labeled, in which i=1,2,… and n is the total number of feature points in labeled feature points. Suspected areas consist of SR=$\{\langle LS_1.\overline{LS_1}\rangle.\langle LS_2.\overline{LS_2}\rangle.\cdots\ .\ \overline{S_n}\rangle\}$, the initial size of the (S) in SLIC algorithm which has been used to zoning host image to small super pixels as it is associated with the size of host images. Generally in this method, for high-quality images like when the image size is approximately 3000 * 3000, initial size is set equal to s = 20 while the initial size for an image with approximate dimensions of 1500 x 1500 is determined as S = 10.

In step 2, for each suspected area $SR_i=\langle LS_i.\overline{LS_i}\rangle$, adjacent blocks are defined as follows:

$SR_i_neighbor=\left\langle LS_{i_\theta}.\overline{LS_{i_\theta}}\right\rangle$in which= $\{45°.90°.135°.180°.225°.270°.315°.360°\}$.

Then, feature of localized color in suspected area (SR_i) and its adjacent blocks ($SR_i\_neighbor$) are measured using equations 7 and 8.

$$F_c\_LS_i=\frac{R(LS_i)+G(LS_i)+B(LS_i)}{3}$$

$$F_c\_\overline{LS_i}=\frac{R(\overline{LS_i})+G(\overline{LS_i})+B(\overline{LS_i})}{3} \qquad (7)$$

$$F_c\_LS_{i\_\theta}=\frac{R\left(LS_{i\_\theta}\right)+G(LS_{i\_}\theta)+B\left(LS_{i\_\theta}\right)}{3}$$

$$F_c\_\overline{LS_{i\_\theta}}=\frac{R\left(\overline{LS_{i\_\theta}}\right)+G\left(\overline{LS_{i\_\theta}}\right)+B\left(\overline{LS_{i\_\theta}}\right)}{3} \qquad (8)$$

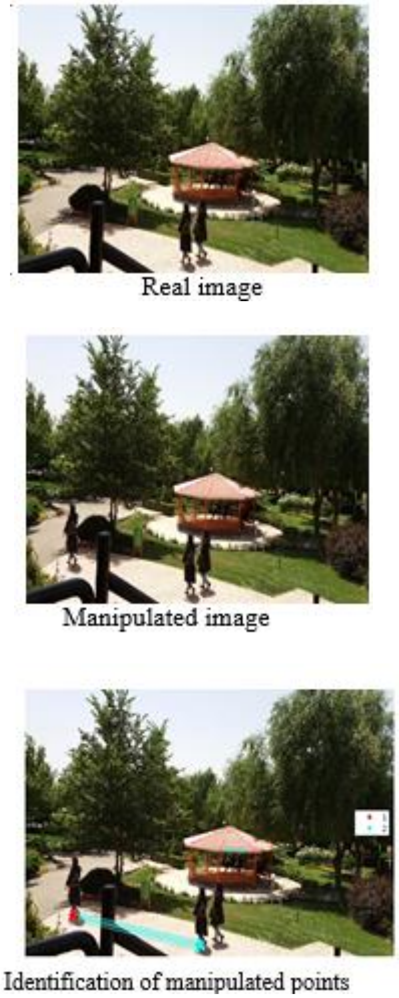
In this equations, R (), G (), B () mean calculation of the RGB components of the corresponding block. When localized color characteristic of adjacent blocks are similar to color property of the corresponding suspected areas, localized features can satisfy the defined conditions in equation 9 and adjacent block is integrated within the corresponding suspected area of the forgery.

$$\left|F_c\_LS_i - F_c\_LS_{i\_\theta}\right| \le TR_{sim}$$

$$\left|F_c\_\overline{LS_i} - F_c\_\overline{LS_{i\_\theta}}\right| \le TR_{sim} \qquad (9)$$

Where $F_c\_\overline{LS_i}$ and $F_c\_LS_i$ are localized features of SR corresponding suspected area, $F_c\_LS_{i\_\theta}$, $F_c\_\overline{LS_{i\_\theta}}$, $SR_i=\langle LS_i.\overline{LS_i}\rangle$ and SR_i are features of localized color of adjacent blocks , ($SR_i\_neigbor$): $SR_i\_neighbor=\left\langle LS_{i\_\theta}.\overline{LS_{i\_\theta}}\right\rangle$ ‹TR_{sim} is threshold of similarity measure among the characteristics of the localized color.

