Improving the Detection Rate of Forgery JPEG Images based on Combining Histogram Features and Discrete Wavelet Transform (DWT) with the use of Support-Vector Machine

Azam Mohammadi[1], Farhad Navabifar[2*]

1- Department of Computer Engineering, Mobarakeh Branch, Islamic Azad University, Mobarakeh, Iran.
2- Department of Electrical Engineering, Mobarakeh Branch, Islamic Azad University, Mobarakeh, Iran.
Email: farhad.navabifar@mau.ac.ir (Corresponding Author)

Received: April 2019 Revised: July 2019 Accepted: August 2019

ABSTRACT:
Manipulating digital images is not often a difficult task due to the rapid development of software and image manipulation techniques. Hence, there is no need for professional skills or training. When used as an artistic tool, it is completely harmless, but when these images can be presented in judicial system as evidence or for the creation of political associations, as well as, using them in legal documents, electronic money circulation or press; in these cases, the distinction between an original image and a forgery image is very important. In order to solve the problem in this research using a Discrete Wavelet Transform (DWT), which is performed by decomposing a signal into smaller and smaller details, as well as, the use of periodic patterns in the histogram generated by double compression with different coefficients, significant improvements were made in terms of reducing computations and increasing the detection rate of forging areas. Many of the proposed methods for detecting image forgery use a feature extraction model from a valid and manipulated dataset and then classify them using machine learning with the aim of optimizing the accuracy. In this research, following the extraction of features in the proposed method, using the SVM classification identifies image forgery and then identifies the forging area after it detects the falsification or originality of the image. The results of this study indicate 97.98% accuracy in the Columbia database and 98.1% in the IFS-TC database.

KEYWORDS: Image Manipulation, Discrete Wavelet, Histogram, JPEG Image, Support Vector Machine.

1. INTRODUCTION

Nowadays, using image editing and processing software, anyone could add or remove features from digital images without any traces, and forge images. The manipulation of an image can change the content of the image, and this has reduced the confidence in the accuracy of the images, which has been particularly influential in the judiciary, politics, and so on. An image can be used with a number of different methods, but image integration is probably the strongest spy action. Image simulation means getting an area from a source image and moving it to a destination image (Fig. 1). The source and destination image can be the same or different, but regardless of the changes, it can have a significant effect on the message of an image. A number of frameworks for detecting image forgery has been proposed over the years, and a number of them have provided significant solutions.

In general, there are two types of image forgery detection methods: active [1] and passive [2, 3]. In active methods, the digital image requires preprocessing of the image that software or hardware records them, which the recorded data is such as marking or signing on images, so this limits their use in practice. However, active methods for daily practical use are not desirable. Unlike document and signature methods, passive techniques do not require any digital signatures and are considered with each sign. Passive approaches, which collect evidences of manipulation with their images, have a higher potential for practical use and more attention in research.

The passive image forgery detection methods can be roughly divided into five categories:

-Pixel-based techniques: detection of statistical anomalies provided at the pixel level.

- Format-based techniques: use statistical correlations made by a particular compression program.

- Camera-based techniques: using the artworks introduced by the camera lens, detect sensor or post-processing process on the chip.

- Physical environment-based techniques: explicitly identify different models and inconsistencies in the three-dimensional interaction between physical objects, light and camera.

-Geometry-based techniques: detect objects measurement in the world and their position relative to the camera.

In this study, a combination of histogram-based features and discrete wavelet transform (DWT) features are used. In the proposed method, using wavelet transform and generating overlapping blocks, it reduces the complexity of the algorithm and results in a significant improvement in time complexity compared to the related algorithms. DWT is quite suitable for detecting the frequency region of the image signal. In addition, the use of periodic patterns in the histogram, due to double compression with different coefficients, will allow detection of the forging area more quickly.

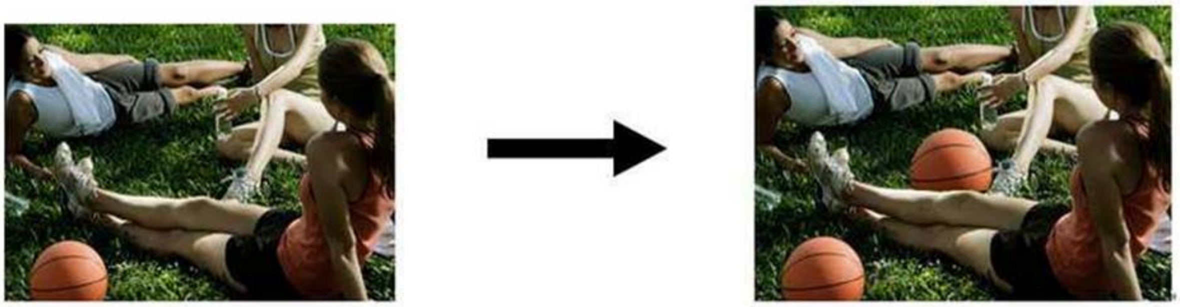


Fig. 1. Duplicating a region and moving it to the same image [4].

In recent years, many techniques have been proposed to examine the comprehensiveness of the images. Some techniques have used digital watermarking schemes to determine the validity of the image and also to determine their comprehensiveness [5]. There are also many other techniques that detect image forgery in the absence of watermarking and encryption. Such techniques use digital image library layers [6-10].

The structure of this paper is as follows: In the second section, the research background is studied, and in the third part, the proposed method is presented. The results are provided in the fourth section and compared with the previous methods. In the final section, the conclusions are presented.

