Indonesian Journal of Electrical Engineering and Computer Science
Vol. 24, No. 1, October 2021, pp. 226~235
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v24.i1.pp226-235

Forgery detection algorithm based on texture features

Ismail Taha Ahmed[1], Baraa Tareq Hammad[2], Norziana Jamil[3]
[1,2]College of Computer Sciences and Information Technology, University of Anbar, Anbar, Iraq
[3]College of Computing and Informatics, Universiti Tenaga Nasional, Selangor, Malaysia

Article Info

Article history:

Received Apr 15, 2021
Revised Jul 22, 2021
Accepted Aug 4, 2021

Keywords:

CMFDs
Haralick
KNN
LBP
Logistics
Naïve Bayes
SFTA

ABSTRACT

Any researcher's goal is to improve detection accuracy with a limited feature vector dimension. Therefore, in this paper, we attempt to find and discover the best types of texture features and classifiers that are appropriate for the coarse mesh finite differenc (CMFD). Segmentation-based fractal texture analysis (SFTA), local binary pattern (LBP), and Haralick are the texture features that have been chosen. K-nearest neighbors (KNN), naïve Bayes, and Logistics are also among the classifiers chosen. SFTA, LBP, and Haralick feature vector are fed to the KNN, naïve Bayes, and logistics classifier. The outcomes of the experiment indicate that the SFTA texture feature surpassed all other texture features in all classifiers, making it the best texture feature to use in forgery detection. Haralick feature has the second-best texture feature performance in all of the classifiers. The performance using the LBP feature is lower than that of the other texture features. It also shows that the KNN classifier outperformed the other two in terms of accuracy. However, among the classifiers, the logistic classifier had the lowest accuracy. The proposed SFTA based KNN method is compared to other state-of-the-art techniques in terms of feature dimension and detection accuracy. The proposed method outperforms other current techniques.

Corresponding Author:

Ismail Taha Ahmed
College of Computer Sciences and Information Technology
University of Anbar, Anbar, Iraq
Email: ismail.taha@uoanbar.edu.iq

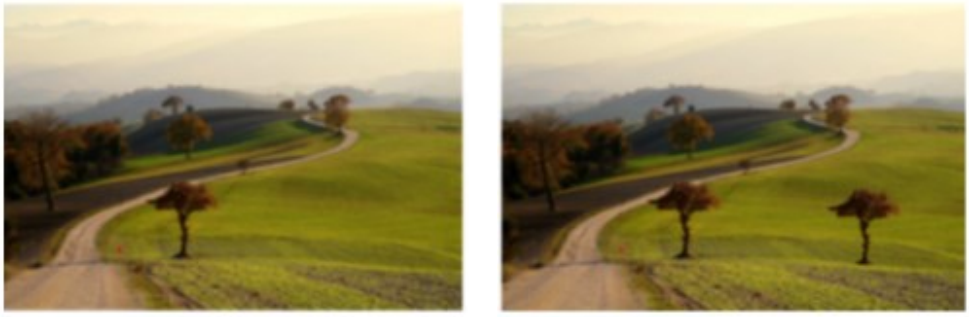
1. INTRODUCTION

Because of the weaknesses of image editing software in the past, image manipulation was difficult and easy to discern by the human eye; however, recent tremendous advancements in image editing software have rendered image manipulation very easy while still making the image difficult to distinguish by the human eye. In general, digital forgery detection can be divided into active and passive method. The active method is fully reliant on the original image data, such as the watermarking information. Nevertheless, we have no information about the watermarking in the passive method. As a result, passive approaches have piqued researchers' interest [1], [2].

One of the most common methods for detecting passive forgery images is the copy-move. It is an operation that copying a portion of an image and pasting it into the same image without leaving any obvious modifications or markings visible to the naked eye as shown in Figure 1. Figure 1 indicates that the forgery does not leave any obvious modifications or marks noticeable to the human eye.

There have been several studies on coarse mesh finite differenc (CMFD) [3]-[11] in recent years. Hussain *et al*. [3], suggested CMFD based on multi-scale local binary pattern (LBP) and multi-scale Weber local descriptors (WLD) texture features. The main drawback of multiscale WLD is that as the number of scales considered grows, the feature dimension grows exponentially. Zhang *et al*. [4], proposed CMFD based

on LBP and discrete cosine transform (DCT). For each the gray image blocks, LBP of magnitude of 2D-DCT coefficient are extracted. Suresh and Rao [5], suggested CMFD based on gray-level co-occurrence matrix (GLCM) texture features. In one direction, 22 statistical features are calculated. Alhussein [6], proposed a CMFD based on LBP texture features and extreme learning machine (ELM) used as classifier. Vidyadharan and Thampi [7], proposed a CMFD based on multi-texture description using LBP, LPQ, binary Gabor pattern (BGP) and orientation using steerable pyramid transform (SPT). The ReleifF algorithm is used to pick features, and the random forest classifier is used to classify them. Zhu *et al*. [8], proposed a CMFD based on gray-level co-occurrence matrix and K-d tree used as classifier. Teerakanok and Uehara [9], proposed a CMFD based on GLCM and rotational invariant feature description technique. Shan *et al*. [10], proposed a CMFD based on GLCM and convolutional neural network (CNN) used as classifier. Jaiswal and Srivastava [11], proposed a CMFD based on combining four features histogram of oriented gradients (HoG), laws texture energy (LTE), digital wavelet transform (DWT), and LBP. As a classifier, they used logistic regression.



