Expert Systems With Applications 164 (2021) 114014

Contents lists available at ScienceDirect

Expert Systems With Applications

journal homepage: www.elsevier.com/locate/eswa

DCT-phase statistics for forged IMEI numbers and air ticket detection

Lokesh Nandanwar [a], Palaiahnakote Shivakumara [a], Swati Kanchan [b], V. Basavaraja [c], D. S. Guru [c], Umapada Pal [b], Tong Lu [d,*], Michael Blumenstein [e]

[a] Faculty of Computer Science and Information Technology, University of Malaya, Malaysia
[b] Computer Vision and Pattern Recognition Unit, Indian Statistical Institute, Kolkata, India
[c] Department of Studies in Computer Science, University of Mysore, Karnataka, India
[d] National Key Lab for Novel Software Technology, Nanjing University, China
[e] University of Technology Sydney (UTS), Sydney, Australia

ARTICLE INFO

Keywords:
IMEI number
Phase spectrum
DCT coefficients
Forgery detection
Fraud document identification

ABSTRACT

New tools have been developing with the intention of having more flexibility and greater user-friendliness for editing the images and documents in digital technologies, but, unfortunately, they are also being used for manipulating and tampering information. Examples of such crimes include creating forged International Mobile Equipment Identity (IMEI) numbers which are embedded on mobile packages and inside smart mobile cases for illicit activities. Another example of such crimes is altering the name or date on air tickets for breaching security at the airport. This paper presents a new expert system for detecting forged IMEI numbers as well as altered air ticket images. The proposed method derives the phase spectrum using the Discrete Cosine Transform (DCT) to highlight the suspicious regions; it is unlike the phase spectrum from a Fourier transform, which is ineffective due to power spectrum noise. From the phase spectrum, our method extracts phase statistics to study the effect of distortions introduced by forgery operations. This results in feature vectors, which are fed to a Support Vector Machine (SVM) classifier for detection of forged IMEI numbers and air ticket images. Experimental results on our dataset of forged IMEI numbers (which is created by us for this work), on altered air tickets, on benchmark datasets of video caption text (which is tampered text), and on altered receipts of the ICPR 2018 FDC dataset, show that the proposed method is robust across different datasets. Furthermore, comparative studies of the proposed method with the existing methods on the same datasets show that the proposed method outperforms the existing methods. The dataset created will be available freely on request to the authors.

