2nd IEEE International Conference on Engineering and Technology (ICETECH), 17th& 18thMarch 2016, Coimbatore, TN, India.

# Detection of copy-move forgery based on Gabor filter

Raichel Philip Yohannan
Electronics and Communication
Rajiv Gandhi Institute of Technology
Kottayam, India
raichelphilip@yahoo.com

Manju Manuel
Electronics and Communication
Rajiv Gandhi Institute of Technology
Kottayam, India
manju.manuel@gmail.com

***Abstract*—In recent years, digital images are widely used in many applications and for multiple purposes. The number of tools and software of digital image editing is also increasing day-by-day which makes it easy to manipulate the actual information of an image. Therefore it is important to ascertain the authenticity of the image under use. There are many ways in which a forger can tamper an image, out of which the most popular way is copy-move forgery. This type of forgery is used to either hide an object or replicate it by copying and pasting it on another area of the same image. This paper proposes a method for detecting such type of forgery. The algorithm uses feature vectors extracted from the Gabor response of each overlapping block of the image. Experimental results show the ability of the method to precisely locate the duplicated regions.**

***Keywords—copy-move forgery; gabor; image forensics***

## I. INTRODUCTION

"A picture is worth a thousand words" is an old adage. But today, a picture may also have scores of interpretations. Digital images are increasingly becoming important in many fields and applications in the areas of military, media, medical diagnosis, the internet websites, on the covers of magazines and newspapers, etc. Even though digital images can be considered a major source of information in today's digital world, the relevance of the proverbs like "seeing is believing" is doubtful.

The advancement of technology and availability of low-cost hardware and software editing tools has made it easy to forge a digital image without leaving any visible clues and hence it is difficult to trace these modifications with naked eyes. The establishment of authenticity of an image has become even more challenging, thanks to the powerful, affordable and extremely easy-to-use digital image processing and editing tools at the disposal of end users. When it comes to sensitive data such as medical records, news items, evidence in court of law, the integrity of the image cannot be taken for granted. Different forensics-related questions arise such as, how an image was acquired? Is it authentic or it has undergone any kind of manipulation after capturing?

Over the past few years, the field of Digital Image Forensics (DIF) has emerged as solution to these growing challenges. DIF is a field that uses variety of methods to analyze images of a particular scenario to establish their authenticity. DIF primarily aims at developing efficient and reliable image forgery detection methods. Several techniques have been proposed for exposing image forgeries, especially copy-move forgery. Copy-move forgery is the most common type of image tampering, wherein part(s) of the original image is(are) copied and moved to another location of the same image. This is usually done in order to hide or replicate certain details of an image. An example of this type of forgery is shown in Fig.1.

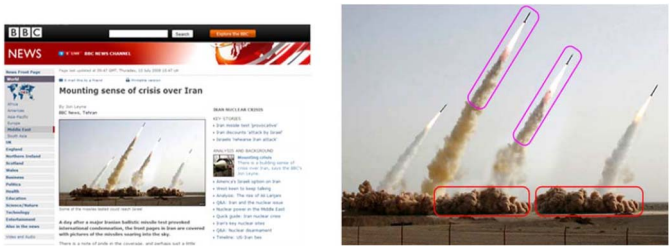



Fig. 1. Example of image tampering that appeared in press in July,2008. The image on the right is a forged one, -- it shows four Iranian missiles, but only three of them are real; Two different sections (encircled in red and purple, respectively) have been replicated by applying a copy-move attack.

Various forensic methods have been developed to counter copy-move tampering. Most of the existing methods aimed at detecting duplicated regions in images are sensitive to geometrical changes in the duplicated areas. Consequently, a simple rotation of the copied region could be used to not only suit the scene of the image, but also hinder its proper detection. This paper presents an image forgery detection method based on Gabor features.

