International Journal of Engineering

Journal Homepage: www.ije.ir

A Novel Image Splicing Detection Algorithm Based on Generalized and Traditional Benford's Law

A. Parnak, Y. Baleghi Damavandi*, S. J. Kazemitabar

Department of Electrical & Computer Engineering, Babol Noshirvani University of Technology, Babol, Iran

PAPER INFO

Paper history:
Received 13 September 2021
Received in revised form 08 December 2021
Accepted 23 December 2021

Keywords:
Image Forgery Detection
Image Splicing
Mantissa Distribution
Benford's Law

ABSTRACT

Due to the ease of access to platforms that can be used by forgers to tamper digital documents, providing automatic tools for identifying forged images is now a hot research field in image processing. This paper presents a novel forgery detection algorithm based on variants of Benford's law. In the proposed method, Mean Absolute Deviation (MAD) feature is extracted using traditional Benford's law. Also, generalized Benford's law is used for mantissa distribution feature vector. In addition to Benford's law-based features, other statistical features are used to construct the final feature vector. Finally, support vector machine (SVM) with three different kernel functions is used to classify original and forged images. The method has been tested on two common image datasets (CASIA V1.0 and V2.0). The experimental results show that 0.27% and 0.21% improvements on CASIA V1.0 and CASIA V2.0 datasets were achieved, respectively in detection accuracy by the proposed method in comparison to best state-of-the-art methods. The proposed efficient algorithm has a simple implementation. Moreover, on the basis of Benford's law rich features are extracted from images so that classification process is efficiently performed by a simple SVM classifier in a short time.

doi: *10.5829/ije.2022.35.04a.02*

1. INTRODUCTION

Nowadays, with the development of digital image editing [1]. software and applications, it is possible to change the content of digital images and share them in a wide range of cyberspace more than before. Accordingly, a platform has been created for abusers to tamper digital documents and images according to their ominous aims. They try to do forgery in a way that is not recognizable through the human eye. Therefore, there is a need for automatic tools for detecting tampered images.

Generally, there are two common kinds of image forgeries: image cloning (or copy-move) and image splicing (or cut-paste). Image tampering is the process of replacing the content of an original image by one or some new content. If the content of original image is replaced by new content of the same image, it is named as copy-move, and if the content of original image is replaced by new content of another image, it is called image splicing. So far, many approaches have been suggested to detect the two common forgeries, and are still being developed, which can be used to prevent possible further damages.

This paper presents a new method based on generalized and traditional Benford's law for detection of spliced images. To do this, the RGB image is converted into YCbCr image and after image blocking, two-dimensional discrete cosine transform (2D-DCT) is applied to each block. Then, features based on mantissa distribution, mean absolute deviation (MAD), standard deviation (STD) and entropy, are extracted and then combined to construct a final feature vector. Finally, support vector machine (SVM) [2]. is applied for classification. The proposed method is able to detect spliced images with the highest accuracry rate on CASIA V1.0 and CASIA V2.0 databases in compare to other recent methods. The method has a simple implementation and using the presented technique of applying Benford's law can extract the powerful features from images so that classification process is efficiently performed by an SVM in a short time.

*Corresponding Author Institutional Email: y.baleghi@nit.ac.ir (Y. Baleghi)

Please cite this article as: A. Parnak, Y. Baleghi Damavandi, S. J. Kazemitabar, A Novel Image Splicing Detection Algorithm based on Generalized and Traditional Benford's Law, ***International Journal of Engineering, Transactions A: Basics*** Vol. 35, No. 04, (2022) 626-634

Rest of the paper is organized as follows: Section 2 presents literature review. The proposed method for image splicing detection is described in section 3. The experimental results and performance evaluation are given in section 4. Finally, section 5 concludes the paper.

2. LITERATURE REVIEW

Despite the huge literature on image splicing detection [3]. they can be categorized as handcrafted and deep features-based algorithms. In the category of deep features-based works, El-Latif et al. [4] applied an algorithm based on Convolutional Neural Network (CNN), that contains 6 convolutional layers and 3 pooling layers, to extract features from the spliced image. The results achieved 95.45% detection rate for CASIA V1.0 and 97.27% for CASIA V2.0 datasets.

On the other hand, several works are reported on handcrafted features. They are often based on coefficients of popular transforms like Discrete Wavelet Transform (DWT). In this category, Kasban and Nassar [5] applied Hilbert–Huang transform (HHT) features for copy-move and image splicing detection. The results showed that the suggested method achieved detection accuracies 98.95% and 99.13% for CASIA V1.0 and CASIA V2.0 databases, respectively.

Fusheng and Gao [6] suggested an approach based on Discrete Cosine Transform (DCT) Coefficient-Pair histogram. In this method, first, the image is transformed by DCT, and then the differential DCT coefficient matrix of two directions, such as horizontal and vertical direction are calculated. Then coefficient-pair histograms for each differential DCT coefficient matrix are computed within the given threshold. The experiments show 99.24% and 97.56% accuracy rates in CASIA V1.0 and CASIA V2.0 datasets, respectively. DWT and Local Binary Pattern (LBP) histogram have been suggested for detecting image splicing by Kaur and Gupta [7]. The results achieved detection accuracies 92.62% and 94.09% for CASIA V1.0 and CASIA V2.0 databases, respectively.