(a) (b)

Figure 1. Copy-move forgery example [1]: (a) original image and (b) copy-move image

While many of the techniques mentioned above have advantages, they also have drawbacks, such as a large number of feature vectors and a high time complexity for example [3], [7], [12], [13]. This encourages us to look for ways to extract the features with the fewest features for each block while remaining resistant to post-processing operations. Therefore, in this paper, we attempt to find and discover the best types of texture features and classifiers that are appropriate for the CMFD. Segmentation-based fractal texture analysis (SFTA), local binary pattern (LBP), and Haralick are the texture features that have been chosen. KNN, naïve Bayes, and Logistics are also among the classifiers chosen. The remainder of this paper is structured in the following way.

The texture analysis techniques are presented in section 2. The proposed methods are described in the section 3. The experimental results and analysis are discussed in section 4. Finally, in section 5, conclusions can be drawn.

2. TEXTURE ANALYSIS

Texture analysis techniques have been uniquely successful in medical imaging [14], [15], steganalysis [16], signature verification [17], and forgery detection [18]. In the applications mentioned above, texture analysis can detect the details that invisible to human eye. In forgery detection, image manipulation was difficult to discern by the human eye. Therefore, the texture analysis plays a distinct role in field of the image forgery detection by disclosing information hidden within the forged image that is harder to identify with the naked eye. The texture feature descriptors SFTA, local binary pattern (LBP), and Haralick feature are used for extracting texture feature in this section. Each texture descriptor is explained in the following sub-section.

2.1. Local binary pattern (LBP)

The key process of the LBP texture descriptor [19] is to mark each pixel in the image by thresholding the neighborhood pixels with the center pixel and considering the output as a binary number as shown in Figure 2. It can be observation from Figure 2 that the LBP can be extracted in a circular neighborhood (P, R), where P is the number of neighbors and R is the radius of the neighborhood. The key justification for using the LBP is that its value in the copied and pasted region remains consistent even after applying a series of post-processing operations. As a result, texture plays an important role in forgery detection.

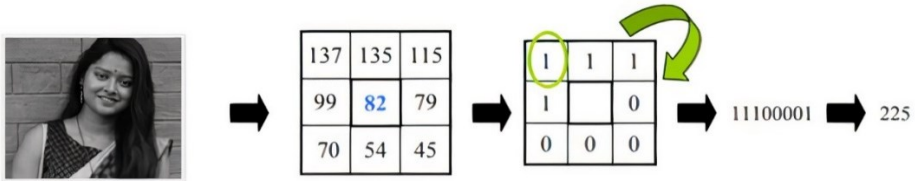


Figure 2. The basic local binary pattern (LBP) operator

2.2. Segmentation-based fractal texture analysis (SFTA)

The main process of the SFTA [20] algorithm depend on two steps. Decompose the input grayscale image into a collection of binary images in the first step. The two-threshold binary decomposition (TTBD) method was used to decompose the data. In the second step, SFTA feature vectors are computed for each binary image generated using the fractal dimension from its regions' boundaries as shown in Figure 3. We also calculate the regions' mean gray level and size (pixel counting). See [20] for more information. The following mathematical expression (1) is used to extract the SFTA features.

$$\emptyset_{sfta}(U) = \begin{cases} 1 \ if \ \exists(i',j') \in N_8[(i,j)]: \\ \quad \emptyset_e(i',j') = 0\text{^} \\ \quad \emptyset_e(i,j) = 1 \\ \quad 0 \ Otherwise \end{cases} \tag{1}$$

Where, N8 [(i, j)] represents the number of connected pixels initialized as 8 in this work. $\emptyset_e(i,j)$ *is* binary image.

The number of thresholds chosen determines the dimension of the features vector. For example, if we were counted as three, seven binary images would be produced. The three characteristics mentioned above were present in each of these binary images. Using the SFTA technique, 21 features were produced for each image. As we mentioned earlier, most of the CMFD techniques have drawbacks, such as a large number of feature vectors and a high time complexity. However, among the texture image analysis methods, SFTA features are used due to robustness and low computationally cost. It is therefore interesting to apply SFTA features extraction in forgery detection.