Finally, in Step 3,RANSAC algorithm for determining internal effective factors within the matched blocks are used in Similar Blocks Matrix (SBM) data points which have been created based on rotation, Scaling and Translation (RST). Then false matched ones can be deleted among other effective external factors. Thus, parameters of such transformation can be estimated and finally all invalid matched blocks can be eliminated. RANSAC algorithm can estimate model parameters with high precision even when there are a large number of inconsistent pairs (.Fischler & Bolles, 1981). An example of identifying forged regions in the proposed algorithm can be observed in Figure 6.



Real image

Manipulated image

Identification of manipulated points

Fig 6. Example of identifying counterfeit areas related to the picture of Islamic Azad University of Karaj in the implemented algorithm

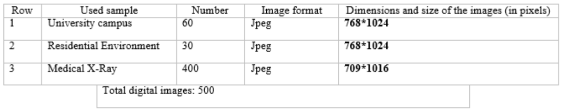
Test dataset which has been used in the proposed algorithm to detect counterfeiting includes:

1. Medical X-ray images of human organs consist of: knee, brain, skull, tooth, kidney, lung, vertebrae of the lower back, etc. with the JPEG file format in size of 709 * 1016 pixels.

2. The images of the landscape that most of them have been taken from the environment of Islamic Azad University of Karaj and some from other parts of the residential environment and nature with high resolution and brightness, JPEG file format and size of 768 x 1024 pixels by 13-megapixel camera of Samsung E7cell-phone.Forging operation of various types have been applied on each of them.

Among the 4000 medical images and 90 photos of nature, which were specified in a classified form, 500 photos were selected. The selected cases were real photos in which no changes or manipulation has happened. 157 counterfeit and manipulated photos were created using the powerful graphic software of Photoshop CS5, in a way that the human eye cannot identify counterfeit areas in the photo. Implemented samples in the proposed algorithm is fully described in Table 1:

Table 1. Specifications of samples used in the test database



Row	Used sample	Number	Image format	Dimensions and size of the images (in pixels)
1	University campus	60	Jpeg	**768*1024**
2	Residential Environment	30	Jpeg	**768*1024**
3	Medical X-Ray	400	Jpeg	**709*1016**
	Total digital images: 500			

Given that some of the available methods and algorithms are not able to identify high-resolution digital images and they are encountered with error, pictures with dimensions of 709 * 768 and 1016 * 1024 pixels were used in the proposed algorithm to increase the precision of the algorithm so that large areas of counterfeit copies can be identified.

4. TEST RESULTS

The most important aspect of a method for practical applications is to distinguish real pictures from the forged ones. Primarily, the ability to position duplicated or forged part in an image is very important; it would be an appropriate evidence to prove forgery in digital images. Thus, the performance of the algorithm can be assessed at two levels: In the picture level which must rely on the fact that whether the image is forged or not and at the pixel level namely way of forgery in different areas of photo with high precision should be determined.
Some important criteria which have been recorded in a level photo are as follows:

The number of forged images which have been recognized correctly (T_p), the number of images that their forgery has not been properly identified (F_p) and the number of forged photos which could not be mistakenly identified (F_N). Thus, the level of precision p and recovery R can be obtained on the basis of equations 10 and 11: (christlein et al., 2012)

$$\text{Recall} = \frac{T_p}{T_p+F_N} \quad (10)$$

$$\text{Precision} = \frac{T_p}{T_p+F_p} \quad (11)$$

The precision is the probability of which, all existing forgeries in an image is completely and correctly identified, while recovery is how much a forged picture can be investigated and points of forgery can be obtained. To determine the precision of the proposed algorithm, Ψ_S was considered as the copied area while $\widetilde{\Psi}_S$ as identified copies, Ψ_T as the changed area and $\widetilde{\Psi}_T$ as the changed and identified area were named. DAR indicates the precision rate of the detection process and FPR represents the false-positive rate. The DAR and FPR are computed as follows: (Cao et al., 2012)

$$DAR = \frac{|\psi_S \cap \widetilde{\psi}_S| + |\psi_T \cap \widetilde{\psi}_T|}{|\psi_S| + |\psi_T|} \quad (12)$$

$$FPR = \frac{|\widetilde{\psi}_S - \psi_S| + |\widetilde{\psi}_T - \psi_T|}{|\widetilde{\psi}_S| + |\widetilde{\psi}_T|} \quad (13)$$

Here, | | Indicates the mentioned area, ∩ represents the intersection of two areas and – Displays the difference between the two areas. Thus, DAR shows that the performance of algorithm has determined the positions of existing pixels of the Copy – Transfer area correctly in counterfeit image. FPR is indicator of percentage of pixels that are not placed in duplicated region but, they have been implemented in proliferation methods. Thus, these two parameters show how the precision of the algorithm can indicate manipulated areas.

In the following sections, the proposed algorithm in section 5-1 is assessed at first. Then, proposed copy-transfer forgery scheme is compared with other present approaches such as methods based on DCT, SVD, BRAVO, FMT and SIFT in section 5.2.

4.1. Testing the precision of the irregular and non-overlapping adaptive block-based proposed algorithm:

In the following test, some color as well as black and white images in size 709 * 1016 and 1024 * 768 pixels were selected of first and second databases to examine the effectiveness of the proposed algorithm. The images are divided into two categories. For the former, random Selection from three types of blocks were done in different sizes including 32 x 32, 128 x 128 and 160 x 160 pixels (i.e. 0.14%, 2.27% and 3.55% of the total area of the image area respectively).The test results in Figures 7,8 can be observed based on the size of the blocks and the proposed algorithm. Fake pictures in row A and results in row B are visible.

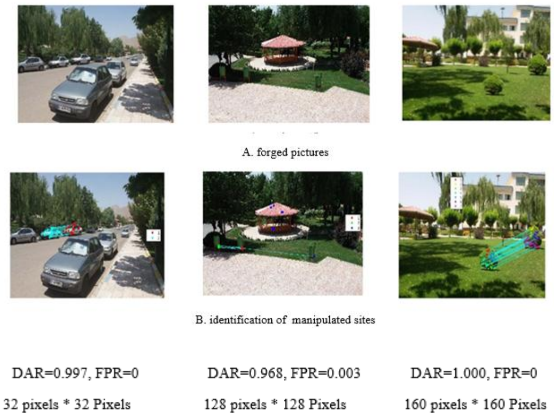


Fig 7. The results of testing the effectiveness and the precision of the implemented algorithm

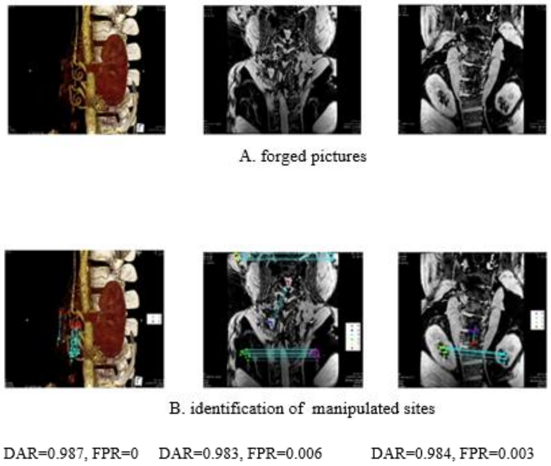


Fig 8. test of the effectiveness and the precision of the implemented algorithm

4.2 evaluation and comparison of the proposed algorithm with other algorithms:

In the last experiment, the proposed method was compared with other existing methods such approaches based on SURF (Bo et al., 2010), SVD (Kang & Wei, 2008), BRAVO (Bravo-

Solorio & Nandi, 2009), FMT (Bayram et al., 2009) and SIFT (Amerini etal., 2011). Before comparison, 500 manipulated images were created. In each of them, an area of 64 x 64 pixels was selected randomly and it was attached to another non-overlapping area. Then, several image processing operations including rotating, blurring, scaling, etc., were applied on the copied images. But here only three cases are mentioned: blurring, rotating and jpeg compressing. Tables 2 and 3 show the detection results for 1000 pictures in the image and pixel levels. According to Tables 2 and 3, it can be easily observed that the scheme can reach the precision of higher than 97% as well as recall rate of almost 100 percent.

Table 2. Results of detection under the copy-transfer in an image level

method	Precision **(%)**	**Recall (%)**	**DAR**	**FPR**
[3] SURF	**58.89**	**49.91**	**89.09**	0.1
[45] SVD	**87.27**	**90.87**	**89.45**	0.11
[2] SIFT	**17.79**	**37.88**	**90.53**	0.12
] BRAVO [46	**100**	**27.87**	**96.00**	0.08
[47] FMT	**84.36**	**69.25**	**74.38**	0.2
proposed	**96**	**100**	**97.96**	0.05

Table 3. Results of detection under the copy-transfer in a pixel level

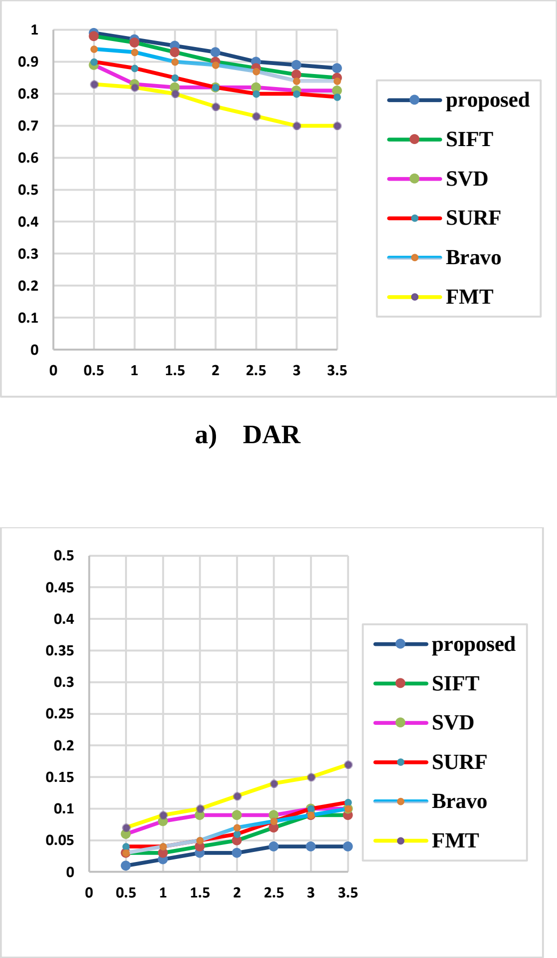
method	Precision **(%)**	**Recall (%)**	**DAR**	**FPR**
SURF]3[	**43.76**	**13.68**	**34.85**	17.0
SVD]45[	**27.89**	**25.80**	**42.70**	25.0
SIFT]2[	**48.71**	**80.60**	**54.69**	27.0
BRAVO]46[	**98.82**	**81.98**	**92.90**	09.0
FMT]47[	**72.61**	**42.70**	**10.65**	3.0
proposed	**22.97**	**79.89**	**95.93**	06.0