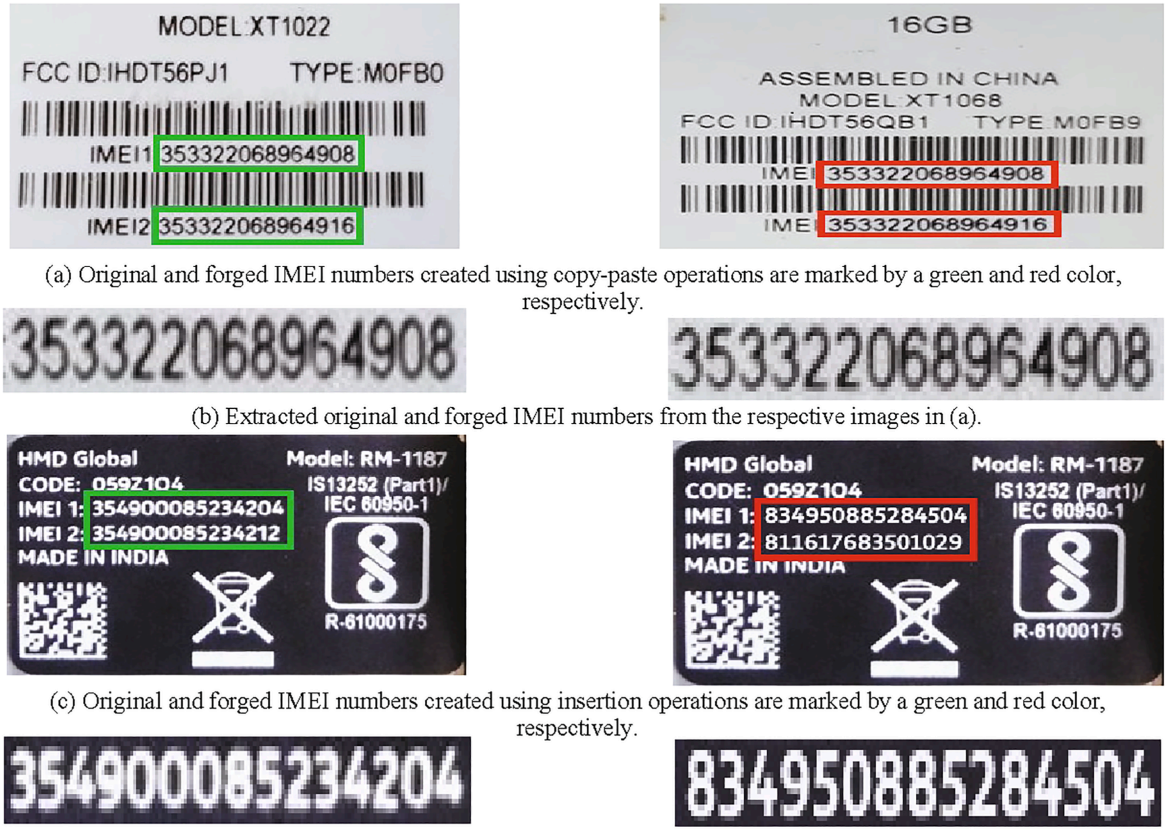
1. Introduction

With the advent of high quality, low cost, user-friendly image editing tools, digital data can be easily modified not only by trained professionals but also by the most common digital camera users (Hou & Lee, 2017). As a result, a person can severely distort the actual meaning of the images by tampering the content in the images (Chen et al., 2016; D'Amiano et al., 2018). Nowadays, it is very popular in the case of second-hand markets where people tamper of the actual content to sell items as new at a higher price (Hou & Lee, 2017). One such emerging crime is that of forging the International Mobile Equipment Identity (IMEI) numbers of smart phones for stealing and smuggling them illegally. Similarly, names and dates of air tickets are altered to enter airports by breaching security. These two issues are challenging and complex for forensic investigation. It is evident from the following links provided in the footnote on the first page that we can see in the news about the seriousness of the above-mentioned crimes. It can be noted from the links that there are smart and skilled people who can use powerful software tools for creating fake IMEI numbers and altered air tickets, which cannot be observed with the unaided eyes.

The reason to consider the above-two cases, namely, forged IMEI number detection and altered air ticket detection is that these two are sensitive applications relating to forensics and security, and hence they require urgent attention. It is noted that these applications are useful to society and are interesting topics for an expert system with applications. Furthermore, when we look at the complexity of the two issues, they are totally different because of the nature of the input images and the objective of the two cases. In the case of IMEI numbers, since the

[*] Corresponding author.
E-mail addresses: shiva@um.edu.my (P. Shivakumara), dsg@compsci.uni-mysore.ac.in (D.S. Guru), umapada@isical.ac.in (U. Pal), lutong@nju.edu.cn (T. Lu), michael.blumenstein@uts.edu.au (M. Blumenstein).

https://doi.org/10.1016/j.eswa.2020.114014
Received 21 February 2019; Received in revised form 25 August 2020; Accepted 13 September 2020
Available online 18 September 2020



(a) Original and forged IMEI numbers created using copy-paste operations are marked by a green and red color, respectively.

(b) Extracted original and forged IMEI numbers from the respective images in (a).

(c) Original and forged IMEI numbers created using insertion operations are marked by a green and red color, respectively.

(d) Extracted original and forged IMEI numbers from the respective images shown in (c).

Fig. 1. Examples of copy-paste and insertion operations for creating forged IMEI number images.