2. AN OVERVIEW OF PREVIOUS WORKS

An image, more than millions of words, can affect viewers. Simultaneously, the wide availability of software packages for editing images, even for novice users, has made it very simple to change the image or create a new one. This increases the likelihood of fraudulent visual information that is no longer confined to experts. As a result, the confidence and integrity of the images, with the advancement of today digital technology, is very low. Since 2000, various ways to detect image forgery have been presented, and this section addresses the solutions presented.

Ghorbani et al. [11] used the wavelet transform and decomposition of the cosine transform coefficients to detect copy-move forgery. In the proposed method, using the wavelet transform, the nature of the unique value decomposition as well as alphabetic sorting result in a significant improvement in terms of time complexity compared to the related algorithms. Naturally, regarding how the wavelet transforms, the decrease in the accuracy of the discovery occurs, which can be neglected due to the increase in speed. Since the human eye is more sensitive to low frequencies, the cosine transformation allows for more accurate detection with additional operations such as retouching the image, after copy-move forgery. The results show that the proposed scheme correctly detects such manipulations, provided that no rotation or scale modification has not taken place on the copied area.

In the next method, Babes et al. have proposed a new method for detecting image forgery based on SPT and LBP. First, according to a color image, it converts it into the color space of YCbCr, and transmits the SPT conversion to the color channels of Cb and Cr, and generates a number of multiple and multi-oriented infrastructures. Then, using LBP histogram, the texture is described in each sub-band of the SPT. Histograms from each sub-band are connected to produce a feature vector. Finally, a support vector machine which uses the feature vector to classify fake or valid images, is used. The best accuracy of the proposed method was 94.89% in the CASIA v1.0 database, 33/97% in the CASIA v2.0 database and 96.39% in the Columbia color image database [12].

Chi Man Pan et al. used noise discrepancies on multiple scales as indicators for detecting forgery image imitation. First, the test image is divided into multiple-scale super pixels. At any scale, the noise level function, which represents the relationship between the noise level and the brightness of each segment, is calculated. These sections are not limited by the noise level function and are considered as suspect areas. In the final stage, pixels are identified in the suspected areas of each scale, after the necessary morphology processing, as a divided area (s) [13].

Mare et al. [14] used a histogram factor to detect image manipulation. In this method, the fake areas in the image are automatically detected based on the histogram of the DCT coefficient factor, which is called as the histogram of the agent. When the image is placed under double compression, this histogram factor is shown in the current quantum state as well as the initial phase of quantization. This algorithm is used to identify the manipulation area for maximum twice image compression. This method can find copy-move, paste, as well as pre-processed counterfeits such as rotation and scaling.

Birajdar et al. [15] proposed contrast detection methods using wavelet transform characteristics. Measurement of cross-information to select information features and also eliminating over-the-counter features increase the speed of execution and the classification process's accuracy. Results were obtained using gray images and G components of the input RGB image. This method works well in a wide range of contrast enhancements with precision detection.

Chi man Pan et al. [16] integrated the block-based forgery detection and key-point based forgery detection methods. First, Adaptive over Segmentation algorithm converts the host image into non-overlapping and irregularly adapted blocks, and then the feature points from each block are extracted as block properties, and the block properties are synchronized to place labeled tag points. This method can almost certainly show areas of suspicion of forgery.

Obara et al. have proposed a forgery identification method based on a reversible histogram, which can identify the partial and general manipulation locations and identify the type of manipulation. In the simulation, they validated the effectiveness of detecting and identifying manipulations using 500 database images. The weakening of a low-level image was maintained with an average PSNR of 57 dB and full reversible operation was confirmed [17].

Kuznetsov et al. have proposed a new hash-based motion detection algorithm, which can be used for converted duplicate detection, due to a special preprocessing technique. This method takes the initial image transformation to combine the changes. Based on the hash function, the algorithm calculates the values in a slider window and is used in the hash table to evaluate hash frequencies. Therefore, in order to use this algorithm, it is necessary to combine repetitive changes such as decreasing the intensity of the image, calculating the gradient, expanding on a regular basis, increasing the linear comparative contrast, and the local binary pattern in an unstable form. The research shows that the high definition of the forgery detection, with variation in intensity (tp> 0.7, fp <0.1) for increasing the linear contrast ratio used to convert duplicates, calculating LBP and ALC leads to high levels of detection quality compared to other primary processing methods [18].

Hayat et al. [19] examined forgery detection in digital images through discrete wavelet and discrete cosine transformation. They initially extracted the lowest sub-band bandwidth or approximation coefficient using the DWT of the image, and in the next step, the DCT was used. Then the block features are arranged in a literal way, so that the similar properties are matched to each other.

Behrad and colleagues have tried to combine the characteristics based on the distribution of the first digits of the DCT coefficients, as well as the features based on the periodic quantization in the DCT coefficients, to detect the forgeries of the images with a recognition mark of 55.33% and improvement of 1.4% compared to other methods [20].