Application of the Markov features in Quaternion Discrete Cosine Transform (QDCT) was proposed by Li et al [8]. In this approach, 96.43% and 92.66% accuracies were achieved at the CASIA V1.0 and CASIA V2.0 datasets. Sheng et al. [9] proposed a method based on Discrete Octonion Cosine Transform (DOCT) and Markov features. Initially, the 8×8 block DOCT is applied to source image and then, the standard deviation is used to process the corresponding parts of all blocks of the image. Finally, the Markov feature vector of the DOCT coefficient is extracted. The method achieved 98.04% and 97.83% detection accuracies for CASIA V1.0 and CASIA V2.0 in databases their results.

Yildirim and Alutas [10] introduced an expert system that extracts features (statistical and textural) from high-level sub-bands of Stationary Wavelet Transform (SWT) domain to detect forgery. The results show that this approach has 99.29% and 99.58% detection rates on CASIA V1.0 and CASIA V2.0 datasets.

Muhammad et al. [11], used YCbCr color space. A directional pyramid conversion is applied for the two Cb and Cr channels that will result in a number of sub-bands. From each sub-band, LBP features are calculated and finally the LBP histograms of each of these sub-bands are merged to construct the final feature vector. 94.89% and 97.33% accuracy rates were obtained on CASIA V1.0 and CASIA V2.0 databases, respectively. Agarwal and Chand [12] presented a technique that applies entropy filter and Local Phase Quantization (LPQ) texture operator. The entropy filter generally highlights the boundary of the forged regions. They achieved 95.41% and 98.33% accuracies for CASIA V1.0 and CASIA V2.0 datasets, respectively.

Alahmadi et al. [13] applied LBP and DCT for detecting forgery and obtained 97% and 97.5% detection rates on the CASIA V1.0 and CASIA V2.0 databases, respectively. Shen et al. [14] detected splicing through a model consisting of Textural Features based on the Gray Level Co-occurrence Matrices (TF-GLCM). In the TF-GLCM, the GLCM was computed based on the Difference Block Discrete Cosine Transform (DBDCT) arrays for capturing the textural information and the spatial relationship between image pixels. In addition, the mean and standard deviation of textural features were used instead as elements in feature vector. In this algorithm, 98.54% and 97.73% accuracy rates were obtained respectively on CASIA V1.0 and CASIA V2.0 datasets. Sharma and Ghanekar [15] presented a two-phase hybrid technique using some features and Extreme Learning Machine (ELM). In the first phase, Laplacian of Gaussian and autocorrelation were used to differentiate computer generated images and natural images. In the second phase, estimation of color filter array pattern and sensor noise were used for splicing detection. A 98.51% precision rate under effect of simple splicing was obtained on Dresden Image database.

Habibi and Hassanpour [16] applied an algorithm based on color distribution of pixels in chroma space. First, edge pixels were extracted using contourlet transform and then, interquartile range (IQR) metric of the Cb and Cr histograms was utilized to distinguish the forged edges and authentic ones in YCbCr color space. The results achieved 97.08% accuracy Columbia Image Splicing Detection Evaluation Dataset.

Singh and Bansal [17] analyzed the use of Benford's law for detecting effects of single and double compression as a sign of image tampering. Their reported results showed that deviation from Benford's curve in the compressed images could be used to detect forgery.

Bonettini et al. [18]. applied this law to detect Generative Adversarial Network (GAN)-generated images. Random forest classifier had been used for classification in their work.

3. PROPOSED METHOD

The framework of the proposed method is shown in Figure 1, which consists of four consecutive steps. In the first step, the RGB image is converted into YCbCr image. In the second step, the blocking operation is performed on the image and then a two-dimensional discrete cosine transform (2D-DCT) is applied to each block. In the third step, the proposed features are extracted and then combined to construct a final feature vector. Finally, support vector machine (SVM) is applied for classification. In the following, the proposed splicing forgery detection method is described in detail.

3. 1. Preprocessing The YCbCr color space, as a preprocessing operation, plays an important and effective role in detecting forged images. In most of the methods presented so far [5, 7, 10-14, 16, 19-25]. this color space conversion has been used. YCbCr channels are given in the following equations:

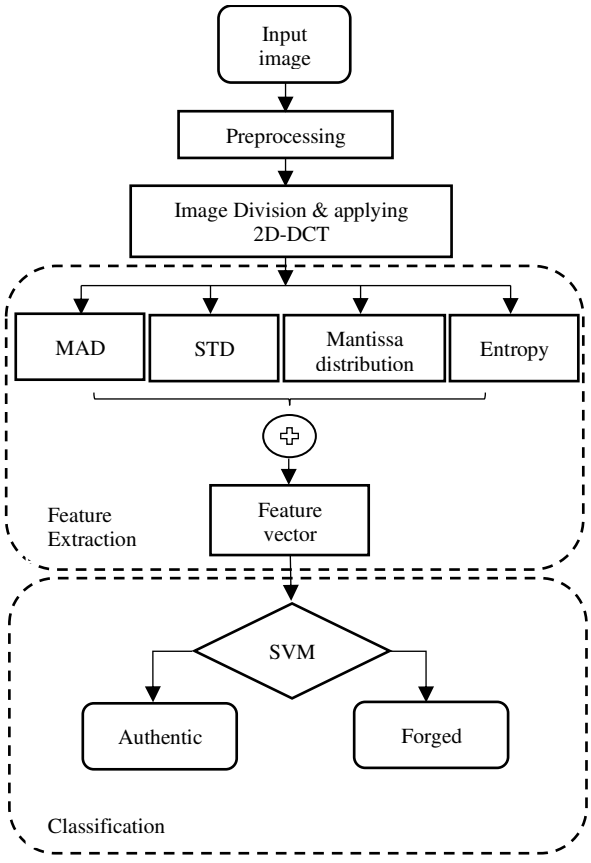

Figure 1. The framework of the proposed method

$$Y = 0.299R + 0.587G + 0.114B \quad (1)$$

$$Cb = 0.168736R + 0.331264G + 0.5B \quad (2)$$

$$Cr = 0.5R + 0.418688G + 0.081312B \quad (3)$$

where Y, Cb, and Cr represent luminance, chrominance blue and chrominance red components, respectively. In this step, the input RGB image is converted into YCbCr image to obtain three images for the Y, Cb and Cr channels.

3. 2. Image Division and Applying 2D-DCT The image is divided into 8×8 non-overlapping blocks and a two-dimensional discrete cosine transform (2D-DCT) is applied to each block to obtain 64 DCT coefficients. The value located in the upper left corner of the block is called the direct current coefficient (DC) and the other 63 values are called the alternative current coefficients (AC). The 2D-DCT transformation is given in Equation (4).

$$F\_uv = \alpha\_u\, \alpha\_v \sum\_(x=0)\^(M-1) \sum\_(y=0)\^(N-1) f\_xy \cos[\pi(2x+1)u/2M \cos[\pi(2y+1)v/2N]]] \quad (4)$$

$$\alpha\_u = \begin{cases} 1/\sqrt{M}, & x = 0 \\ \sqrt{(2/M)}, & 1 \le x \le M-1 \end{cases}$$

$$\alpha\_v = \begin{cases} 1/\sqrt{N}, & y = 0 \\ \sqrt{(2/N)}, & 1 \le x \le N-1 \end{cases}$$

where f_{xy} and F_{uv} denote the pixel values at coordinates (x, y) and the DCT coefficient at coordinates (u, v), respectively. The values of M and N are equal to 8 here. Some studies [19-22]. show that the low frequency AC components have effective role in performance of splicing detection system. In this paper, inspired by the studies and different tests, DCT coefficients are selected for extracting features.

3. 3. Feature Extraction In this step, four types of features are used, each of which can be identified separately with a very good percentage, and by combining them the recognition rate has increased. The most important proposed features are based on Benford's law including: mantissa distribution and mean absolute deviation (MAD). Their theoretical basis is given in the following subsections. Also, popular entropy and standard deviation (STD) are used as complementary features to discriminate the forged and authentic images.

3. 3. 1. Mean Absolute Deviation Benford's law [23]. also called the first digit law, is an empirical law that states the probability distribution of the first digits in a set of natural numbers is logarithmic and is defined as:

$$p(x) = \log\_10 [(1 + 1/x), \quad x = 1,2,\dots,9] \quad (5)$$

where x is the value of the first digits and $p(x)$ denotes the probability of the value x. The most significant digit or

first digit (FD) [19] for a positive integer Y can be computed as Equation (6).

$$FD(Y) = \lfloor Y/10\hat{}\lfloor \log\_10\ Y \rfloor \rfloor \quad (6)$$

where is the operation of floor rounding. Mean absolute deviation (MAD) [24] in fraud detection systems is a measure of conformity to Benford's law and is calculated using Equation (7).

$$MAD = (\sum\_(i = 1)\hat{}N \blacksquare |AP - EP|\ )/N \quad (7)$$

where EP is the probability predicted by Benford's law, AP is the actual first digit probability, and N represents the number of bins (which equals 9 for the first digits). The data with the least MAD has the closest conformity to Benford's law. Here, the calculated MAD values are used as distinguishing features. All of the DCT coefficients located in the same position of the 8×8 blocks form a mode [21]. In order to achieve better performance in using these features, 25 first AC modes are selected from the DCT coefficients for each block. First, the proposed method obtains histogram of first digits with 10 bins for each of the 25 first AC modes and then, computes the MAD value for each of them. Therefore, a vector with 25 features is extracted. Lastly, the final feature vector contains 75 (3×25) features for three channels.

3. 3. 2. Mantissa Distribution The mantissa distribution in image forensics was first introduced by Parnak et al. [25], which is a generalized form of Benford's law. This distribution is mentioned centrally by Kazemitabar and Kazemitabar [26] The logarithmic property that was found by Newcomb and elaborated by Hill, states that if you take the logarithm of a set of practical numbers the fractional part of the log values will be uniformly distributed [25].

Mantissa distribution is defined as: if x is a positive random variable, then Φ is a function that maps x to a new random variable and is defined as follows:

$$\Phi(x) = \ \llbracket log \rrbracket\_10\ x \quad mod\ 1 \quad (8)$$

$$\Phi(x)\ \sim uniform\ [0, 1) \quad (9)$$

where x is random variable, Φ is a function that maps x to a new variable, namely $\Phi(x)$ and mod denotes fractional part or mantissa of a number. If a dataset is presented to check whether it is valid or not, $\Phi(x)$ must be calculated for all information in the data set and compared to uniform [0, 1). If it fits well, it obeys the law and vice versa. DCT coefficients play a key role in using this theorem in the field of image forensics, like Benford's law. Experiments show that the mantissa distribution of DCT coefficients will have a uniform distribution from 0 to 1, while the mantissa distribution of other coefficients will have a non-uniform form. In order to achieve the features based on mantissa distribution, 25 first AC modes are selected from the DCT coefficients for each block. Then, histogram of the mantissa with 10 bins for each mode is calculated and finally, the 25 outputs obtained from these modes are arranged in a vector. The feature vector contains 750 (3×25×10) features for three channels.