The rest of the paper is structured as follows: In section II, an overview of the area of Copy-Move Forgery Detection is presented. Gabor filters are defined and mathematical theory behind them is explained in Section III. The proposed forgery detection method is presented in Section IV. Section V describes about a Graphical User Interface developed to enable a user to perform interactive tasks. In section VI, the experimental results are presented.

## II. RELATED WORKS

In general, there are two types of techniques that can be used for image tampering detection --- active methods/authentication and passive methods/authentication.

978-1-4673-9916-6/16/$31.00 ©2016 IEEE

### A. Active Methods

The Active approaches are those wherein prior information regarding the image is necessary to the process and these are mostly concerned with the data hiding techniques. The Active methods can be classified into two categories. The first category is based on digital watermarking --- concealing a watermark into the image at the capturing end and extracting it at the authentication end. The main drawback is the requirement of a specially equipped camera and an authorized person for the insertion and extraction of watermark, respectively. The second category is based on digital signatures --- extracting unique features from the image as a signature at the receiving end, regenerating the signature using the same method at the authentication end and identifying the authenticity of the image through comparison. Digital signatures have similar drawbacks as digital watermarking.

### B. Passive Methods

Passive or Blind image authentication, which is also called Digital Image Forensics, is the process of authenticating digital images without using any additional information aside from the picture itself. Its goal is to determine the authenticity and the origin of digital images without the support of an embedded security scheme. Within this field, copy-move forgery detection (CMFD) is the most researched topic. The main difference between the existing methods used for CMFD lies in the type and size of the features that are used for matching the image blocks or keypoints. In [2], Al-Qershi classified the existing methods according to the extracted features as follows:

- DCT-based algorithms.
- Log-polar transform-based algorithms.
- Texture and intensity-based algorithms.
- Algorithms based on invariant key-points.
- Algorithms based on invariant image moments.
- PCA-based algorithms.
- SVD-based algorithms

In addition to the algorithms mentioned above, there are more algorithms that can be found in the literature.

## III. Gabor Filters For Robust Features

### A. Motivation

The use of features based on Gabor filters has been promoted in image processing and computer vision applications for almost three decades, because of their useful properties. Features constructed from responses of Gabor filters --- Gabor features, are among the top performers in face recognition and fingerprint matching. The most important properties are related to invariance to illumination, rotation, scale and translation. These properties are based on the fact that they are all parameters of Gabor filters themselves. This prompted us to use Gabor features in our algorithm.

### B. Review of Gabor Filters

A Gabor filter is obtained by modulating a sinusoid with a Gaussian. For the case of one dimensional (1D) signals, a 1D sinusoid is modulated with a Gaussian. For two dimensional signals such as images, consider the sinusoid shown in Fig. 2(a). By combining this with a Gaussian (Fig. 2(b)), we obtain a Gabor filer (Fig.2(c)).

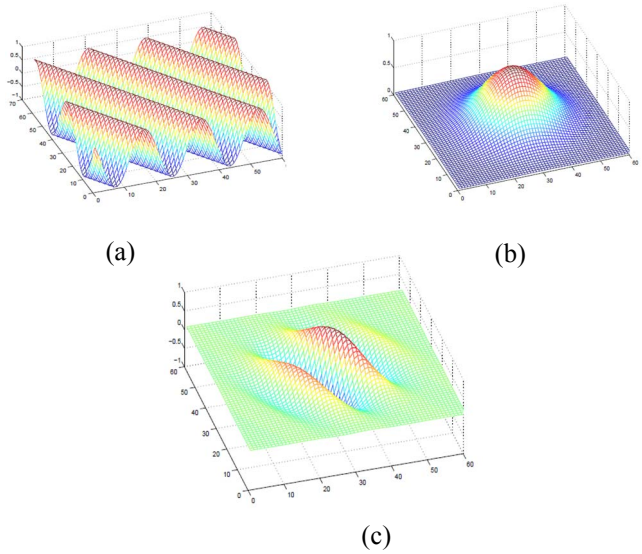



Fig. 2. Gabor filter composition: (a) 2D sinusoid oriented at 30° with the x-axis, (b) a Gaussian kernel, (c) the corresponding Gabor filter.