3. THE PROPOSED METHOD

Fig. 2 shows the block diagram of the proposed method. In this method, first the image used to extract the attribute is transferred to the gray level. The gray level can show the most manipulation in the image. Of course, it is worth noting that the normal eye cannot detect this image forgery. In gray levels space, image concepts such as edges, image geometry and texture could be displayed. The method of converting color images to gray is calculated according to the following equation.

$$F(R,G,B)=0.299\times R+0.587\times G+0.114\times B \qquad (1)$$

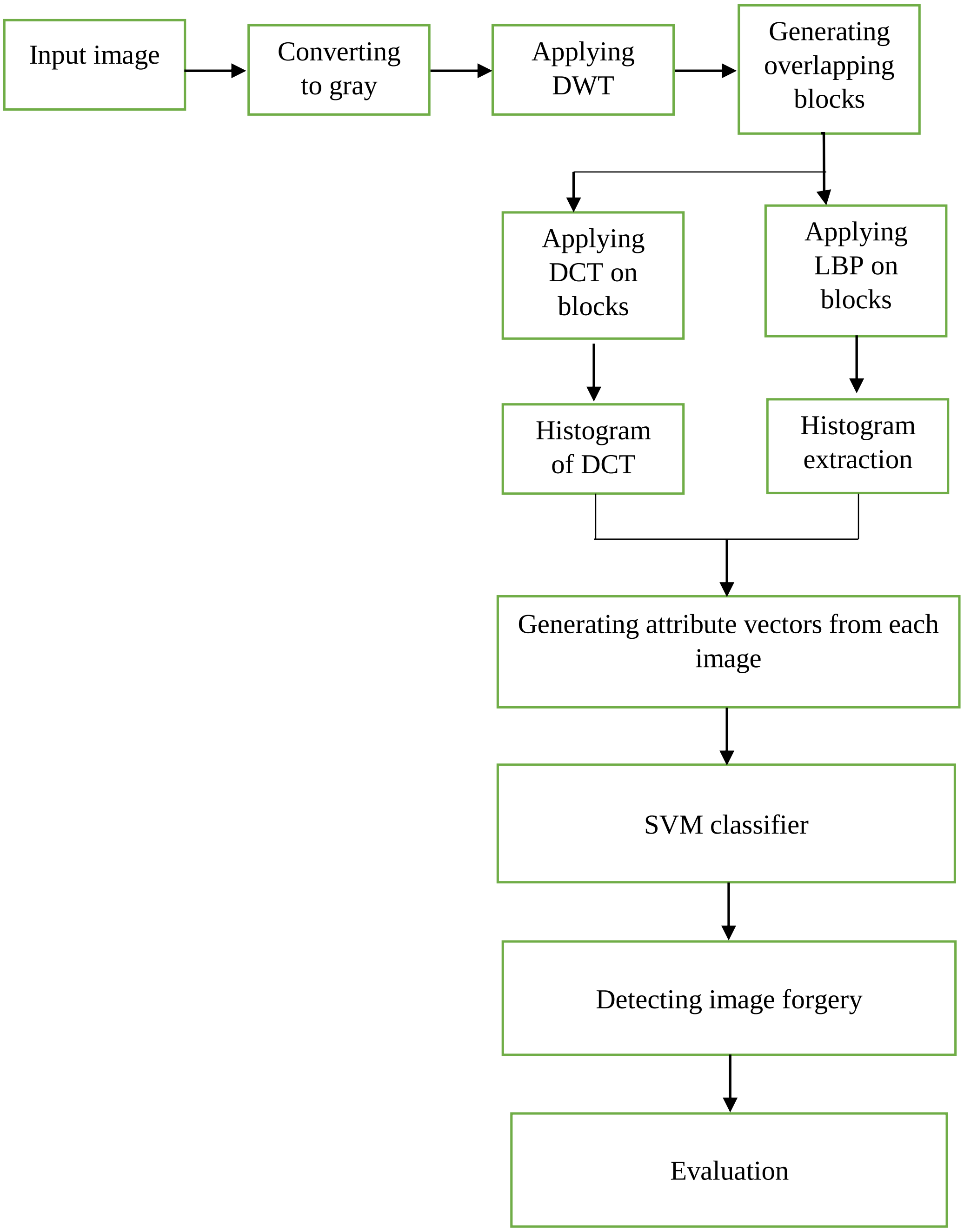


Fig. 2. Diagram block of the proposed method.

3.1. Applying Discrete Wavelet on Image

In the proposed method, the necessary and useful features for detecting forgery will be extracted using the DWT descriptor. With the help of a discrete wavelet transform, the image dimensions will be reduced at each level of conversion. For example, if the size of the image is $2^J \times 2^K$, then in each level of conversion, the dimensions of the image would be $2^{\frac{j}{2}} \times 2^{\frac{j}{2}}$ (Fig. 3). The images in the database used in this research and its dimensions are shown in Table 1. The dimensions of the various parts created by the discrete wavelet transform are shown in this section.

Table 1. Dimensions of images created on images due to the application of discrete wavelet.

Database	Image dimensions	Dimensions of parts created after wavelet transform			
		LL dimensions	HH dimensions	HL dimensions	LH dimensions
Columbia	757×568	190*142	190*142	190*142	190*142
IFS-TC	1024×768 3648×2376	256*192	256*192	256*192	256*192