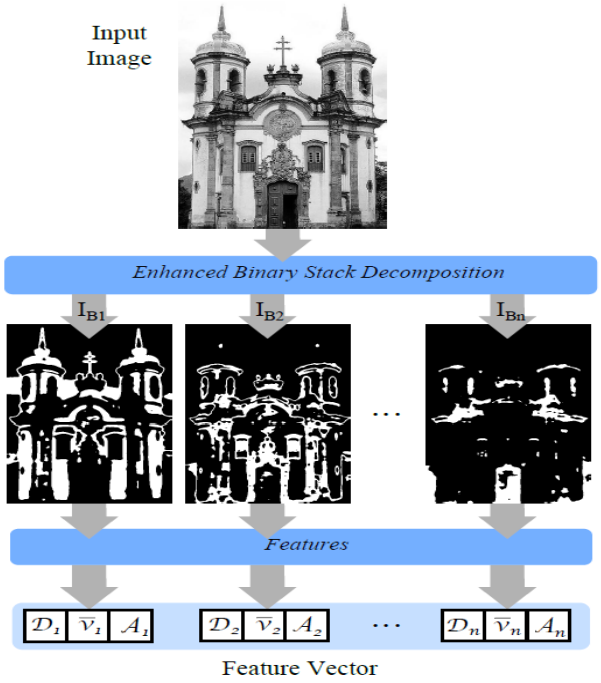


Figure 3. SFTA extraction diagram

2.3. Haralick

The common texture features are the Haralick descriptors. The Haralick descriptors [21] are derived from a co-occurrence matrix and are based on statistical moments. Haralick for a given image I(x,y) of size M*N having Gt as total distinct gray levels illustrates the number of times a pixel I at position (x,y) occur in accordance with pixel j at position (x+ Δx, y+ Δy). A(i,j,d,) denotes the frequency of occurrence and is mathematically expressed as:

$$A(i,j,d,\theta) = \sum_{X=1}^{M}\sum_{y=1}^{N}\begin{Bmatrix} 1, if\ I(x,y) = \ i\ and\ I\ (x+\Delta x, y+\Delta y) = j \\ 0\ otherwise \end{Bmatrix} \quad (2)$$

where 'd' specifies the offset distance Δx, Δy between the pixel and its neighbor and θ represents the direction.

There were fourteen Haralick features suggested. angular second moment (ASM), correlation, homogeneity, sum average, entropy, energy, comparison, sum variance, inverse different moment (IDM), maximum correlation coefficient (MCC), sum entropy, contrast, difference entropy, and variance are some of these features. Gray level co-occurance matrices feature extraction method is applied to each forged image to extract distinctive properties that are used to enhance feature extraction accuracy.

3. THE PROPOSED METHODS

Here, the block diagram of the proposed work is shown in Figure 4. Three algorithms are also developed (algorithms 1-3). The steps and algorithms are explained as:

Algorithm 1. Proposed CMFD_ based KNN classifier

```
Input: Image Dataset.
Output: Detection as Authentic/Forged Image (Copy-move)).

for (all the images) apply
    1. Read the image from the folder using I = Imread (image).
    2. Converting the RGB image to gray image (rgb2gray (I)).
    3. Apply Block Partition on gray image to obtain non-overlapping block.
    4. For each of block, Extract the SFTA features {fsfta1, fsfta2, fsfta3, fsfta4,…
       fsfta21} to obtain 21-dimension feature vector.
    5. For each of block, Extract the LBP features {flbp1, flbp2, flbp3, flbp4, flbp5…
       flbp59} to obtain 59-dimension feature vector.
    6. For each of block, Extract the Haralick features {fharck1, fharck2, fharck3,
       fharck4… fharck14} to obtain 14-dimension feature vector.
    7. Feed these feature vectors to the KNN classifier for training.
    8. Test the trained KNN model to identify the image as original or forged.
End for
```

Algorithm 2. Proposed CMFD_ based naïve Bayes classifier

```
Input: Image Dataset.
Output: Detection as Authentic/Forged Image (Copy-move)).

for (all the images) apply
    1. Read the image from the folder using I = Imread (image).
    2. Converting the RGB image to gray image (rgb2gray (I)).
    3. Apply block partition on gray image to obtain non-overlapping block.
    4. For each of block, Extract the SFTA features {fsfta1, fsfta2, fsfta3, fsfta4,…
       fsfta21} to obtain 21-dimension feature vector.
    5. For each of block, Extract the LBP features {flbp1, flbp2, flbp3, flbp4, flbp5…
       flbp59} to obtain 59-dimension feature vector.
    6. For each of block, Extract the Haralick features {fharck1, fharck2, fharck3,
       fharck4… fharck14} to obtain 14-dimension feature vector.
    7. Feed these feature vectors to the Naïve Bayes classifier for training.
    8. Test the trained Naïve Bayes model to identify the image as original or forged.
End for
```

Algorithm 3. Proposed CMFD_ based logistic classifier

```
Input: Image Dataset.
Output: Detection as Authentic/Forged Image (Copy-move)).

for (all the images) apply
    1. Read the image from the folder using I = Imread (image).
    2. Converting the RGB image to gray image (rgb2gray (I)).
    3. Apply block partition on gray image to obtain non-overlapping block.
```

```
    4. For each of block, Extract the SFTA features {fsfta1, fsfta2, fsfta3, fsfta4,…
       fsfta21} to obtain 21-dimension feature vector.
    5. For each of block, Extract the LBP features {flbp1, flbp2, flbp3, flbp4, flbp5…
       flbp59} to obtain 59-dimension feature vector.
    6. For each of block, Extract the Haralick features {fharck1, fharck2, fharck3,
       fharck4… fharck14} to obtain 14-dimension feature vector.
    7. Feed these feature vectors to the Logistic classifier for training.
    8. Test the trained Logistic model to identify the image as original or forged.
End for
```