Let $g(x, y, f, \theta)$ be the function defining a Gabor filter centered at the origin with $f$ as the spatial frequency and $\theta$ as the orientation. We can view Gabor filters as

$$g(x, y, f, \theta) = exp\left(-\frac{x^2+y^2}{\sigma^2}\right) \exp(2\pi fi(xcos\theta + ycos\theta)) \quad (1)$$

Here $\sigma$is the standard deviation of the Gaussian kernel. The response of a Gabor filter to an image is obtained by a 2D convolution operation. Let $I(x, y)$denote the image and $G(x, y, f, \theta)$ denote the response of a Gabor filter with frequency $f$ and orientation $\theta$, to an image at point $(x, y)$on the image plane. $G(\cdot)$is obtained as:

$$G(x, y, f, \theta) = \iint I(p, q)g(x - p, y - q, f, \theta)dp\, dq \quad (2)$$

### C. Extraction of Gabor-based invariant features

This work draws its idea from the field of image retrieval. The Gabor filter has been widely used as an efficient method of extracting texture features for image retrieval. This paper uses the rotation-invariant Gabor representation proposed in [3] which requires a few summations on the conventional Gabor filter impulse response; and proposes a block-based framework that extracts features based on Gabor response which can be used as evidence to detect copy-move manipulation in a digital image. Throughout the description given below,$I(x, y)$will refer to a single sub-block of the given image.

For each image sub-block, we form feature vectors using rotation invariant representations of [3]. A 2-D Gabor function can be expressed as:

$$g(x,y) = \frac{1}{2\pi\sigma_x\sigma_y} exp\left[-\frac{1}{2}\left(\frac{x^2}{\sigma_x^2}+\frac{y^2}{\sigma_y^2}\right)+2\pi iWx\right] (3)$$

Here $\sigma_x$ and $\sigma_y$ characterize the spatial extent and frequency bandwidth of the Gabor filter, and *(W,0)* represents the center frequency of the filter in the frequency domain rectilinear coordinates $(u,v)$. Let $g(x,y)$be the mother generating function for the Gabor filter family. A set of Gabor functions $g_{m,n}(x,y)$ can be generated by rotating and scaling $g(x,y)$, that is,

$$g_{m,n}(x,y) = a^{-2m} g(x',y') (4)$$

Where$x' = a^{-m}(xcos\,\theta_n + ysin\theta_n)$,

$$y' = a^{-m}(-xsin\theta_n + ycos\theta_n),$$

$a > 1$, $\theta_n = \frac{n\pi}{K}$, $m = 0,1,\dots,S-1$,

and $n = 0,1,\dots,K-1$.

Parameter S is the total number of scales, and parameter K is the total number of orientations. Given an image $I(x,y)$, its Gabor filtered images are:

$$J_{m,n}(x,y) = \sum_{x_1}\sum_{y_1} I(x_1,y_1) g_{m,n}(x-x_1, y-y_1) \quad (4)$$

By summing all the K filters in (4) with different orientations at each scale, the rotation invariant Gabor filter family is obtained. That is,

$$g_m(x,y) = \sum_{n=0}^{K-1} g_{m,n}(x,y), \quad m = 0,1,\dots,S-1 \quad (5)$$

Hence the transformation of the image$I(x,y)$ is

$$J_m(x,y) = \sum_{x_1}\sum_{y_1} I(x_1,y_1)\, g_m(x-x_1, y-y_1), \quad (6)$$

$$m = 0,1,\dots,S-1.$$

The mean $\mu_m$of the transform coefficients $J_m(x,y)$ is used to construct the feature vector which is computed as follows:

$$\mu_m = \frac{1}{N}\sum_x\sum_y |J_m(x,y)| \quad (7)$$

The feature vector is then constructed as follows:

$$f = [\mu_0, \mu_1, \dots, \mu_{S-1}] \quad (8)$$

## IV. Copy-move Forgery Detection System

As said earlier, since copy-move forgery is created by copying and then duplicating the required area, there must be at least two similar regions in the tampered image. A natural image, on the contrary, is very unlikely to have two large similar regions (except for the images that have two large smooth regions). Thus an image can be suspected as copy-move forged if two similar regions are detected. Since the location, shape and other features of the regions are not known, it is computationally impossible to try to examine every possible pair of region. Hence, it is more desirable to divide an image into fixed-size overlapping blocks and test whether the pairs of blocks are duplicated. Fig. 3 shows the flow of algorithm.