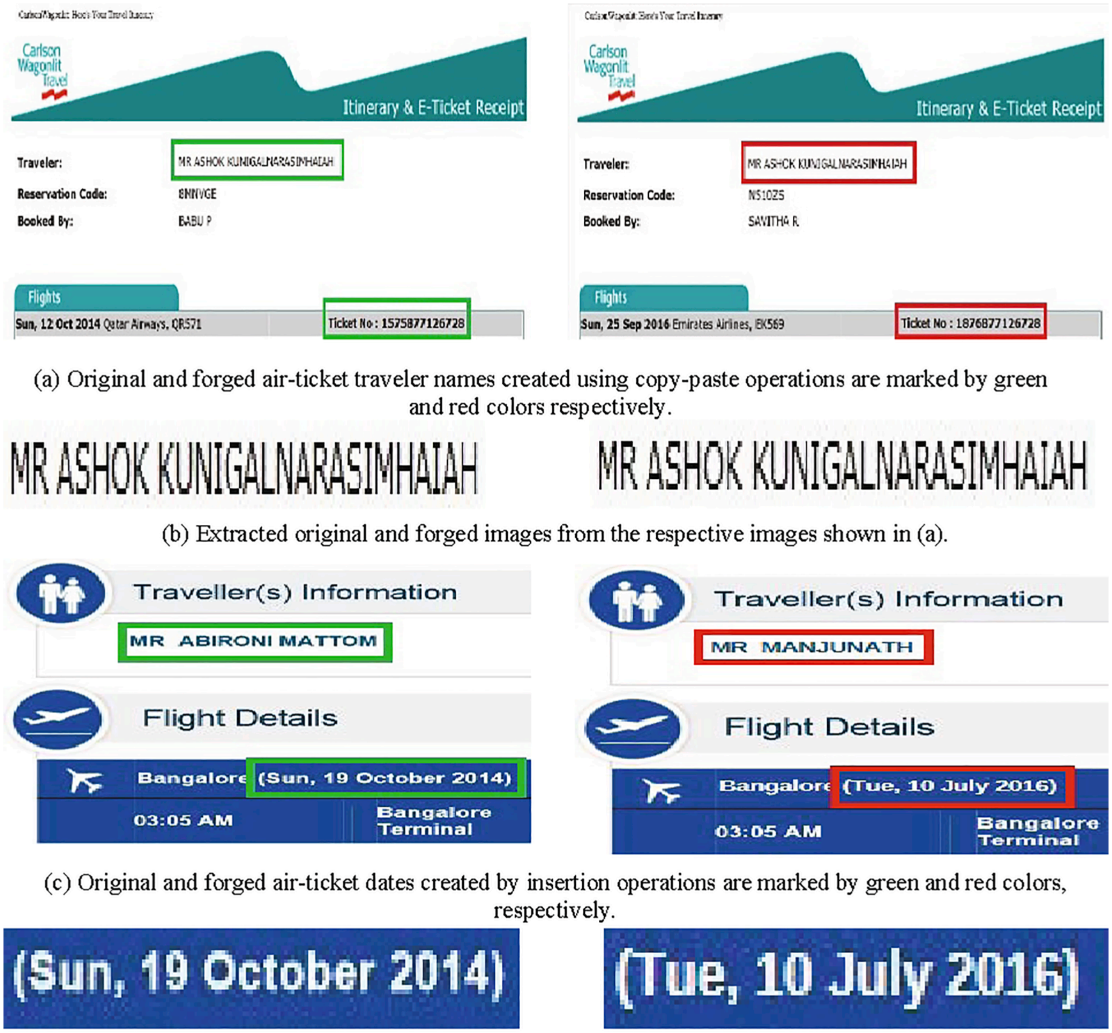
background is complex and it depends on the design of the mobile cases, it is not so easy to detect its forgery. Therefore, one can expect that a robust feature is required to handle the situation. This makes forged IMEI number detection more challenging. In the same way, in the case of an altered air ticket, since it is a document, we can expect a plain background in contrast to the complex background of IMEI images. Making forgeries of document images is easy compared to IMEI images. Therefore, the forgery operation may not introduce high variations or distortion as in IMEI images. This makes altered air ticket detection more challenging. Although the expectations are the same for the both issues, the degree of complexity is different. In other words, detecting forgeries is easy when the distortion created by a forgery operation is noticeable, while it is hard when the distortion is small. These two cases pose different challenges for forgery detection in images. Developing a method that can work for both cases is an open issue. In order to show the proposed method is robust to different situations (clutter and plain background images), and independent of the content of the input image, we consider two different cases in this work as case studies. Finding a solution to such a complex problem requires a new expert system, which illustrates a substantial difference compared to existing work.