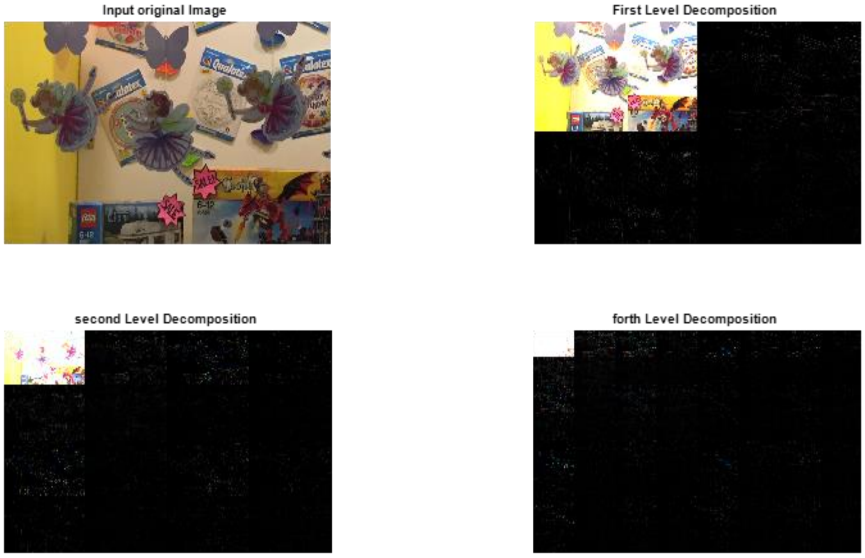

Input original Image
First Level Decomposition
second Level Decomposition
forth Level Decomposition

Fig. 3. a) Wavelet transform at one level b) Wavelet transform at two levels.

These sub-images can be combined together to make the original image redone. DWT decomposition will be used for comparison between multiple images. In order to reduce the properties, an m*n window moves to overlap onto the estimated image, resulting in blocking approximately k1 = (M / 2j-n + 1) (N / 2j-n + 1) blocks. Each block is transformed into a row vector with a length of n2 in the form of column to column known as attribute vectors. These vectors are inserted into an attribute matrix with dimensions of k_1*n2; in which, for each block, an attribute vector is calculated. Attribute vectors are first arranged in a lexical way, and then they are stored in rows of a matrix. Clearly, the benefit of this block is to reduce computations. The resulting step enters the next step and the histogram is applied to it [11].

3.2. Applying the Histogram on the DCT Coefficients of the Image and Extracting the Coefficients

Histogram is a statistical diagnostic of the entire image. In fact, the histogram is a discrete function that is displayed by $h(r_k) = n_k$; where r_k is the gray levels and n_k is the number of pixels which have the surface of r_k in the image. The histogram usually provides very useful statistical information and, since having a small computation, is rapidly processed.

A discrete cosine transform is a kind of discrete Fourier transform, in which the image is split into a set of cosine coefficients with real values. The DCT discontinuous cosine transformation is applied only to functions and the image has a pairwise symmetry. DCT is used to detect manipulations created in the image, especially images that are compact; because the energy is compressed or image information is in the fewer coefficients of the image. In this method, the histogram is calculated for each DCT coefficient. However, since these frequency coefficients are often quantized to zero, only low-frequency histograms are used. After sorting the coefficients, a certain number of high-coefficient coefficients are chosen to produce the histogram. Next, the generated histogram period is calculated [20].

To calculate the period, equation (2) is used [20]:

$$H(p) = \frac{1}{i_{\max} - i_{\min} + 1} \sum_{i\,\min}^{i\,\max} h(i \times p + s_0) \qquad (2)$$

Where, h is histogram, P coefficient is histogram period and S_0 is the interval index of the histogram with the highest value.

i_{max} and i_{min} are obtained as follows[20]:

$$i_{\max} = \frac{s_{\max} - s_0}{p} \qquad i_{\min} = \frac{s_{\min} - s_0}{p} \tag{3}$$

Where, S_{max} and S_{min} are the highest and lowest index in the histogram of the DCT coefficients.

3.3. Applying Local Binary Patterns Algorithm

The local binary pattern algorithm, or LBP, compares the image of the gray intensity and the brightness of the neighboring pixels of a central pixel with the intensity of the brightness in the center pixel and calculates a new value for the central pixel, and finally the histogram of the total new values of the pixels creates the characteristics of the LBP algorithm. Each part of the LL image is divided into blocks with dimensions of B*B, and then are applied on each LBP. In Equation 4, the local binary pattern is calculated for each pixel.

$$LBP_{r,p}(x_i) = \sum_{n=0}^{P-1} s\left(x_{r,p,n} - x_c\right), s(x) = \begin{cases} 1 & x \geq 0 \\ 0 & x < 0 \end{cases} \tag{4}$$

In equation 4, xi represents the central pixels, r represents the neighboring radius under the calculation, P is the number of pixels under the calculation and in the neighborhood, and n is the desired pixel index. The columns of this histogram are considered as attribute vector.

3.4. Attribute Vector and Matrix

The histogram characteristics described in the previous steps are derived from DCT histogram and LBP histogram in each image. The final attribute vector is created by combining the attribute vector derived from the DCT histogram and the LBP histogram. These features should be such that they can describe that part of the image well with the least amount of information. If these features are very detailed or very general, in both cases, the accuracy of the algorithm will be decreased. These attribute vectors will be assigned to the SVM class as a training attribute vector. As a general rule, 70% of the attribute matrix would be considered for training and 30% for testing. In the next section, the dimensions of the attribute vector as well as the attribute matrix will be discussed. In summary, the number of attribute matrix rows is the number of images in the database, and the number of extracted attributes of this matrix has columns (Table 2).

The dimensions of the feature matrix and the feature vector are shown in Table 2 in the two databases used in the study. The Columbia [22] database contains 363 images of 658*757 dimensions and the database of IFS-TC [23] has 875 images of 1024*768 dimensions. The feature vector length generated by combining the DCT histogram and the LBP histogram on the approximate segment in the violet conversion is shown in this table.

Table 2. Dimensions of the attribute matrix and attribute vector in the proposed method.