### A. Dividing input image into sub-blocks

Suppose that the minimal size of the segment that should

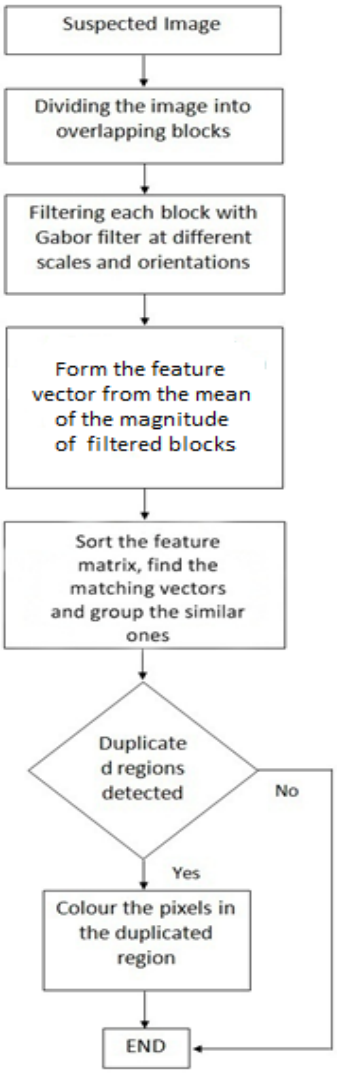



Fig.3. Algorithm workflow.

be considered for match is a square with B*B pixels. Then, a square with B*B pixels slides once along the image, pixel by pixel, starting from the upper left corner right down to the lower right corner. Suppose the image has M*N pixels, then the sliding will generate $N_b = (M-B+1)(N-B+1)$ blocks.

### B. Representing sub-blocks using proper features

As described in the previous section, for every image sub-block, feature vectors are formed using rotation-invariant Gabor representations. These feature vectors are robust representations of the corresponding sub-blocks. Every time a feature vector is computed, it goes into the feature matrix *A*. The feature matrix represents the whole image, and it is used for further processing.

### C. Sorting

Then the vectors are sorted in a lexicographic order. Let the matrix $\hat{A}$denote the matrix of sorted vectors. In the process, the top left corner's coordinate, $(x_i, y_i)$, of each block (i.e. the block position) is recorded.

### D. Matching

Let the $i^{th}$ row of $\hat{A}$ is denoted as $\overrightarrow{a_i}$ . In the matching step, for each row $\overrightarrow{a_i}$ in the matrix $\hat{A}$ , every $\overrightarrow{a_j}$ that satisfies $j - i < N_f$ is tested whether it is similar with $\overrightarrow{a_i}$ based on the Euclidean similarity measure. Here $N_f$ is a parameter that controls the number of neighboring rows that are tested to find the similarity. If $\overrightarrow{a_i} = (v_i^1, v_i^2, v_i^3)$ and $\overrightarrow{a_j} = (v_j^1, v_j^2, v_j^3)$ , then the Euclidean similarity measure between $\overrightarrow{a_i}$ and $\overrightarrow{a_j}$ is defined as

$$\sqrt{\left(v_i^1 - v_j^1\right)^2 + \left(v_i^2 - v_j^2\right)^2 + \left(v_i^3 - v_j^3\right)^2 + \ \ldots}$$

For two row vectors to be similar, this distance between them must be less than a threshold$D_{similar}$ . If $\overrightarrow{a_i}$ and $\overrightarrow{a_j}$turn out to be similar, the Euclidean distance(spatial distance) between their corresponding blocks, $d = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2}$, where $(x_i, y_i)$ and $(x_j, y_j)$ are the corresponding block positions, is calculated. Since two neighboring blocks may have similar feature vectors, the distance $d$ should be more than a threshold $N_d$.