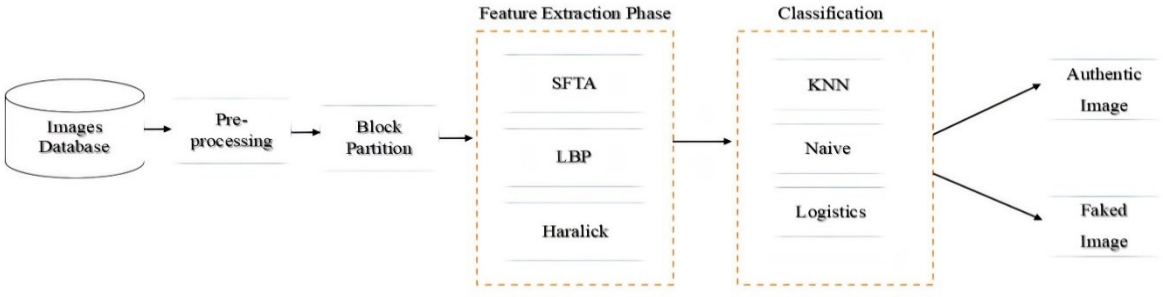


Figure 4. Flow diagram of the proposed method

3.1. Preprocessing of input image

To reduce the overall computational complexity, we first create a gray-scale image from a RGB image using the formula in (3).

$$Igray = 0.228R + 0.587G + 0.114B \quad (3)$$

Where R, G, and B are the input color image channels, and Igray is the gray-level values.

3.2. Block partition

In order to reduce the time consuming, non-overlapping blocks are uesd in this paper. The grayscale image (*Igray*) of size M×N is divided into non-overlapping blocks of size R×R pixels. As a result, the image is broken down into (M-R+1) (N-R+1) blocks. Various texture features are obtained for each block in the following section.

3.3. Texture feature extraction

Feature extraction is a crucial step in copy move forgery detecting. The choice of distinct features will make a significant impact in forgery detection. The two most important criteria of good features are to reduce dimensionality and prevent duplication. Three types of texture features are extracted from these blocks in order to obtain the feature vector, as explained in the following section.

3.3.1. Segmentation-based fractal texture analysis (SFTA)

For each block, SFTA features are extracted. The obtained SFTA feature vectors are {fstfa1, fstfa2, fstfa3, fstfa4, fstfa5… fstfa21}. The dimension of SFTA feature vector is 1×21.

3.3.2. The LBP features

For each block, LBP features are extracted. The obtained LBP feature vector are {flbp1, flbp2, flbp3, flbp4, flbp5… flbp59}. The dimension of LBP feature vector is 1×59.

3.3.3. Haralick

For each block, Haralick features are extracted. The obtained Haralick feature vectors are {fharck1, fharck2, fharck3, fharck4… fharck14}. The dimension of Haralick feature vector is 1×14.

3.4. Classification

Here, Image forgery detection is a two-class problem, i.e. authentic vs. forged. A crucial step is classifying authentic and forged (copy-moved) images from a standard image dataset. According to the literature survey, three well-known classifiers such as k-nearest neighbors (KNN) [22], naive Bayes [23], and logistics [24] are utilized in this article. Bayes' theorem is the foundation of the naive Bayesian classifier. It's

a simple probabilistic classifier that counts the frequency and combinations of values in a dataset to calculate a set of probabilities. It is assumed that one attribute's likelihood has no bearing on the probability of the others [23].

To use the KNN classifier [22], first, the Euclidean distance between the feature vector of test sample and all the feature vector of training samples are calculated. The unknown class label is then determined using the KNN class labels, with k being an integer. The Logistic regression, also known as statistical regression model, is based on ordinary regression [24]. The aim of logistic regression is to select the best model for assessing the relationship between a collection of independent variables (predictor) and a dichotomous feature of interest (outcome variable).

4. EXPERIMENTAL RESULTS AND ANALYSIS

This section explains the experimentation and evaluation of different classifiers' output on different texture features. The image datasets are identified first, and then the performance evaluation and results are presented. Finally, the proposed methods are compared to current methods in a comparative study.

4.1. Dataset

The image datasets MICC-F220 [25] and MICC-F2000 [26] are public databases that have been commonly used for copy-move detection. There are 220 images in MICC-F220: 110 tampered images and the other 110 are originals. The images have a resolution ranging from 722×480 to 800×600. The MICC-F2000 contains 2000 images, including 1300 original images, and 700 forgeries. The resolution is 2048×1536.