Examples of fake IMEI numbers and air ticket information created using copy-paste and insertion operations are shown in Figs. 1 and 2, respectively. Copy-paste and insertions are standard operations for creating fake images (Chen et al., 2016; Feng et al., 2017; D'Amiano et al., 2018) in the realm of forgery. In the case of insertions, tools can be used to insert characters or numbers for creating forgeries. It is noted from Figs. 1 and 2 that the original IMEI numbers and air ticket information are marked by green rectangles, as shown in Figs. 1(a) and 2(a) on the left side, which are used to create forged IMEI and air ticket information, respectively. These forgeries are marked by a red rectangle as shown on the right-hand side. In Figs. 1 and 2, when we look at the extracted original and forged images shown in Figs. 1(b-d) and 2(b-d), it is hard to notice the difference between the original images and the forged ones without some knowledge of the forged information.

Hence, detecting forged IMEI numbers and altered air tickets is a challenging problem. There are many methods proposed in the literature for forging images and videos in different ways (Chen et al., 2016; Feng et al., 2017; D'Amiano et al., 2018), which use texture, color, gradient, blur artifacts, etc. However, the primary objective of the methods is to address the challenges of video and general images but not documents like forged IMEI and altered air tickets which require robust features. Similarly, we can find methods for spoof detection in the case of identifying biometrics for person identification (Kho et al., 2019), which are generally used for enhancing security systems. These methods focus on biometric information, such as fingerprints and face images but not IMEI numbers and air ticket images.

There are methods proposed for authenticating personal identity based on signature verification and identification (Behera et al., 2018; Bouamra et al., 2018; Sharma & Sundaram, 2018). The methods are able to identify forged and genuine signatures based on misalignment caused by forgery operations. However, the scope of the method does not cover forged IMEI numbers and altered air ticket images because these methods are limited to handwriting text and online writing information. Similar to the proposed work, there are methods for tampered text detection from video images (Shivakumara et al., 2014; Xu et al., 2014; Bhardwaj & Pankajakshan, 2016; Roy et al., 2016), which focus on text properties to identify forged text, that is, edited text and scene text, which is considered as natural text in the video. In other words, the methods differentiate caption and scene text in video images based on text properties. However, these methods work well when the whole word or text line gets affected by forgery operations.

It is also noted from the literature (Gupta et al., 2016; Yue et al., 2019) that methods have been developed for generating artificial synthetic scene characters and text images using source information, which



Carlson Wagonlit Travel

Itinerary & E-Ticket Receipt

Traveler: MR ASHOK KUNIGALNARASIMHAIAH

Reservation Code: 8MNVGE

Booked By: BABU P

Flights

Sun, 12 Oct 2014 Qatar Airways, QR571 Ticket No : 1575877126728

Carlson Wagonlit Travel

Itinerary & E-Ticket Receipt

Traveler: MR ASHOK KUNIGALNARASIMHAIAH

Reservation Code: NS10Z5

Booked By: SAVITHA R

Flights

Sun, 25 Sep 2016 Emirates Airlines, EK569 Ticket No : 1876877126728

(a) Original and forged air-ticket traveler names created using copy-paste operations are marked by green and red colors respectively.