3. 3. 3. Standard Deviation For a random variable vector x made up of N scalar observations, the standard deviation (STD) is the square root of the variance and is given in Equation (10).

$$s = \sqrt{}(1/(N - 1)\ \sum\_(i = 1)\hat{}N \blacksquare |x\_i - \bar{x}|\hat{}2\ ) \quad (10)$$

where $\bar{x}$ is the mean of x_i. The method computes the STD value for each of the 25 first AC coefficients obtained from the previous step. Therefore, a vector with 25 features is extracted. Finally, the final feature vector contains 75 (3×25) features for three channels.

3. 3. 4. Entropy Gonzalez [27] has mainly introduced Entropy's application in texture characterization in image processing. Entropy is a statistical measurement of variability and is defined as Equation (11).

$$e = -\sum_{i=0}^{L-1} p(z_i) \log_2 p(z_i) \quad (11)$$

where $p(z_i)$ is the probability of the gray-level z_i. In order to prepare the entropy features to detect forgery in the images, all 64 DCT coefficients are selected and entropy is applied for each block. So, the feature vector contains 192 (3×64) features according to three channels.

3. 3. 5. Final Feature Vector In this section, the output vectors obtained from previous step are combined to generate the final feature vector. This vector contains 1092 features.

3. 4. Classification Image tampering detection is a two-class classification problem (i.e., authentic and forged) and consequently, one of the most suitable classifiers for the problem is support vector machine (SVM). In the suggested approach, SVM with polynomial function with the first three degrees (i.e., linear, quadratic and cubic kernels) is employed for classification to detect authentic and tampered images based on the final feature vector.

4. EXPERIMENTAL RESULTS AND DISCUSSION

In this section, performance of the proposed method and the results of the experiments are evaluated. The method is implemented in MATLAB R2017b, on the Laptop with Intel Core i7 CPU 2.40 GHZ and 8 GB RAM.

4. 1. Datasets The method is tested with two different image datasets: CASIA V1.0 and CASIA V2.0 [28], which are publicly available. Table 1 summarized

adescription of the datasets. Some examples of the authentic and forged images from the datasets can be seen in Figure 2.

4. 2. Evaluation and Results In this work, support vector machine (SVM) is applied and tested with three types of kernel functions (i.e. linear, quadratic, and cubic) for classification to detect authentic and forged images based on the feature vectors. The images were randomly split to 70:30%, 5/6:1/6 and 80:20% train/test sets before training and testing algorithm. In order to protect against overfitting, the performance is evaluated using 10-fold cross-validation in terms of the evaluation parameters and for reliability improvement the average of the parameters was calculated during 10 times of running the algorithm.

For evaluation of the system, accuracy, sensitivity, and specificity measures are considered which are defined as:

$$Accuracy = (TP + TN)/(TP + FP + FN + TN) \quad (12)$$

$$Sensitivity\ (TPR) = TP/(TP + FN) \quad (13)$$

$$Specificity\ (TNR) = TN/(TN + FP) \quad (14)$$

where *TP* (true positive) is the number of forged images classified as forged, *FP* (false positive) is the number of forged images classified as authentic, *TN* (true negative) is the number of authentic images classified as authentic and *FN* (false negative) is the number of authentic images classified as forged images. Table 2 shows the performance results of different channels for the proposed features separately on CASIA V1.0 dataset. In this experiment, SVM classifier with linear kernel function and the data dividing at rate of 70:30% were considered. As can be seen in this table, the highest detection accuracy is related to the features based on mantissa distribution with a value equal to 99.76%, which indicates the high performance of them compared with other features. In terms of feature dimensions, the features based on MAD and STD in three channels have lower feature size than others.

Table 3 indicates the performance results of the proposed method based on the kernel functions on CASIA V1.0 database. 70% of the data is assigned to the training data and 30% of the data is assigned to the test data. The performance is evaluated using 10-fold cross-validation and 10 times of running the algorithm. As can be observed in the table, the highest mean accuracy, TPR and TNR are 99.94% (standard deviation, SD = 0.0918), 99.94% (SD = 0.1810) and 100% for SVM with quadratic kernel, respectively.

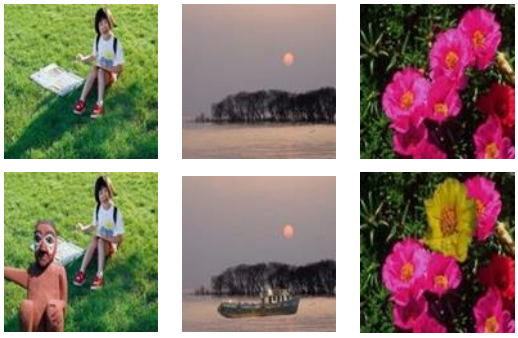

Figure 2. Some samples of images in the two utilized datasets (top row = Authentic , bottom row = Forged)

TABLE 1. Characteristics of the datasets

Dataset	Authentic	Forged	Size	Format
CASIA V1.0	800	921	384×256, 256×384	JPEG
CASIA V2.0	7491	5123	240×160, 900×600	TIFF,JPEG,BMP