4.2. Performance evaluation and results

4.2.1. Performance evaluation

When the training dataset is tiny, the k-fold cross-validation evaluation provides accurate results. As a result, feature vectors are randomly split into 10 folds of roughly equal size in our experiments. Seventy percent of the feature vectors are used for training, while thirty percent are used for testing. In order to evaluate the performance of the KNN, naïve Bayes, and logistics classifiers, the confusion matrix shows three measures such as detection accuracy, sensitivity, and specificity. These metrics can be calculated as follows:

$$Sensitivity = \frac{Tp}{(Tp+Fn)} \quad (4)$$

$$Specificity = \frac{Tn}{(Tn+Fp)} \quad (5)$$

$$Detection\ Accurcy = \frac{(Tp+Tn)}{(Tp+Tn+Fp+Fn)}\ x\ 100\ \% \quad (6)$$

where the number of correctly identified forged images is indicated by true positive (*Tp*). The number of false negatives (*Fn*) shows how many forged images were detected incorrectly. The number of incorrectly detected unchanged images is referred to as false positive (*Fp*). The number of correctly detected unchanged images is indicated by true negative (*Tn*).

4.2.2. Evaluation result

To compare the performance of different classifiers within different textures features, detection accuracy of KNN, naïve Bayes, and Logistics classifiers are computed in order to find the best one. Table 1 and Table 2 show the detection accuracy of 3 feature extraction methods and 3 classification methods across MICC-F220 and MICC-F2000 database.

Table 1. Detection accuracy of three classifiers across different features and MICC-F220 database

Classifier	LBP	Haralick	SFTA
	Detection accuracy (%)		
KNN	81.81	86.36	95.45
Naive Bayesian	72.27	77.05	86.81
Logistic	63.23	68.18	72.63

Table 2. Detection accuracy of three classifiers across different features and MICC-F2000 database

Classifier	LBP	Haralick	SFTA
	Detection accuracy (%)		
KNN	80.13	79.05	83.39
Naive Bayesian	61.67	67.43	72.18
Logistic	59.88	62.28	69.50

Although the same feature vectors are entered into all classifiers, they produce different results, and the reason is that each classifier contains different characteristics. The following section details the performance of each classifier.

a) KNN

The accuracy of KNN classifier is found to be 81.81, 86.36, and 95.45 for LBP, Haralick, and SFTA, respectively as shown in Figure 5. As a result, it's fair to assume that the KNN classifier performs better than the other two.

b) Naive Bayesian

The accuracy of Naive Bayesian classifier is found to be 72.27, 77.05, and 86.81 for LBP, Haralick, and SFTA, respectively as shown in Figure 6. As a result, the Naive Bayesian classifier is coming as a second rank after the KNN classifier, and it is regarded as superior to the logistic classifier.

c) Logistic

The accuracy of logistic classifier is found to be 63.23, 68.18, and 72.63 for LBP, Haralick, and SFTA, respectively as shown in Figure 6. As a result, the logistic classifier is coming as a last rank after the KNN and Naive Bayesian classifier, and it yields the worst outcomes.

Tables 1 and 2 show that the SFTA texture feature outperformed all other texture features in all classifiers, making it the best texture feature to use in forgery detection. Haralick feature has the second-best texture feature performance in all of the classifiers. The performance of the LBP feature is lower than that of the other texture features. The results collected with the help of SFTA features show that SFTA can be successful for CMFD.

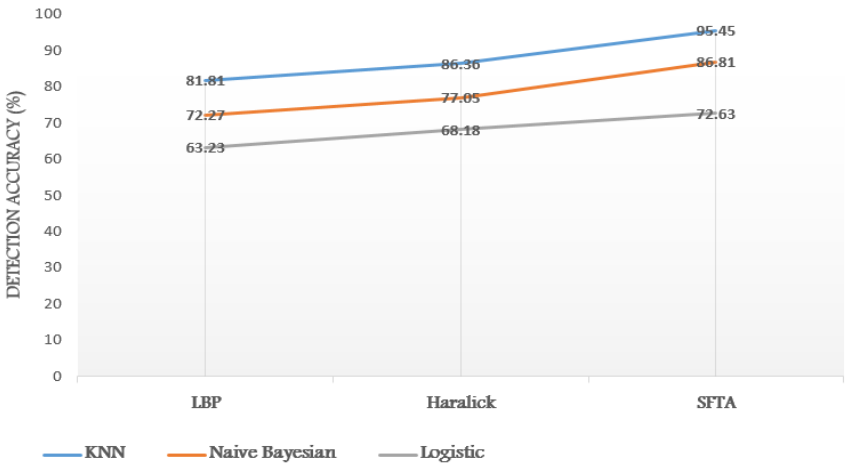


Figure 5. Detection accuracy of KNN, naive Bayesian, logistic classifiers based on different texture features across MICC-F220 database