Database	Number of images			Length of attribute vector	Dimensions of original images attribute matrix	Dimensions of fake images attribute matrix
	Original	Fake	Total			
Columbia	183	180	363	1*6745	183*6745	180*6745
IFS-TC	424	451	875	1*12288	424*12288	451*12288

3.5. Classification

In the last step of this study, the optimized attribute vectors are classified by the classifier and the accuracy of identifying each of the classifications for each descriptor is calculated. In this research, a support vector machine classifier has been used to classify attribute vectors (Table 3). This categorization uses the super-pages to classify attribute feature vectors. The support vector machine categorization method, one of the linear classification methods, finds the best substrate that separates data from two classes with maximum distance. Since SVM controls a different set of values from each part, it has the ability to distinguish and identify forged parts as well as counterfeit values. SVM classifier has different kernels (windows) for separating interrelated data, such as RBF, MLP, Linear, and Polynomial, which is used to classify the RBF kernel in this study. This is due to the high efficiency and high resolution capability of this kernel.

SVM is a binary classifier. Therefore, in the case of more than two classes, it cannot be used directly. One of the effective methods for using in multi-class mode is the one-on-one approach. In these methods, each time considering two of the classes, the decision boundary between the two is calculated. Then for a different K classes, the K(k-1)/2 distinct classifiers should be designed. To categorize the unknown X data, it is placed in all the classifications obtained and each classifier applies X to a particular class, eventually X belongs to the class with the maximum votes. In practical applications, this method has better performance than other methods [21].

The SVM teaches itself by the properties known as inputs to its learning algorithm. SVM selects the appropriate margins between classes during SVM training.

If the points of the training are defined as xi, xj and input vector is $x_i \epsilon R^n$ and the value of the class of i=1,……, N is defined as $x_j \epsilon \{-1,1\}$, then, in the case where the data are linearly separable, the output is given by the equation below[20]:

$$y = \left(\sum_{i=1}^{N} a_i\, x_j (x_i \times x) + b\right) \tag{5}$$

Where, y is the output of the equation, x_j is the value of the training sample class of x_i and represents the interior product. N is the number of records used for training. a_i is a positive integer smaller than the constant number of C, and x_i is also a support vector. If the data are not linearly segregated, the above equation changes to the following equation [20]:

$$y = \left(\sum_{i=1}^{N} a_i\, x_j k(x_i . x) + b\right) \tag{6}$$

The function $k(x_i,x_j)$ is the kernel function [22].

Table 3. Dimensions of training attribute matrix and SVM classifier test in the proposed method.

Database	Length of attribute vector	Dimensions of the attribute matrix of original images	Dimensions of the attribute matrix of fake images	Dimensions of the training matrix in original images	Dimensions of the test matrix in original images	Dimensions of the training matrix in fake images	Dimensions of the test matrix in fake images
Columbia	1*6745	183*6745	180*6745	121*6745	62*6745	120*6745	60*6745
IFS-TC	1*12288	424*12288	451*12288	297*12288	127*12288	315*12288	136*12288

4. EVALUATION OF RESULTS

In this section, the proposed method is implemented on the Columbia [22] and IFS-TC [23] databases and the results are compared with the baseline methods. The basic methods include detecting counterfeiting in the image using a discrete wavelet-based method, DWT and DCT, and a histogram.

4.1. Database

This study is implemented to evaluate the proposed method in the Columbia and IFS-TC databases. The Columbia database contains 1845 images with 128x128 pixels. This database was developed at Columbia University and at the Digital Image Processing Lab. There are 933 original images and 912 forged images in this database. The IFS-TC database is provided by the challenge committee of image forgery at IEEG. This database contains the original images taken by digital camera types and is divided into two main categories of original and fake.

4.2. Accuracy of the Algorithm

To evaluate the proposed method, this method is applied to the two databases and compared with other results. The results of detection accuracy in detecting image forgery in DWT, DCT and histogram methods are compared in Table 4 with the proposed method.

Table 4. Accuracy of detection in detecting image forgery in the proposed method and other methods in the SVM classifier with the RBF kernel.

Database	DWT[15]	DCT[15]	HIST[14]	Proposed
Colombia	81/83	85/85	75/38	97/98
IFS-TC	82/02	86/11	76/35	98/14

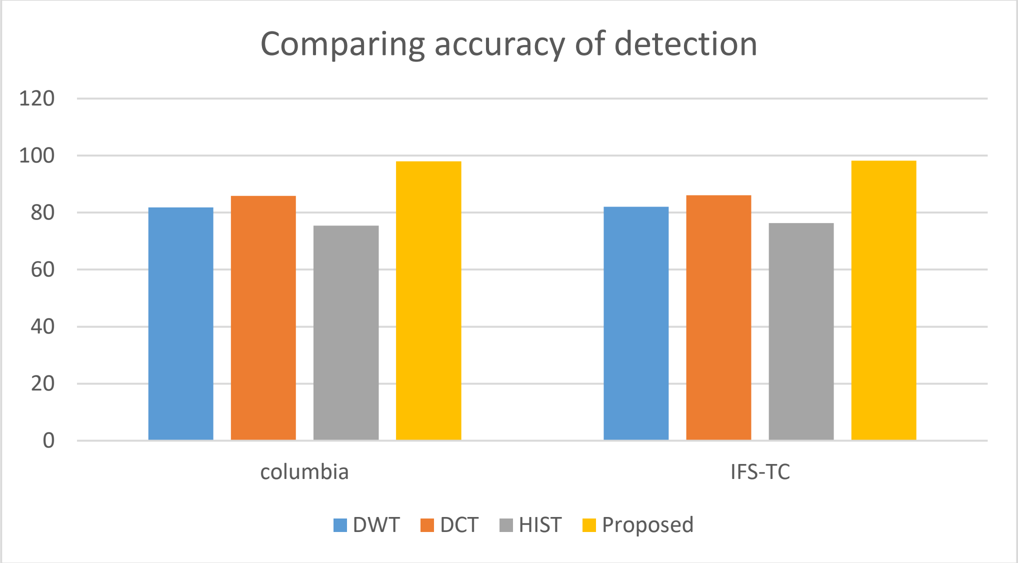


Fig. 4. Detection accuracy graph for image forgery in the proposed method and other methods.