TABLE 2. Performance results of different channels for the proposed features separately on CASIA V1.0

Feature	Channel	Accuracy (%)	TPR(%)	TNR (%)	Size
MAD	Y	96.70	95.64	97.97	25
	Cb	84.76	84.49	85.11	25
	Cr	88.44	89.51	87.26	25
	CbCr	90.95	91.73	90.07	50
	YCbCr	98.15	98.12	98.18	75
	Y	85.27	80.15	91.43	25
	Cb	90.71	85.00	97.29	25
	Cr	90.09	81.99	99.26	25
	CbCr	91.22	84.68	98.43	50
	YCbCr	93.27	96.71	89.19	75
Entropy	Y	98.60	97.68	99.66	250
	Cb	98.54	99.67	97.31	250
	Cr	99.16	99.64	98.61	250
	CbCr	98.93	99.77	98.01	500
	YCbCr	99.76	99.67	99.87	750
	Y	95.58	95.16	96.05	64
	Cb	91.37	90.98	91.86	64
	Cr	93.37	93.43	93.28	64
	CbCr	95.33	94.18	96.64	128
	YCbCr	98.43	98.11	98.81	192

Tables 4 and 5 summarized the performance results of the proposed method based on data splitting and the kernel functions on two common image splicing evaluation datasets. As can be seen in Table 4, the highest detection accuracies for the three divisions70:30%, 5/6:1/6, and 80:20% are 99.94%, 99.89% and99.85% for SVM with quadratic kernel, respectively. According to Table 5, the highest detection accuracies for the three divisions 70:30%, 5/6:1/6, and 80:20% are 99.84% for SVM with quadratic kernel, 99.79% for SVM with cubic kernel and 99.78% for SVM with cubic kernel, respectively. So, it can be found that the proposed method has a high detection capability in CASIA V2.0, which is a challenging database.

TABLE 3. Performance results of the proposed method based on the kernel functions on CASIA V1.0

kernel	Accuracy (%) (mean ± SD)	TPR (%) (mean ± SD)	TNR (%) (mean ± SD)
Linear	99.71 ± 0.1391	99.71 ± 0.2434	99.67 ± 0.2590
Quadratic	99.94 ± 0.0918	99.94 ± 0.1810	100 ± 0.0000
Cubic	99.88 ± 0.0981	99.88 ± 0.1810	99.87 ± 0.2559

TABLE 4. Performance results of the proposed method based on data splitting and the kernel functions on CASIA V1.0

	70:30			5/6:1/6			80:20		
Kernel	**Accuracy (%)**	**TPR (%)**	**TNR (%)**	**Accuracy (%)**	**TPR (%)**	**TNR (%)**	**Accuracy (%)**	**TPR (%)**	**TNR (%)**
Linear	99.71	99.74	99.67	99.72	99.60	99.84	99.76	99.62	99.93
Quadratic	99.94	99.88	100	99.89	99.80	100	99.85	99.83	99.87
Cubic	99.88	99.88	99.87	99.75	99.75	99.78	99.79	99.83	99.75

TABLE 5. Performance results of the proposed method based on data splitting and the kernel functions on CASIA V2.0

	70:30			5/6:1/6			80:20		
Kernel	**Accuracy (%)**	**TPR (%)**	**TNR (%)**	**Accuracy (%)**	**TPR (%)**	**TNR (%)**	**Accuracy (%)**	**TPR (%)**	**TNR (%)**
Linear	99.56	99.55	99.56	99.56	99.54	99.58	99.56	99.66	99.50
Quadratic	99.84	99.90	99.79	99.76	99.82	99.71	99.77	99.80	99.75
Cubic	99.79	99.86	99.74	99.79	99.86	99.74	99.78	99.80	99.76

TABLE 6. Comparison between the detection performances of the proposed method and state-of-the-art techniques

	CASIA V1.0			CASIA V2.0			
Method	Accuracy (%)	TPR (%)	TNR (%)	Accuracy (%)	TPR (%)	TNR (%)	Size
El-Latif et al. [4]	95.45	-	-	97.27	-	-	2048
Kasban and Nassar [5]	98.95	98.91	99.00	99.13	99.70	98.30	**32**
Fusheng and Gao [6]	99.24	99.40	99.09	97.56	-	-	676
Kaur and Gupta [7]	99.62	89.25	95.55	94.09	91.87	97.35	1024
Li et al. [8]	96.43	95.73	97.13	92.66	89.42	95.91	1452
Sheng et al. [9]	99.06	-	-	97.59	-	-	1452
Yıldırım and Ulutas [10]	99.29	99.45	99.95	99.58	98.61	**99.87**	1002
Muhammad et al. [11]	94.89	95.15	93.91	97.33	98.50	96.53	475
Agarwal and Chand [12]	95.41	97.65	93.16	98.33	99.22	97.73	2048
Alahmadi et al. [13]	97.00	96.75	98.24	97.50	98.45	96.84	-
Shen et al. [14]	98.54	97.48	99.51	97.73	97.72	97.80	96
Proposed(linear)	99.72	99.60	99.84	99.56	99.54	99.58	1092
Proposed(quadratic)	**99.89**	**99.80**	**100**	99.76	99.82	99.71	1092
Proposed(cubic)	99.75	99.75	99.78	**99.79**	**99.86**	99.74	1092