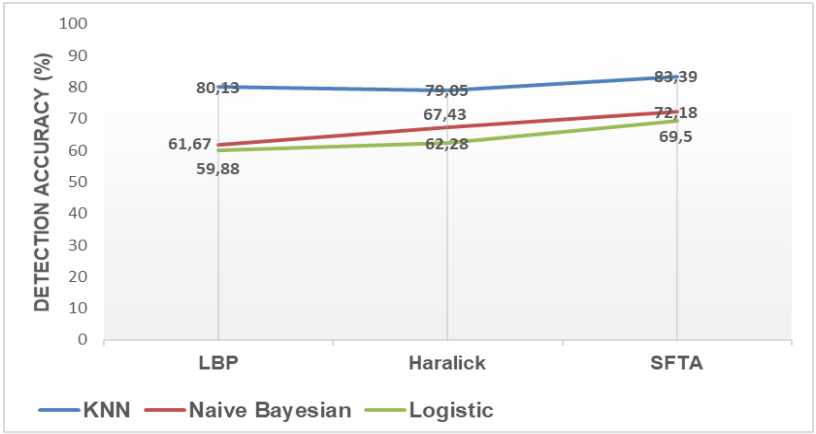


Figure 6. Detection accuracy of KNN, naive Bayesian, logistic classifiers based on different texture features across MICC-F2000 database

4.3. Comparison with previous ic-mfd works

This section compares the propose approach to the other CMFD approaches that have been used previously. Because the CMFD keypoint-based approach has several drawbacks, such as failing to detect small duplicate regions and failing to discriminate between copy-move areas and naturally equivalent areas. Therefore, our comparison will be limited to existing block-based methods.

Depending on the detection accuracy and the feature size, a comparison will be made between them. A comparison will be made between them based on detection accuracy and feature size. some of the approaches that have been considered for comparison in [3], [7], [12], [27]-[29]. Each of these approaches are focused on the of texture features extraction. The proposed method is compared to other state-of-the-art techniques in terms of feature dimension and detection accuracy, as shown in Table 3. In terms of detection accuracy and small feature vector dimension, the proposed method outperforms other existing methods, as shown in Table 3. The suggested feature extraction technique has less features vector dimensions than most current methods, making the techniques computationally simpler as shown in Figure 7. The two techniques [7], [12] yielded good results. However, they use 480 and 970 feature vectors, respectively. The high dimension of the feature vector requires a lot of computational effort.

Table 3. Performance comparison with previous methods

Methods	Feature vector dimension	Features	Classifier	Detection accuracy (%)
[3], 2015	1203	Multi-WLD & LBP	SVM	85.56
[7], 2017	970	LBP&LBQ,	Random Forest	92.13
[12], 2014	480	LBP	SVM	94.89
[27], 2017	256	RLBP	g2NN	83.3
[28], 2019	128	GLCM	RANSAC	82.72
[29], 2020	24	GLCM	SVM	90.45
Proposed	21	STFA	KNN	*95.45*

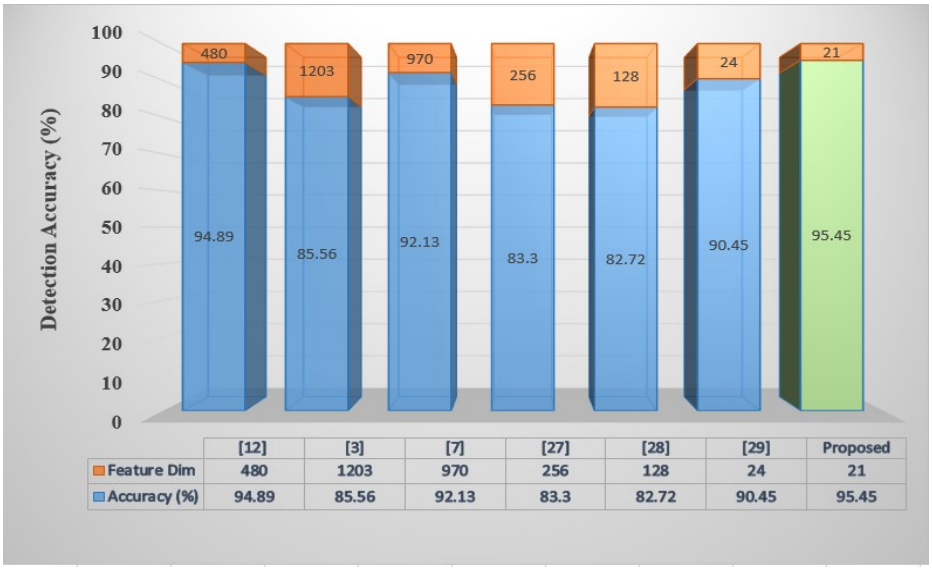


Figure 7. Performance evaluation of current methods in various sets of feature vector dimensions

5. CONCLUSION

This paper focuses on the copy move image identification using different texture features extraction methods and classifiers. First step is image preprocessing, then splitting the image, next, texture feature extraction methods are applied. The texture feature extraction methods are SFTA, LBP, and Haralick and these feature values are fed to three different classifiers like KNN, Naïve Bayesian and logistic which identify the forged and authentic images. The accuracy of KNN classifier is found to be 81.81, 86.36, and 95.45 for LBP, Haralick, and SFTA, respectively. As a result, it's fair to assume that the KNN classifier performs better than the other two. Among classification algorithms KNN and Naïve Bayesian algorithms have been more successful. The most successful combination is the combination of SFTA and KNN with 95.45%.