Table 5. Accuracy of detection in detecting image forgery in the proposed method and other methods in SVM classifier with MLP kernel.

Database	DWT[15]	DCT[15]	HIST[14]	Proposed
Columbia	80/73	84/75	73/35	97/91
IFS-TC	79	87/28	74/81	97/99

Table 6. Accuracy of detection in detecting image forgery in the proposed method and other methods in the SVM classifier with Linear kernel.

Database	DWT[15]	DCT[15]	HIST[14]	Proposed
Columbia	81/83	85/85	75/38	97/95
IFS-TC	82/02	86/11	76/35	98/14

To further evaluate the classification, the support vector machine classifier with two other kernels was also evaluated. Linear and MLP kernels are among the most widely used kernels used in the support vector machine. As it is clear from the above tables, the RBF kernel has had better results. As shown in Table 4, the proposed method yields better results in detecting accuracy in image counterfeiting. Although the histogram method has better results than the old and most used DCT and DWT approaches. As shown in Table 4 and Fig. 5, the histogram-based method has the weakest result.

4.3. Real Positive and Negative Rates

Table 7 shows the positive real rate, Fig. 5 is the graph related to positive real rate, Table 8 shows the results of the negative real rate and Fig. 6 is the graph related to negative real rate. As shown in Tables 7 and 8, both in the negative and the positive real rates, the proposed method has been superior to the basic methods, so that the positive real rate of 94.1 and the negative real rate of 5.95%, compared to other results indicate the superiority of this approach. Although the DWT method has been able to garner a more positive real rate than the traditional and old DCT method, the negative real rate of this DCT approach to DWT, as well as considering the better accuracy of this method compared to DWT, prove the superiority of this method to DWT. It should be noted that the histogram-based method, due to the small size of the training vector and the uniqueness of the extracted features, could not successfully handle the separation of fake and manipulated data.

Table 7. Positive real rate for detecting image forgery in the proposed method and other methods.

Database	DWT	DCT	HIST	proposed
Columbia	88/87	80/84	73/36	94/10
IFS-TC	87/84	84/21	69/21	93/21

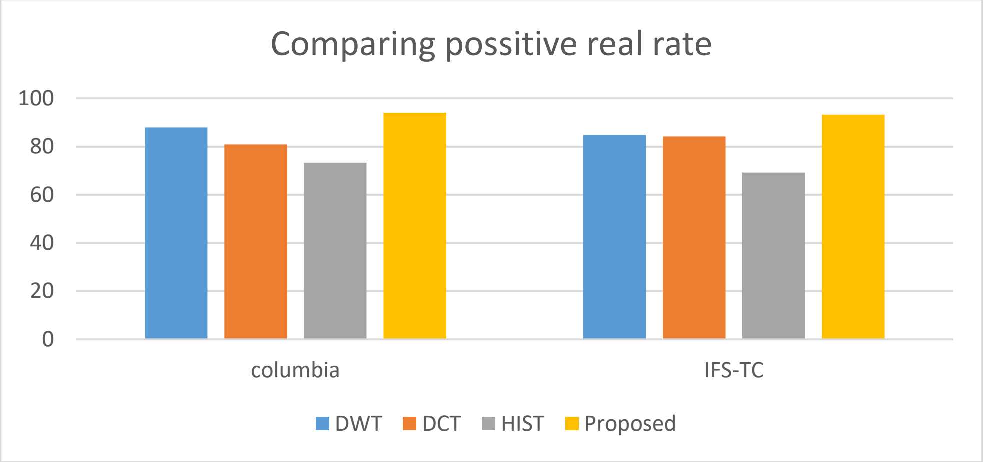


Fig. 5. The positive real rate graph of the detection of image forgery in the proposed method and other methods.

Table 8. Negative real rate in detecting image forgery in the proposed method and other methods.

Database	DWT	DCT	HIST	proposed
Columbia	79/52	81/99	73/41	95/50
IFS-TC	81/25	80/63	75/25	93/14