In practice, the overall average performance, in 500 manipulated images were compared and results are visible in figure 9.Blur method was used to manipulate images (Figure 9 (a) - (b)). As can be observed in Figure 9, if the blur method is used, DAR curve shows that the proposed method can be better than other algorithms which means DAR ≥92% even when the radius of the blur increases. FPR curve also indicates that the results of the proposed method are very desirable i.e. its FPR is lower than other methods, even when the radius of the Blur is more (σ =3). But methods based on key points and block cannot identify such forged cases properly.in rotation test, copied areas with the rotation angle of 2 ° to 10 ° And step of 2 ° with rotation angles of 20, 60 and 180 degrees are turned. In this case, 8 x 500 = 4000 images should be tested. The output of the algorithm as shown in Figure 10 (c) - (d), has better performance compared to other mentioned methods. The jpeg compression test counterfeit images with quality factor of 70, 75.80, 85, 90, 95 and 100 were compressed as JPEG. Proposed method based on output of the algorithm, as shown in Figure 11 (e) - (f), works better when compression rate is slight in images.

Detection results at the pixel level and under various attacks are shown in Figures 9, 10 and 11: a and b) blur, c and d) rotation, e and f) jpeg Compression; Here, the results which are marked blue and are specified by the word "proposed" , show the results of the proposed scheme with adaptive block. Results which are shown in in green and red with signs of «SIFT» and «SURF», represent the outcome forgery detection methods based on key points according to SIFT and SURF while the results that are presented in blue, yellow and pink and they are specified as «Bravo», «FMT» and «SVD» indicate block-based methods of counterfeiting.

X-axis in (a and b) of Figures 9,10 and 11 shows the radius of the blur, in (c and d) indicates the angle of rotation and in (e and f) represents quality factor .Figures 9, 10 and 11, show detailed results of the proposed model compared with existing methods.

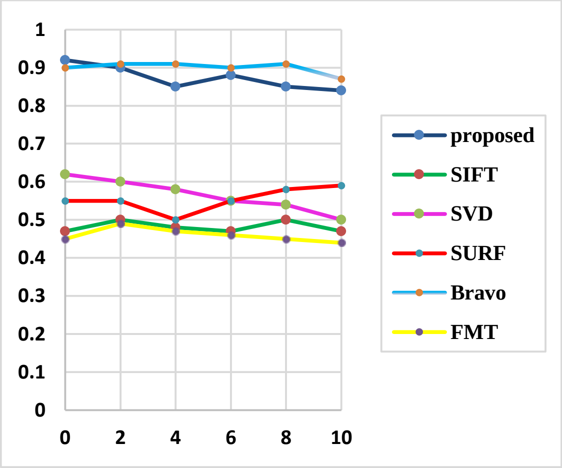
It can be easily observed that the precision of the proposal is more than existing methods which are on the basis of the key point (of The SIFT and SURF) moreover, it is as well as block-based methods which have been proposed in BRAVO, SVD and FMT including under attack from various common image processing. According accurate results implemented plan also outperforms fixed-size blocking by combining the block-based methods and key points.



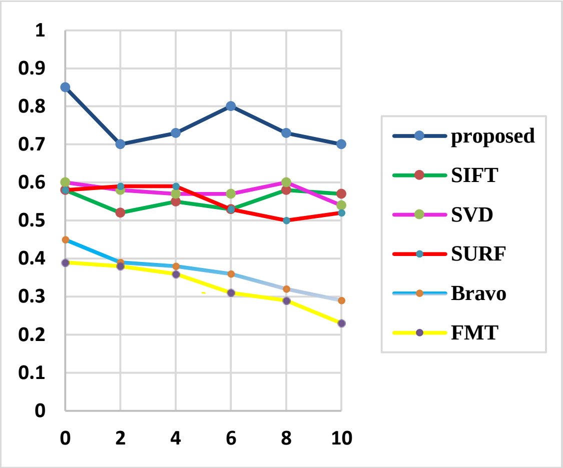
a) DAR

b) FPR

Fig 9. The results of comparing DAR and FPR in the implemented algorithm With other algorithms in the blurring method.