Experiments results show that the SFTA texture feature outperformed all other texture features in all classifiers, making it the best texture feature to use in forgery detection. Haralick feature has the second-best texture feature performance in all of the classifiers. The performance of the LBP feature is lower than that of the other texture features. The proposed method is compared to other state-of-the-art techniques in terms of feature dimension and detection accuracy. In terms of detection accuracy and small feature vector dimension, the proposed method outperforms other existing copy-move image forgery detection methods. The suggested feature extraction technique has less features vector dimensions than most current methods, making the techniques computationally simpler.

ACKNOWLEDGEMENTS

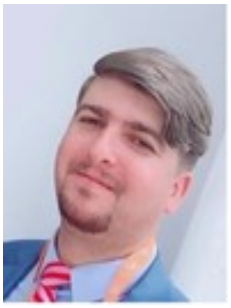
This research is supported by Uniten BOLD Publication Fund 2021.

REFERENCES

[1] K. Liu, *et al*., "Copy move forgery detection based on keypoint and patch match," *Multimedia Tools and Applications*, vol. 78, no. 22, pp. 31387–31413, 2019, doi: 10.1007/s11042-019-07930-5.
[2] I. T. Ahmed, B. T. Hammad, and N. Jamil, "Image Copy-Move Forgery Detection Algorithms Based on Spatial Feature Domain," *2021 IEEE 17th International Colloquium on Signal Processing & Its Applications (CSPA)*, 2021, pp. 92-96, doi: 10.1109/CSPA52141.2021.9377272.
[3] M. Hussain, S. Qasem, G. Bebis, G. Muhammad, H. Aboalsamh, and H. Mathkour, "Evaluation of image forgery detection using multi-scale Weber local descriptors," *International Journal on Artificial Intelligence Tools*, vol. 24, no. 4, 2015, doi: 10.1142/s0218213015400163.
[4] Y. Zhang, C. Zhao, Y. Pi, S. Li, and S. Wang, "Image-splicing forgery detection based on local binary patterns of DCT coefficients," *Security and Communication Networks*, vol. 8, pp. 2386–2395, 2015, doi: 10.1002/sec.
[5] G. Suresh and C. S. Rao, "Copy Move Forgery Detection Using GLCM Based Statistical Features," *Int. J. Cybern. Informatics*, vol. 5, no. 4, pp. 165–171, 2016, doi: 10.5121/ijci.2016.5419.
[6] M. Alhussein, "Image Tampering Detection Based on Local Texture Descriptor and Extreme Learning Machine," *2016 UKSim-AMSS 18th International Conference on Computer Modelling and Simulation (UKSim)*, 2016, pp. 196-199, doi: 10.1109/UKSim.2016.39.
[7] D. S. Vidyadharan and S. M. Thampi, "Digital image forgery detection using compact multi-texture representation," *J. Intell. Fuzzy Syst*., vol. 32, no. 4, pp. 3177–3188, 2017, doi: 10.3233/JIFS-169261.
[8] Y. Zhu, X. J. Shen, and H. P. Chen, "Covert copy-move forgery detection based on color LBP," *Acta Automatica Sinica*, vol. 43, no. 3, pp. 390–397, 2017, doi: 10.16383/j.aas.2017.c160068.
[9] S. Teerakanok and T. Uehara, "Copy-move Forgery Detection Using GLCM-Based Rotation-Invariant Feature: A Preliminary Research," *2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC)*, 2018, pp. 365-369, doi: 10.1109/COMPSAC.2018.10259.
[10] W. Shan, Y. Yi, R. Huang, and Y. Xie, "Robust contrast enhancement forensics based on convolutional neural networks," *Signal Process. Image Commun*., vol. 71, pp. 138–146, 2019, doi: 10.1016/j.image.2018.11.011.
[11] A. K. Jaiswal and R. Srivastava, "A technique for image splicing detection using hybrid feature set," *Multimedia Tools and Applications*, vol. 79, pp. 11837–11860, 2020, doi: 10.1007/s11042-019-08480-6.
[12] G. Muhammad, M. H. Al-Hammadi, M. Hussain, and G. Bebis, "Image forgery detection using steerable pyramid transform and local binary pattern," *Machine Vision and Applications*, vol. 25, no. 4, pp. 985–995, 2014, doi: 10.1007/s00138-013-0547-4.
[13] C. S. Prakash, A. Kumar, S. Maheshkar, and V. Maheshkar, "An integrated method of copy-move and splicing for image forgery detection," *Multi. Tools Appl*., vol. 77, pp. 26939-26963, 2018, doi: 10.1007/s11042-018-5899-3.
[14] A. H. Mir, M. Hanmandlu, and S. N. Tandon, "Texture analysis of CT images," *IEEE Engineering in Medicine and Biology Magazine*, vol. 14, no. 6, pp. 781-786, Nov.-Dec. 1995, doi: 10.1109/51.473275.
[15] S. G. Mougiakakou, I. K. Valavanis, A. Nikita, and K. S. Nikita, "Differential diagnosis of CT focal liver lesions using texture features, feature selection and ensemble driven classifiers," *Artif. Intell. Med*., vol. 41, no. 1, pp. 25-37, 2007, doi: 10.1016/j.artmed.2007.05.002.
[16] Y. Q. Shi, C. Chen, G. Xuan, and W. Su, "Steganalysis versus splicing detection," *International Workshop on Digital Watermarking*, pp. 158–172, 2007, doi: 10.1007/978-3-540-92238-4_13.
[17] M. A. Ferrer, J. F. Vargas, A. Morales, and A. Ordonez, "Robustness of Offline Signature Verification Based on Gray Level Features," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 3, pp. 966-977, June 2012, doi: 10.1109/TIFS.2012.2190281.
[18] J. Dong, W. Wang, T. Tan, and Y. Q. Shi, "Run-length and edge statistics based approach for image splicing detection," *Int. Workshop on Digital Watermarking*, pp. 76–87, 2008, doi: 10.1007/978-3-642-04438-0_7.
[19] T. Ojala, M. Pietikäinen, and D. Harwood, "A comparative study of texture measures with classification based on featured distributions," *Pattern Recognition*, vol. 29, no. 1, pp. 51–59, 1996, doi: 10.1016/0031-3203(95)00067-4.
[20] A. F. Costa, G. Humpire-Mamani, and A. J. M. Traina, "An Efficient Algorithm for Fractal Analysis of Textures," *25th SIBGRAPI Conference on Graphics, Patterns and Images*, 2012, pp. 39-46, doi: 10.1109/SIBGRAPI.2012.15.
[21] R. M. Haralick, "Statistical and structural approaches to texture," *Proceedings of the IEEE*, vol. 67, no. 5, pp. 786-804, May 1979, doi: 10.1109/PROC.1979.11328.