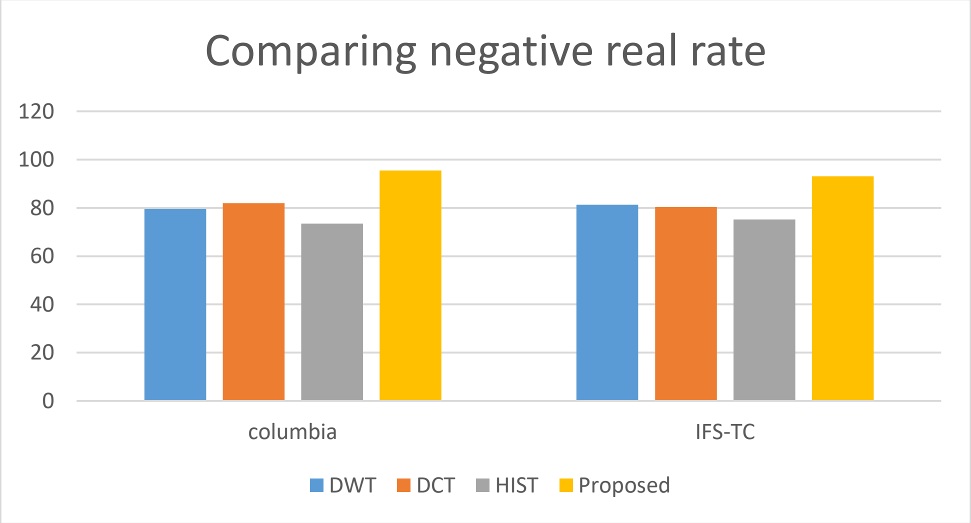
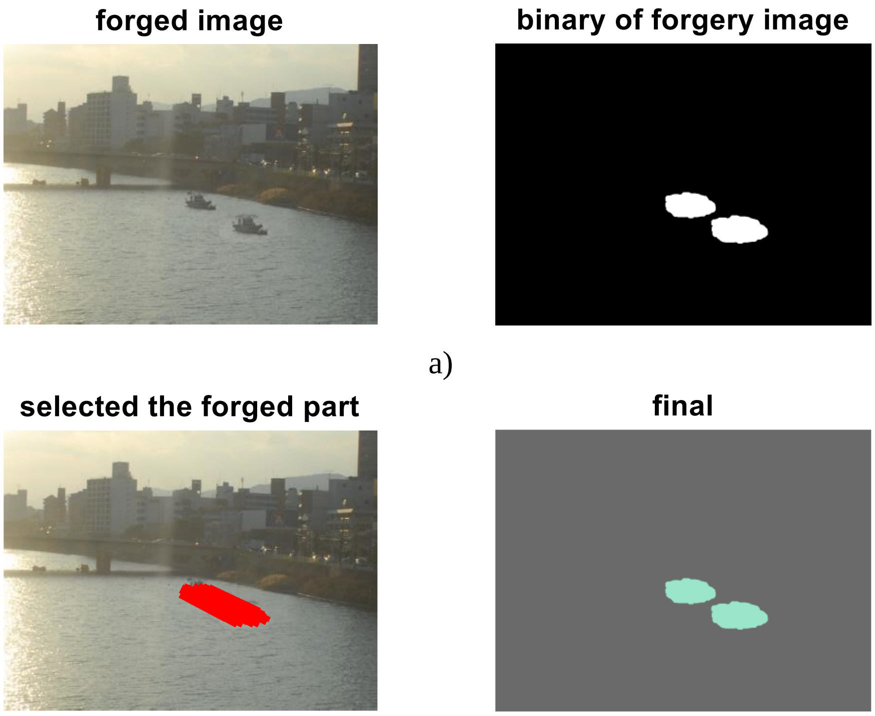


Fig. 6. Negative real rate graph of the detection of image forgery in the proposed method and other methods.

4.4. Image Examples of Identification

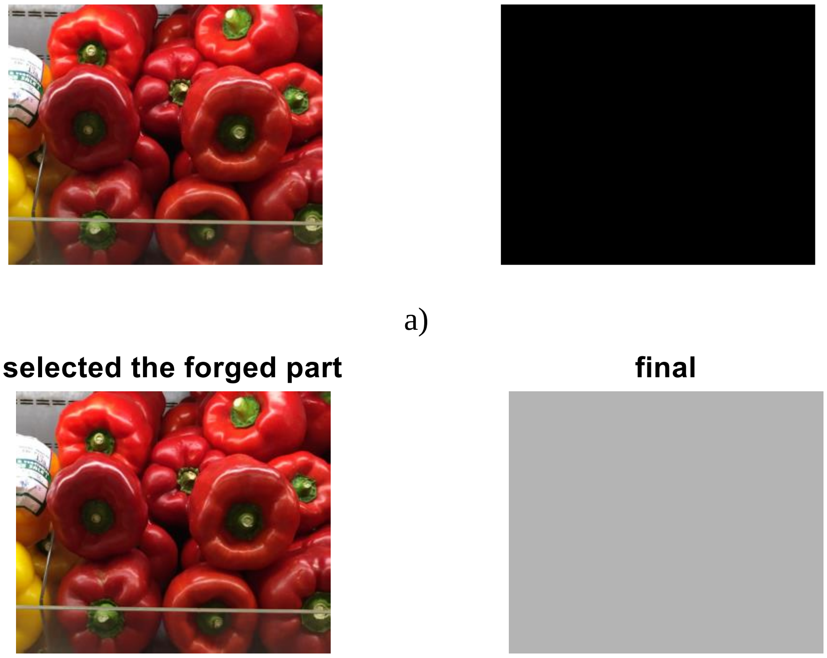
After identifying the image in which it was forged, it is time to carefully identify the forged areas in the image. Fig. 7 shows the forged area in the forged image. Since the proposed method has a high ability to identify and distinguish the original images and fake images, the identification of forged regions would be very simple.



a)

b)

Fig. 7. a) Identification of image forgery; b) Identification of the forged area by the proposed algorithm.



a)

b)

Fig. 8. a) a picture in which no forging has occurred; b) an unidentified area of forging in the original image.

5. CONCLUSION

The proposed method was implemented in the MATLAB environment and tested with the Columbia and IFS-TC databases. The results show the accuracy of 98.97 and 14.98, respectively, at best status.