4. 3. Comparison with Other Methods In this section, the suggested approach is compared with various state-of-the-art methods. The performance is evaluated in terms of accuracy, TPR, TNR, and feature vector size. Table 6 shows a comparison of detection results in previous studies and this work on CASIA V1.0 and CASIA V2.0 datasets. The classifier used in these studies is support vector machine (SVM) and since most of them had used a proportion of 5/6 training and 1/6 testing images, the same proportion for the proposed method is considered in this comparison. As it can be observed, the proposed method with the detection accuracies of 99.72% and 99.82% for quadratic SVM and cubic SVM, respectively on CASIA V1.0 and the detection accuracies of 99.76% and 99.79% for quadratic SVM and cubic SVM, respectively on CASIA V2.0 overperform other works. The highest sensitivity belongs to the proposed method with 99.80% and 99.86% on CASIA V1.0 and CASIA V2.0 datasets, respectively. In addition, the method has the highest value of 100% specificity on CASIA V1 dataset and only has 0.13% less specificity than the method introduced by Yıldırım and Ulutaş [10] on CASIA V2.0 dataset. In terms of feature dimension, the proposed approach has lower feature dimension in compare with the methods discussed in literature [4, 8, 9, 12]. Table 6 summarized comparative analysis of the proposed method with the others stated methods.

4. 4. Training Time In this section, training time of the proposed approach is compared with the method introduced by Niyishaka and Bhagvati [29] on CASIA V2.0 database. This method [29] is the only recent method that has been reported the training time on CASIA V2.0. using various classifiers such as LR, SVM, KNN, LDA, Dtree and NB with data dividing at rate of 60:40% for classification. The training time of their method was 210 seconds for all combined classifiers and the highest accuracy rate of their method was 93.79% on 12614 images from CASIA V2.0 dataset, when feature vector size was 768. In order to make a fair comparison in this experiment, the images are split to 60:40% train/test sets and the performance of the proposed method is evaluated using 10-fold cross-validation and the average of the parameters is calculated during 10 times of running the algorithm. The results show the detection accuracy of 99.54% ± 0.1243 for linear SVM, 99.72% ± 0.0760 for quadratic SVM and 99.69% ± 0.068 for cubic SVM. Table 7 indicates a comparison of training time and feature vector size in method by Niyishaka and Bhagvati [29] and this work on CASIA V2.0 dataset. The reported training time of the proposed method is 36.35 ± 1.42 seconds for linear SVM, 34.07 ± 0.7326 seconds for quadratic SVM and 35.82 ± 0.9086 seconds for cubic SVM, which shows optimal performance of classification of the method compared to method by Niyishaka and Bhagvati [29]. Although as mentioned earlier, the reported training time for the method by Niyishaka and Bhagvati [29] is for all combined classifiers and the time spent on 10-fold cross-validation for safe classification and the larger feature vector size of the proposed method should be considered in the relative comparison.

4. 5. Misclassification Cases In some images from the databases, the proposed alghorithm failed and the images are misclassified (i.e. some forged images are classified as authentic and some authentic images are classified as forged). Figures 3 and 4 show examples of misclassified images from CASIA V2.0 database. The images shown in Figure 3 contain the following characteristics: JPG format, various sizes, small blurring regions, illumination variation, different texture pattern (such as regular and stochastic), same objects with scaling and rotation. The images shown in Figure 4 contain the following characteristics: TIFF format, various size, filtering small regions, blurred and smoothed edges, small forged regions same objects with scaling and rotation.

From the above characteristices, it can be seen that the proposed algorithm on the challenging dataset in some cases, is sensitive to very small forged regions,

TABLE.7. Comparison of training time and feature vector size in method by Niyishaka and Bhagvati [29] and this work on CASIA V2.0

Method	Training time (s) (mean ± SD)	Feature vector size
Niyishaka et al. [29]	210	768
Proposed (linear)	36.35 ± 1.4200	1092
Proposed (quadratic)	34.07 ± 0.7326	1092
Proposed (cubic)	35.82 ± 0.9086	1092

Figure 3. Examples of authentic images misclassified as forged images

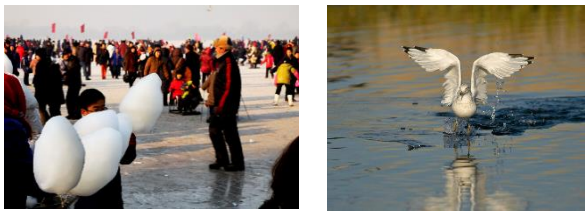

Figure 4. Examples of forged images misclassified as authentic images

blurred edges, regions containing copy-move forgery, compression and decompression of the images.

Our future works include the localization of the forgery in the image using segmentation fusion [30] and the variants of Benford's law and enriching the feature vector with other popular features like Zernike Moments [31]. In addition, other classifiers like Radial Basis Function (RBF) neural networks [32] can be applied to improve the classification accuracy.

5. CONCLUSION

This paper presents a novel forgery detection algorithm using combined features and SVM classifier. In the proposed method, features based on mantissa distribution (using generalized Benford's law), Mean Absolute Deviation (MAD) of traditional Benford's law, entropy and Standard Deviation (STD) are extracted and combined to construct the final feature vector. The method is evaluated on two common image datasets. The experimental results show the superiority of the suggested approach in comparison with previous works.

6. ACKNOWLEDGEMENT

The authors acknowledge the funding support provided by Babol Noshirvani University of Technology through Grant programs No. BNUT/370123/00. Authors also aknowledged the editor and anynomous reviewers for their constructive comments.