[22] M. Tanveer, K. Shubham, M. Aldhaifallah, and S. S. Ho, "An efficient regularized K-nearest neighbor based weighted twin support vector regression," *Knowledge-Based Systems*, vol. 94, pp. 70-87, 2016, doi: 10.1016/j.knosys.2015.11.011.
[23] D. Lowd and P. Domingos, "Naive Bayes models for probability estimation," *Proceedings of the 22nd International Conference on Machine learning*, 2005, pp. 529-536, doi: 10.1145/1102351.1102418.
[24] J. R. Wilson and K. A. Lorenz, *Modeling binary correlated responses using SAS, SPSS and R (ICSA Book Series in Statistics 9)*, Switzerland: Springer, 2015, doi: 10.1007/978-3-319-23805-0.
[25] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, and G. 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, pp. 1099-1110, Sept. 2011, doi: 10.1109/TIFS.2011.2129512.
[26] V. S. Kulkarni and Y. V Chavan, "Comparison of methods for detection of copy-move forgery in digital images," *Spvryan's International Journal of Engineering Sciences & Technology*, vol. 1, no. 1, 2014.
[27] A. Roy, A. Konda, and R. S. Chakraborty, "Copy move forgery detection with similar but genuine objects," *2017 IEEE International Conference on Image Processing*, 2017, pp. 4083-4087, doi: 10.1109/ICIP.2017.8297050.
[28] M. Chowdhury, H. Shah, T. Kotian, N. Subbalakshmi, and S. S. David, "Copy-Move Forgery Detection using SIFT and GLCM-based Texture Analysis," *TENCON 2019 - 2019 IEEE Region 10 Conference (TENCON)*, 2019, pp. 960-964, doi: 10.1109/TENCON.2019.8929276.
[29] G. Suresh and C. S. Rao, "Copy Move Forgery Detection Through Differential Excitation Component-Based Texture Features," *International Journal of Digital Crime and Forensics*, vol. 12, no. 3, pp. 27–44, 2020, doi: 10.4018/IJDCF.2020070103.

BIOGRAPHIES OF AUTHORS



Ismail Taha Ahmed received his B.E. and M.Sc. degrees in Computer Science from College of Computer Science and Information Technology, University of Anbar, Anbar, in 2005 and 2009, respectively. He received his Ph.D. degrees in Computer Science from College of Computer Science and Information Technology, Universiti Tenaga Nasional, Putrajaya, Malaysia, in 2018. His research interests Include Image Processing, Image Quality Assessment, Deep Learning, Image Forgery Detection, and Computer Vision.

Baraa Tareq Hammad received her B.E. and M.Sc. degrees in Computer Science from College of Computer Science and Information Technology, University of Anbar, Anbar, in 2005 and 2012, respectively. She received her Ph.D. degrees in Computer Science from College of Computer Science and Information Technology, Universiti Tenaga Nasional, Putrajaya, Malaysia, in 2018. Her research interests Include Information Security, IoT and Network Security.

Norziana Jamil received her BSc (Information Technology), 2000, form Universiti Kebangsaan Malaysia, and she received her M.Sc. (Information Security), 2005, from Royal Holloway Universiti of London, UK, while she finishes her PhD (Security in Computing), 2013, from UPM university, she is interested in cryptography, Authentication, SCADA system, wireless sensor network.