The matching blocks are then colored with the same color in a map image and thus identified as segments that might have been copied and moved. The algorithm outputs this map image, in which, the regions which are considered to be duplicated are marked with a special color and the remaining area is white or black. With the map image and visual judgment, it can be quickly determined whether the input image is original or tampered. The block size B controls the minimal size of copy-move segment that can be detected. There may be some false matches. So, a morphological opening operation is performed to remove the isolated blocks.

## V. Graphical User Interface

A graphical user interface (GUI) was developed in Matlab R2011b to allow a user to perform copy-move forgery detection interactively. Fig. 4 Shows the GUI.

## VI. Experimental Results And Discussion

This section evaluates the performance of the presented method on a set of forged images. The forgery detection performance of the described algorithm was tested on several images taken from a publicly available database designed for image forgery detection [4].

The experiments were carried out on MatlabR2011b (7.13.0.564). All images used in the experiment were taken from the data set [4].The format of all the images used for testing is .png. Different size images were employed for testing. The parameters used in the experiment were set as follows: B (block size) = 8, $D_{similar}$ (Euclidean similarity threshold) = 3, $N_f$ (neighbourhood threshold) = 3, $N_d$(Euclidean distance threshold) = 16. A 10×10 square was used in the morphological opening operation.

### A. Performance

We can quantify the performance of the algorithm in detecting copy-move forgery, using the following definitions:

1) True positive (TP): forged images detected as forged
2) False negative (FN): forged images detected as genuine.
3) False positive (FP): genuine images detected as forged
4) True Negative(TN): genuine images detected as genuine

The above numbers can be put into a table as shown below in Table I, which helps to understand the performance better.As shown in Table I, total 30 images were tested, out of which 22 were forged images (true matches) and 8 were genuine images (true non-matches). Out of the 22 forged images, the algorithm detected 20 images correctly as forged. Out of the 8 genuine images, the algorithm falsely detected 4 images as forged.

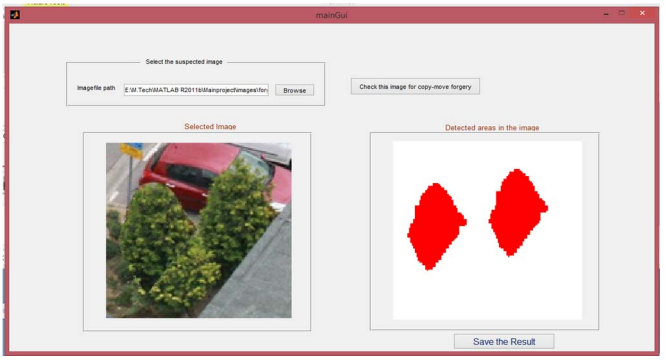



Fig.4. GUI.

TABLE I.Contigency Table

| | True matches | True non-matches | |
|---|---|---|---|
| **Detected matches** | TP=20 | FP=4 | P'=24 |
| **Detected matches** | FN=2 | TN=4 | N'=6 |
| | P=22 | N=8 | Total=30 |

Thus, the total number of detected matches (P') is 24(20+4) and detected non-matches (N') is 6(2+4). The above numbers can be converted into unit rates by defining the following quantities:

1) True positive rate (TPR) or Recall

$$\text{TPR} = \frac{\text{TP}}{\text{TP+FN}} = \frac{\text{TP}}{\text{P}} = 0.909 \quad \text{i.e.}$$

$$\frac{\text{no. of images detected as forged being forged}}{no.of\ forged\ images}$$