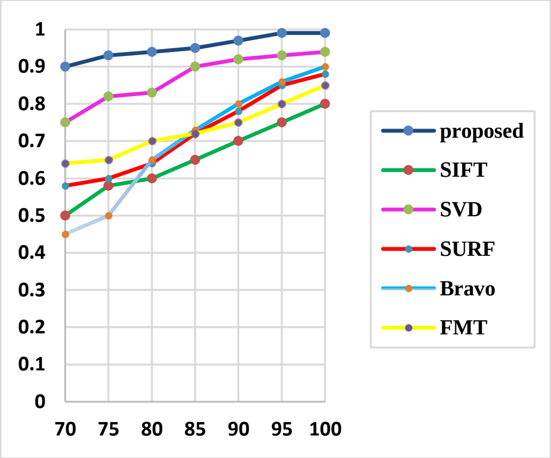


c) precision

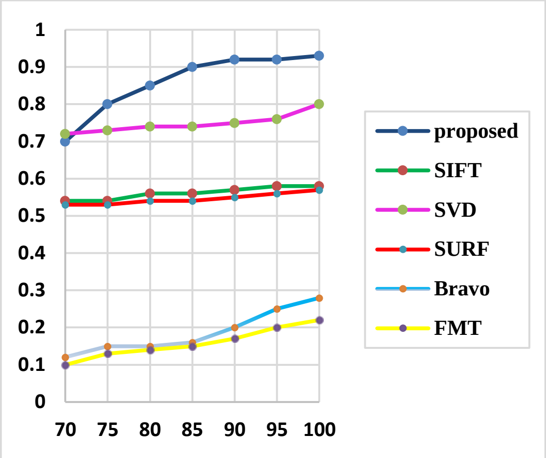


d) recall

Figure 10. The results of comparing the precision and recall of implemented plan with other algorithms in rotation method



e) precision



f) recall

Fig 11. comparing the results of the precision and recall of implemented plan With other algorithms in the compression method

5. CONCLUSION AND RECOMMENDATION

In the proposed algorithm, which is based on combined method of key points and block, the new plan for the detection of counterfeiting especially copy - transfer counterfeit was provided to identify areas suspected of counterfeiting and forged locations .This algorithm is almost the same as combined and clustering algorithms but in the blocking algorithm due to time and cost reduction, input image was divided into irregular and non-overlapping blocks in which good and acceptable results in terms of precision and recall were achieved as the output of the algorithm.

Other researchers implemented their own algorithms using algorithms based on key points SURF and SIFT, in which the output was poor in terms of speed of the recall and identification of the forged points. Some other researchers also attempted to implement their algorithm using block-based algorithms such as SVD, DCT, DWT and etc., in which the output was weak in terms of speed of recalling and sorting blocks. The algorithms based on blocking, which divide the input image to the same regions of rectangular, square or polygonal shapes and compare formed areas with the adjacent blocks to identify counterfeit areas , were not successful in terms of time complexity and geometric changes in the manipulated areas and they sometimes had large rate of errors as well as lack of proper detection of forgery. Therefore, this hybrid implemented approach is able to achieve better results for the forged copy - transfer images under different challenging conditions compared with other available leading plans of forgery.

The mentioned conditions include blurring, jpeg compression, rotating, scaling and resizing. This method is used in multiple copied areas and quality of images does not have a major impact in the way of finding forgery.

Therefore, it is suggested that a framework in the form of open-source programming language is designed and implemented to cover all methods of detecting image forgery including block-based and key points which can identify the location and any types of forgery especially the combined forgeries depending on the input image of any format and any size.

REFERENCES

A.E. Dirik, S. Bayram, H.T. Sencar and N. Memon, 2007, "New features to identify computer generated images", IEEE International Conference on Image Processing, pp. 433–436.

A. Leykin, F. Cutzu, 2003, "Differences of edge properties in photographs and paintings", ICIP, pp. 541–544.

Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, G. Serra, (2011), "A SIFT-based forensic method for copy-move attack detection and transformation recovery", IEEE, pp. 1099–1110.