7. REFERENCES

1. Saadati, M., Vahidi, J., Seydi, V. and Sheikholharam Mashhadi, P.J.I.J.o.E., "Proposing a new image watermarking method using shearlet transform and whale optimization algorithm", ***International Journal of Engineering, Transactions A: Basics***, Vol. 34, No. 4, (2021), 843-853, doi: 10.5829/ije.2021.34.04a.10.
2. Nasiri, J.A. and Shakibian, H., "Probabilistic twin support vector machine for solving unclassifiable region problem", ***International Journal of Engineering, Transactions A: Basics***, Vol. 35, No. 1, (2022), 1-13, doi: 10.5829/ije.2022.35.01A.01.
3. da Costa, K.A., Papa, J.P., Passos, L.A., Colombo, D., Del Ser, J., Muhammad, K. and de Albuquerque, V.H.C.J.A.S.C., "A critical literature survey and prospects on tampering and anomaly detection in image data", ***Applied Soft Computing***, (2020), 106727, doi: 10.1016/j.asoc.2020.106727.
4. El-Latif, A., Eman, I., Taha, A., Zayed, H.H.J.A.J.f.S. and Engineering, "A passive approach for detecting image splicing based on deep learning and wavelet transform", ***Arabian Journal for Science & Engineering (Springer Science & Business Media BV)***, Vol. 45, No. 4, (2020), doi: 10.1007/s13369-020-04401-0.
5. Kasban, H. and Nassar, S.J.A.S.C., "An efficient approach for forgery detection in digital images using hilbert–huang transform", ***Applied Soft Computing***, Vol. 97, (2020), 106728, doi: 10.1016/j.asoc.2020.106728.
6. Fusheng, Y. and Gao, T., "A novel image splicing forensic algorithm based on generalized dct coefficient-pair histogram", in Chinese Conference on Image and Graphics Technologies, Springer. (2015), 63-71.
7. Kaur, M. and Gupta, S., "A passive blind approach for image splicing detection based on dwt and lbp histograms", in International Symposium on Security in Computing and Communication, Springer. (2016), 318-327.
8. Li, Y., Wang, X., Sun, S., Ma, X. and Lu, G.J.T.R.P.C.E.T., "Forecasting short-term subway passenger flow under special events scenarios using multiscale radial basis function networks", Vol. 77, (2017), 306-328, doi. https://doi.org/10.1016/j.trc.2017.02.005
9. Sheng, H., Shen, X., Lyu, Y., Shi, Z. and Ma, S.J.I.I.P., "Image splicing detection based on markov features in discrete octonion cosine transform domain", ***IET Image Processing***, Vol. 12, No. 10, (2018), 1815-1823, doi: 10.1049/iet-ipr.2017.1131.
10. Yıldırım, E.O. and Ulutaş, G.J.E.S.w.A., "Augmented features to detect image splicing on swt domain", ***Expert Systems with Applications***, Vol. 131, (2019), 81-93, doi: 10.1016/j.eswa.2019.04.036.
11. Bebis, G.J.M.V. and Applications, "Ghulam muhammad, munner h. Al-hammadi, muhammad hussain &", ***Machine Vision and Applications***, Vol. 25, (2014), 985-995, doi: 10.1007/s00138-013-0547-4.
12. Agarwal, S., Chand, S.J.I.j.o.i., graphics and processing, s., "Image forgery detection using multi scale entropy filter and local phase quantization", ***International Journal of Image, Graphics and Signal Processing***, Vol. 7, No. 10, (2015), 78, doi: 10.5815/ijigsp.2015.10.08.
13. Alahmadi, A., Hussain, M., Aboalsamh, H., Muhammad, G., Bebis, G. and Mathkour, H., "Passive detection of image forgery using dct and local binary pattern", ***Signal, Image and Video Processing***, Vol. 11, No. 1, (2017), 81-88, doi: 10.1007/s11760-016-0899-0.
14. Shen, X., Shi, Z. and Chen, H.J.I.I.P., "Splicing image forgery detection using textural features based on the grey level co-occurrence matrices", ***IET Image Processing***, Vol. 11, No. 1, (2017), 44-53, doi: 10.1049/iet-ipr.2016.0238.
15. Sharma, S. and Ghanekar, U.J.O., "A hybrid technique to discriminate natural images, computer generated graphics images, spliced, copy move tampered images and authentic images by using features and elm classifier", ***Optik***, Vol. 172, (2018), 470-483, doi: 10.1016/j.ijleo.2018.07.021.
16. Habibi, M. and Hassanpour, H.J.I.J.o.E., "Splicing image forgery detection and localization based on color edge inconsistency using statistical dispersion measures", ***International Journal of Engineering, Transactions B: Applications***, Vol. 34, No. 2, (2021), 443-451, doi: 10.5829/ije.2021.34.02b.16.
17. Singh, N. and Bansal, R., "Analysis of benford's law in digital image forensics", in 2015 International Conference on Signal Processing and Communication (ICSC), IEEE. (2015), 413-418.
18. Bonettini, N., Bestagini, P., Milani, S. and Tubaro, S., "On the use of benford's law to detect gan-generated images", in 2020 25th

International Conference on Pattern Recognition (ICPR), IEEE. (2021), 5495-5502.