2) False Positive Rate (FPR)

$$FPR = \frac{FP}{FP+TN} = \frac{FP}{N} = 0.5 \quad \text{i.e.}$$

$$\frac{\text{no. of images detected as forged being original}}{no.\,of\ original\ images}$$

3) Positive Predictive Value (PPV) or Precision

$$PPV = \frac{TP}{TP+FP} = \frac{TP}{P'} = 0.833$$

4) Accuracy

$$ACC = \frac{TP+TN}{P+N} = 0.80$$

*B. Robustness against different attacks*

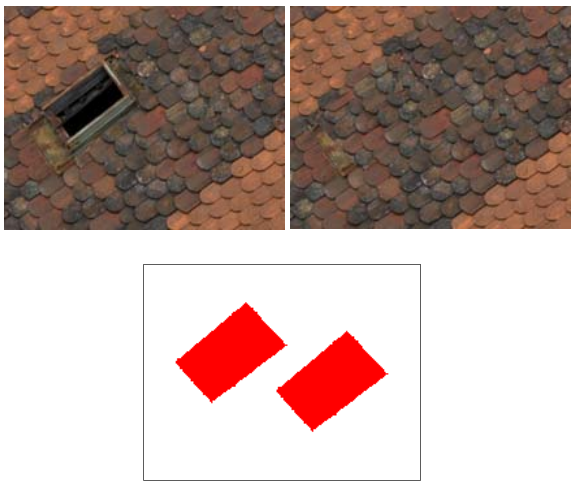
*1) Additive white Gaussian noise:* To test the robustness of the method to Gaussian noise, AWGN of SNR=15db was added to the tampered region.

2) *Multiple copy-move:* We tested this type of scenario by copying an area of the image and pasting it multiple times on different locations of the same image. The algorithm could precisely detect this type of forgery.

*3) Gaussian blurring:* For adding Gaussian blurring to the tampered image, a Gaussian window of size3 × 3and σ = 0.5 was used. The results show that the method is able to detect the tampered regions accurately.

*4) Rotation:* To test the robustness of the algorithm to rotation, we rotated the copied area by arbitrary angles before pasting it elsewhere in the image. The performances resulted by using S = 4, 5, and 6 are very close to each other. Therefore, S = K = 4 is considered as the most suitable parameter value.

Fig. 4 shows the results for each of the above scenario.



(a)