B. Dybala, B. Jennings, D. Letscher, 2007, "Detecting filtered cloning in digital images", Proceedings of the 9th Workshop on Multimedia & Security, ACM, New York, NY, USA, pp. 43–50.

Chi-Man Pun, Xiao-Chen Yuan, Xiu-Li Bi, 2011,"Image Forgery Detection Using Adaptive Over-Segmentation and Feature Point Matching", IEEE, pp. 1-12.

Cao YJ, Gao TG, Fan L, Yang QT, 2012, "A robust detection algorithm for copy-move forgery in digital images", Forensic Sci, pp. 33–43.

D.-Y. Hsiao, S.-C. Pei, 2005, "Detecting digital tampering by blur estimation", IEEE Computer

Society, p. 264.

G. Muhammad et al, 2012, "Passive copy move image forgery detection using undecimated dyadic wavelet transform", Digital Investigation 9, pp. 49–57.

G. Cao, Y. Zhao, R. Ni, 2010, "Edge-based blur metric for tamper detection", Journal of Information Hiding and Multimedia Signal Processing, pp. 20–27.

G. Cao, Y. Zhao, R. Ni, 2009, "Detection of image sharpening based on histogram aberration and ringing artifacts", IEEE International Conference on Multimedia and Expo, pp. 1026–1029.

G. Sankar, V. Zhao, Y.-H. Yang, 2009, "Feature based classification of computer graphics and real images", IEEE Computer Society, pp. 1513–1516.

H. Cao, A.C. Kot, 2008, "A generalized model for detection of demosaicing characteristics", ICME, pp. 1513–1516.

H. Cao, A.C. Kot, 2009, "Accurate detection of demosaicing regularity for digital image forensics", IEEE Transactions on Information Forensics and Security, pp. 899–910.

H. Farid, M. Bravo, 2010, "Image forensic analyses that elude the human visual system", SPIE Symposium on Electronic Imaging, pp. 1-7.

H. Gou, A. Swaminathan, M. Wu, 2007, "Noise features for image tampering detection and steg analysis", ICIP (6) and IEEE, pp. 97–100.

H. Farid, 2006, "Exposing digital forgeries in scientific images", ACM Multimedia and Security Workshop, pp. 1-6.

H. Farid, 2009, "Exposing digital forgeries from jpeg ghosts", IEEE Transactions on Information Forensics and Security, pp. 154–160.

I. Avcibas, S. Bayram, N.D. Memon, M. Ramkumar and B. Sankur, 2004, "A classifier design for detecting image manipulations", ICIP, pp. 2645–2648.

J. Zheng, M. Liu, 2008, "A digital forgery image detection algorithm based on wavelet homomorphic filtering", IWDW, pp. 152–160.

J. Fridrich, "Digital image forensics", 2009, IEEE Signal Processing Magazine, pp. 26–37.

J. Fridrich, D. Soukal, J. Lukas, 2003, "Detection of copy–move forgery in digital images", IEEE Computer Society, pp. 55–61.

J. Dong, W. Wang, T. Tan, Y. Shi, 2008, "Run-length and edge statistics based approach for image splicing detection", Digital Water marking, pp. 76–87.

Liu G, Junwen W, Shiguo L, Zhiquan W, 2011, "A passive image authentication scheme for detecting regionduplication forgery with rotation", J Netw Comput Appl, pp. 1557–1565.

M.A. Fischler, R.C. Bolles, 1981, "Random Sample cousensus: A paradigm for model fitting with applications to image analysis and automated cartography", ACM, pp.381-394

R. Davarzani et al, 2013, "Copy-move forgery detection using multi resolution local binary patterns", Forensic Science International 231, pp. 61–72.

R. Achanta, A. Shaji, K. Smith, A. Lucchi, P. Fua, and S. Susstrunk, 2012, "SLIC super pixels compared to state-of-the-art super pixel methods", IEEE, pp. 2274-2282.