19. Milani, S., Tagliasacchi, M., Tubaro, S.J.A.T.o.S. and Processing, I., "Discriminating multiple jpeg compressions using first digit features", ***APSIPA Transactions on Signal and Information Processing***, Vol. 3, (2014), doi: 10.1017/ATSIP.2014.19.
20. Li, B., Shi, Y.Q. and Huang, J., "Detecting doubly compressed jpeg images by using mode based first digit features", in 2008 IEEE 10th Workshop on Multimedia Signal Processing, IEEE. (2008), 730-735.
21. Li, X.H., Zhao, Y.Q., Liao, M., Shih, F.Y. and Shi, Y.Q.J.E.J.o.a.i.s.p., "Detection of tampered region for jpeg images by using mode-based first digit features", ***EURASIP Journal on Advances in Signal Processing***, Vol. 2012, No. 1, (2012), 1-10, doi: 10.1186/1687-6180-2012-190.
22. Alipour, N. and Behrad, A.J.T.J.o.E.E., "Forgery and double compression detection in digital images using combined features of quantization effects on dct coefficients", ***Tabriz Journal of Engineering Electrical***, Vol. 47, No. 2, (2017), doi.
23. Benford, F.J.P.o.t.A.p.s., "The law of anomalous numbers", ***Proceedings of the American Philosophical Society***, (1938), 551-572, doi.
24. Nigrini, M.J., "Benford's law: Applications for forensic accounting, auditing, and fraud detection, John Wiley & Sons, Vol. 586, (2012).
25. Parnak, A., Baleghi, Y. and Kazemitabar, J., "A novel forgery detection algorithm based on mantissa distribution in digital images", in 2020 6th Iranian Conference on Signal Processing and Intelligent Systems (ICSPIS), IEEE. (2020), 1-4.
26. Kazemitabar, J., Kazemitabar, J.J.C.i.S.-T. and Methods, "Measuring the conformity of distributions to benford's law", ***Communications in Statistics-Theory and Methods***, Vol. 49, No. 14, (2020), 3530-3536, doi: 10.1080/03610926.2019.1590599.
27. Gonzalez, R.C., Eddins, S.L. and Woods, R.E., "Digital image publishing using matlab, Prentice Hall, (2004).
28. Dong, J. and Wang, W., *Casia tampered image detection evaluation database*. 2011.
29. Niyishaka, P., Bhagvati, C.J.M.T. and Applications, "Image splicing detection technique based on illumination-reflectance model and lbp", ***Multimedia Tools and Applications***, Vol. 80, No. 2, (2021), 2161-2175, doi: 10.1007/s11042-020-09707-7.
30. Nikbakhsh, N., Baleghi Damavandi, Y. and Agahi, H.J.I.J.o.E., "Plant classification in images of natural scenes using segmentations fusion", ***International Journal of Engineering, Transactions C: Aspects***, Vol. 33, No. 9, (2020), 1743-1750, doi: 10.5829/IJE.2020.33.09C.07.
31. Dadgar, A., Baleghi, Y. and Ezoji, M.J.I.J.o.E., "Improved object matching in multi-objects tracking based on zernike moments and combination of multiple similarity metrics", ***International Journal of Engineering, Transactions C: Aspects***, Vol. 34, No. 6, (2021), 1445-1454, doi: 10.5829/IJE.2021.34.06C.08.
32. Asvadi, A., Karami-Mollaie, M., Baleghi, Y. and Seyyedi-Andi, H., "Improved object tracking using radial basis function neural networks", in 2011 7th Iranian Conference on Machine Vision and Image Processing, IEEE. (2011), 1-5.

Persian Abstract

چکیده

با توجه به سهولت دسترسی به بسترهایی که جاعلان می‌توانند اسناد دیجیتالی را دستکاری نمایند، ارائه ی ابزارهای خودکار برای شناسایی تصاویر جعلی در حال حاضر یک زمینه تحقیقاتی داغ در پردازش تصویر است. این مقاله یک الگوریتم جدید تشخیص جعل بر اساس ماهیت قانون بنفورد ارائه می‌دهد. در روش پیشنهادی، ویژگی‌های میانگین قدرمطلق انحراف با استفاده از قانون بنفورد معمولی و ویژگی‌های توزیع مانتیس با استفاده از قانون بنفورد تعمیم یافته استخراج می شوند. علاوه بر ویژگی‌های مبتنی بر قانون بنفورد، سایر ویژگی‌های آماری برای ساخت بردار ویژگی نهایی به کار گرفته شده است. در نهایت ماشین بردار پشتیبان با سه تابع هسته مختلف جهت طبقه‌بندی تصاویر اصلی و جعلی استفاده می‌شود. این روش روی دو پایگاه داده رایج CASIA V1.0 و CASIA V2.0 آزمایش شده است. نتایج تجربی نشان می‌دهد که به کمک روش پیشنهادی می‌توان به بهبود ۰/۲۷ درصدی روی پایگاه داده CASIA V1.0 و به بهبود ۰/۲۱ درصد روی پایگاه داده CASIA V2.0 در مقایسه با سایر روش‌های پیشرفته دست یافت. الگوریتم موثر پیشنهادی، پیاده‌سازی ساده‌ای دارد و با استفاده از تکنیک بکارگیری قانون بنفورد ارائه شده در این مقاله، می‌تواند ویژگی‌های غنی از تصاویر استخراج نماید تا فرآیند طبقه‌بندی به طور موثری توسط طبقه‌بند ساده‌ای مانند SVM در مدت زمان کوتاه انجام شود.