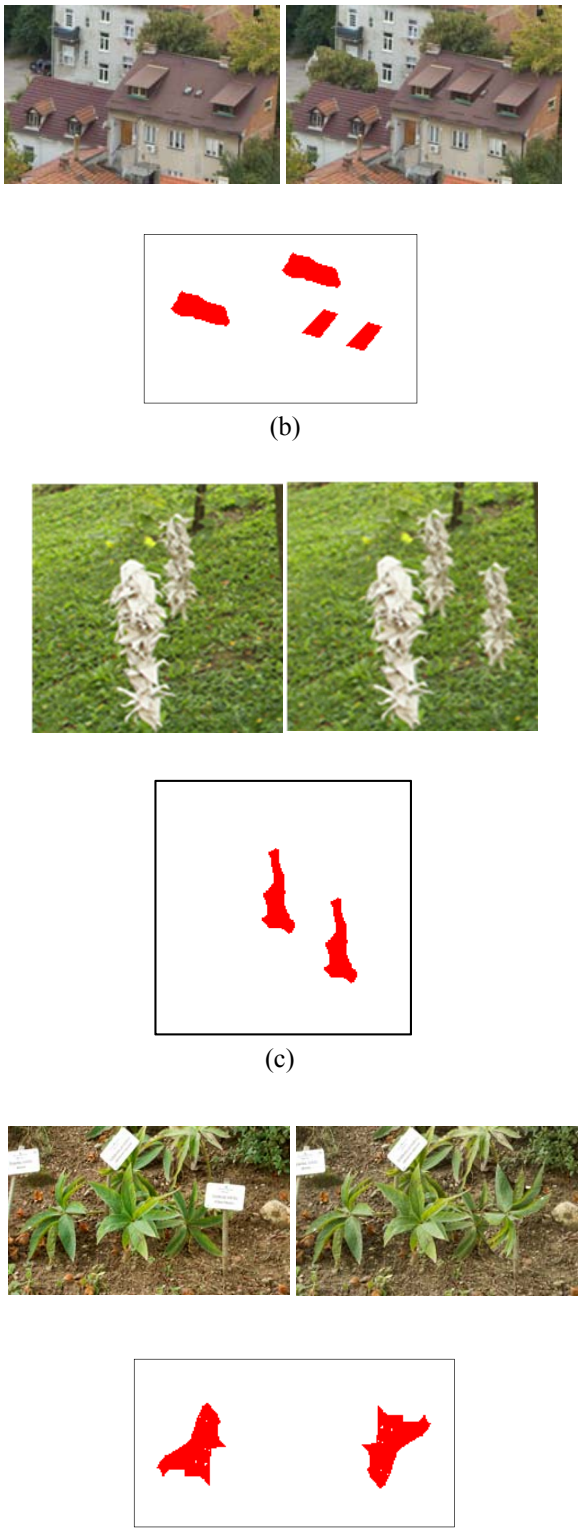


Fig.4. Original image, tampered image and detection results in case of a)AWGN b) Multiple copy-move c)Gaussian blurring d) Rotation

## VII. CONCLUSION

In this study, the problem of copy-move image forgery in digital images is addressed. An efficient method is proposed for copy-move forgery detection. The characteristics of Gabor filters were exploited in order to look for forgery clues. The proposed method is evaluated on a number of original and forged images. Experimental results showed that the method is quite attractive

## *References*


[1] J. Fridrich, D. Soukal and J. Lukas, "Detection of copy-move forgery in digital images," in Proceedings of DFRWS 2003, Cleveland, OH, USA, 2003.

[2] Al-Qershi, Osamah M. and Bee EeKhoo, "Passive detection of copy-move forgery in digital images: State-of-the-art,"Forensic science international 231, pp. 284-295, 2013.

[3] Ju Han and Kai-Kuang Ma, "Rotation-invariant and scale-invariant Gabor features for texture image retrieval," in Elsevier, Image and Vision Computing 25, pp. 1474–1481, 2007.

[4] http://www.vcl.fer.hr/comofod.

[5] Yanping Huang et.al., "Improved DCT-based detection of copy-move forgery in images," in Elsevier, Forensic Science International 206, pp. 178-184, 2011.

[6] A.C. Popescu and H. Farid, "Exposing digital forgeries by detecting duplicated image regions,"Tech. Rep. TR2004-515, Dartmouth College, 2004.

[7] Michael Zimba, Sun Xingming, "DWT-PCA (EVD) based copy-move image forgery detection," in International Journal of Digital Content Technology and its Applications. Volume 5, Number 1, January 2011.

[8] Sunil Kumar, Jagannath Desai and Shaktidev Mukherjee, "A fast DCT based method for copy move forgery detection," in Proceedings of the 2013 IEEE Second International Conference on Image Information Processing (ICIIP-2013).

[9] Irene Amerini, Lamberto Ballan, Roberto Caldelli, Alberto Del Bimboand Giuseppe Serra, "A SIFT-based forensic method for copy–move attack detection and transformation recovery," IEEE transactions on information forensics and security, vol. 6, no. 3, september 2011.

[10] Osamah M. Al-Qershi and Bee Ee Khoo, "Passive detection of copy-move forgery in digital images: State-of-the-art," Forensic Science International 231 (2013) 284–295.

[11] Vincent Christlein, Christian Riess,Johannes Jordan, Corinna Riess, and Elli Angelopoulou,"An Evaluation of popular copy-moveforgery detection approaches,"IEEE transactions on information forensics and security, vol. 7, no. 6, december 2012

[12] Hany Farid, "Image forgery detection, a survey".