In the proposed method in this paper, due to the large volume of features, a number of features were selected, for which we used the Benford property selection method. After testing on the images of the databases, the following results were obtained:

1. The accuracy of detection in detecting image forgery in the proposed method is 98.97 and 98.14 at best.
2. The results of the negative and positive real rates are 95.5% and 94.1%, respectively and show the superiority of this method compared to other results.
3. Finally, the new proposed method identifies the area of forgery after it detects the forging or originality of the image.

In this study, a new method for identifying forgery in images was implemented and simulated on the Columbia and IFS-TC databases. In this method, after extracting the attribute in the process presented, using the SVM classification, the image forgery is detected. The new proposed method identifies the domain of forgery after it recognizes the forging or originality of the image. The accuracy of detection is 97.1%, and the real positive rate is 94.1 and the actual negative rate is 95.95 in the proposed method.

REFERENCES

[1] Rey, C. and J. LD, **"A Survey of Watermarking Algorithms for Image Authentication"**, *EURASIP Journal on Ap plied Signal Processing*, Vol. 6, 2002.

[2] Ng, T.T ,.C.Y. Lin, and Q. Sun, "**Passive-blind im-Age Forensics**", *in Multimedia Security Technologies for Digital Rights, chapter 06. Elsvier*, 2006.

[3] Ng, T.T. and Q. Sun, **"Blind Detection of Photomontage using Higher Order Statistics",** in *IEEE International Symposium on Circuits and Systems*, 2004.

[4] J. Dong, W.W., **"CASIA Tampered Image Detection Evaluation Database (CASIA TIDE v2 ٠.)[**Online]", *Available: http://forensics.idealtest.org:8080/index_v2.html.* Chinese Academy of Sciences, 2010.

A. C. Popescu, "**Exposing Digital Forgeries in Color Filter Array Interpolated Images",** *IEEE Transactions on Signal Processing*, Vol. 53(10), pp. 12, 2005.

[5] Dirik, A.E. and N. Memon, "**Image Tamper Detection based on Demosaicing Artifacts",** *in IEEE International Conference on Image Processing (ICIP)*, pp. 4, 2009.

[6] Johnson, M.K., **"Exposing Digital Forgeries by Detecting Inconsistencies in Lighting",** *in ACM Multimedia and Security Workshop*, pp. 10, 2005.

[7] M. K. Johnson, H.F., **"Exposing Digital Forgeries in Complex Lighting Environments",** *IEEE Transactions on In-formation Forensics and Security*, Vol. 2(3), pp. 11, 2007.

[8] Ng, T.T. and Q. Sun, **"A Data Set of Authentic and Spliced Image Blocks",** *Tech. Rep., DVMM, Columbia University, Dataset*: http://www.ee.columbia.edu/ln/dvmm/downloads/AuthSplicedDataSet/photographers.htm., 2004.

[9] Shi, Y.Q. and G. Xuan, **"Steganalysis Versus Splicing Detection",** *in International Workshop on Digital Watermarking,* 2007.

[10] Ghorbani, M., M. Firozmand, and A. Faraahi, "**DWT-DCT (QCD) Based Copy-Move Image Forgery Detection"**, *in 18th IEEE International Conference on Systems, Signals and Image Processing (IWSSIP*), pp. 14, 2011.

[11] Gh. Muhammad, M.H.A.-H., and M. H. George Bebis, **"Image Forgery Detection using Steerable Pyramid Transform and Local Binary Pattern",** *Springer*, 2013.

[12] Chi-Man Pun, Xiao-Chen Yuan, and Xiu-Li Bi, **"Image Forgery Detection Using Adaptive Over-Segmentation and Feature Point Matching",** *IEEE Transactions on Information Forensics and Security*, 2015.

[13] Archana V. Mire, S. B. Dhok, N. J. Mistry and P. D. Porey, **"Factor Histogram based Forgery Localization in Double Compressed JPEG Images",** *Procedia Computer Science 54*, pp. 690–696, 2015.

[14] L. G. Birajdar, e., **"Passive Image Manipulation Detection Using Wavelet Transform and Support Vector Machine Classifier"**, *Springer*, 2016.

[15] Chi-Man Pun, X.-C. Yuan, and Xiu-Li Bi**, "Multi-Scale Noise Estimation for Image Splicing Forgery Detection**", *Elsevier Inc*., 2016.

[16] Y. Obara, Y. Niwa, and SH. Wada, **"Detection and Identification of Image Manipulation Based on Reversible Histogram shift.",** *Wiley Periodicals*, Inc., 2017.

[17] A. Kuznetsov and V. Myasnikov, **"A New Copy-Move Forgery Detection Algorithm using Image Preprocessing Procedure",** *Elsevier Inc*., 2017.

[18] Khizar Hayat, Tanzeela Qazi, **"Forgery Detection in Digital Images via Discrete Wavelet and Discrete Cosine Transforms",** *Computers and Electrical Engineering, elsevier*, pp.1-11, 2017

[19] N. Alipour and A. Behrad, **"Forgery and Double Compression Detection in Digital Images using Combined Features of Quantization Effects on DCT Coefficients"**, *Tabriz Jouornal of Engineering Electrical*, Vol. 47(2), 2017.

[20] Srivastava, D.K. and L. Bhambhu, **"Data Classification using Support Vector Machine",** *Journal of Theoretical and Applied Information Technology*, 12, pp. 8, 2010.

[21] http://www.ee.columbia.edu/ln/dvmm/downloads/authsplcuncmp/dlform.html

[22] http://ifc.recod.ic.unicamp.br/fc.submission/