S. Bravo-Solorio, A.K. Nandi, 2009, "Passive forensic method for detecting duplicated regions affected by reflection, rotation and scaling", European Signal Processing Conference, pp. 824–828.

Solario SB, Nandi AK, 2009, "Passive forensic method for detecting duplicated regions affected by reflection, rotation, and scaling", Proc. EUSIPCO09, p. 824–8.

S. Bayram, I. Avcibas, B. Sankur, N. Memon, 2005, "Image manipulation detection with binary similarity measures", Proceedings of 13th European Signal Processing Conference,pp. 752–755.

S. Bayram, H.T. Sencar, N. Memon, 2009, "An efficient and robust method for detecting copy-move forgery", IEEE International Conference on Acoustics, pp. 1-12.

T.-T. Ng, S.-F. Chang, J. Hsu, L. Xie, M.-P. Tsui, 2005, "Physics-motivated features for distinguishing photographic images and computer graphics", ACM International Conference on Multimedia, ACM, pp. 239–248.

T.-T. Ng, S.-F. Chang, C.-Y. Lin, Q. Sun, 2006, "Passive-blind image forensics", Eds, pp. 1-7.

T.-T. Ng, S.-F. Chang, 2006, "An online system for classifying computer graphics images from natural photographs", SPIE Electronic Imaging, pp. 1-4.

T.-T. Ng, S.-F. Chang, M.-P. Tsui, 2007, "Lessons learned from online classification of photo-realistic computer graphics and photo- graphs", IEEE Workshop on Signal Processing Applications for Public Security and Forensics (SAFE), pp. 1-6.

T.ojala, M.pietikinen, D.harwood, 1996, "A Comparative study of texture measures with classification based on featured distribution", pattern recog.29, pp. 51–59.

V.christlein, C.Riess and J.Jorden, 2012, “An evaluation of popular copy-move forgery detection approaches”, IEEE Trans. Inf. Forensics Secur. 7(6), pp. 1841-1854

W. Luo, Z. Qu, J. Huang, G. Qiu, 2007, "A novel method for detecting cropped and recompressed image block", IEEE International Conference on Acoustics, pp. 217–220.

W. Luo, Z. Qu, F. Pan, J. Huang, 2007, "A survey of passive technology for digital image forensics", Frontiers of Computer Science in China, pp. 166–179.

Wei W, Wang S, Tang Z, 2010, "Estimation of image rotation angle using interpolation-related spectral signatures with application to blind detection of image forgery", IEEE, pp. 507–517.

X. Bo, W. Junwen, L. Guangjie, and D. Yuewei, 2010, "Image copy-move forgery detection based on SURF", Multimedia Information Networking and Security (MINES),pp. 889-892.

X. Kang, S. Wei, 2008, "Identifying tampered regions using singular value decomposition in digital image forensics", Proceedings of International Conference on Computer Science and Software Engineering, pp. 926–930.

Y. Sutcu, B. Coskun, H.T. Sencar, N. Memon, 2007, "Tamper detection based on regularity of wavelet transform coefficients", IEEE, pp. 397–400.

Zhang Z, Yuan R, Jian P, Zhang H, Shan-Zhong. 2008, "A survey on passive-blind image forgery by doctor method detection", In: Proc. of the seventh International conference on machine learning and cybernetics, p. 3463–3467.

Z. Qu, W. Luo and J. Huang, 2008, “A convolutive mixing model for shifted double jpeg compression with application to passive image authentication”, in: IEEE International Conference on Acoustics, Speech and Signal Processing, Las Vegas, USA, pp. 1483–4244.

Z. Fan, R.L. de Queiroz, 2003, "Identification of bitmap compression history: jpeg detection and quantizer estimation", IEEE Transactions on Image Processing, pp. 230–235.

Z. Li, J. Bin Zheng, 2008, "Blind detection of digital forgery image based on the local entropy of the gradient", IWDW, pp. 161–169.

Z. Qu, G. Qiu, J. Huang, 2009, "Detect digital image splicing with visual cues", Information Hiding, 11th International Workshop, pp. 247–261.