MR ASHOK KUNIGALNARASIMHAIAH MR ASHOK KUNIGALNARASIMHAIAH

(b) Extracted original and forged images from the respective images shown in (a).

Traveller(s) Information

MR ABIRONI MATTOM

Flight Details

Bangalore (Sun, 19 October 2014)

03:05 AM Bangalore Terminal

Traveller(s) Information

MR MANJUNATH

Flight Details

Bangalore (Tue, 10 July 2016)

03:05 AM Bangalore Terminal

(c) Original and forged air-ticket dates created by insertion operations are marked by green and red colors, respectively.

(Sun, 19 October 2014) (Tue, 10 July 2016)

(d) Extracted original and forged Air-ticket dates from the respective images shown in (c).

Fig. 2. Example of copy-paste and insertion operations for creating forged air ticket images.

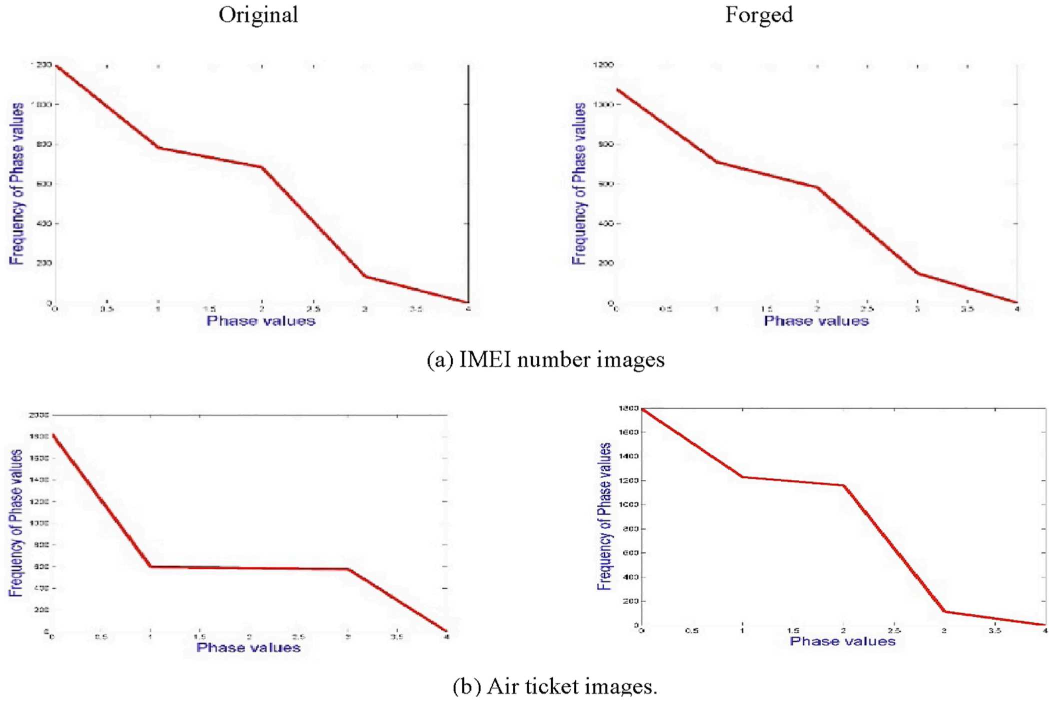
can be used for improving recognition performance. Since the objective of the methods is to generate text which is similar to the source image, the generated text may not be the same as the source images. As a result, the generated text can be an entirely different image from the original. Therefore, these methods may not be appropriate for forged IMEI number and altered air ticket detection because forged text appears exactly the same way as in the original images with some alterations. Hence, the problem is challenging and unsolved, and there is an urgent need for developing an effective and robust approach.

The organization of the rest of the paper is as follows. Section 2 discusses background of the proposed work. This section also reviews the existing methods of forgery detection in imagery and document images to highlight the state-of-the-art and challenges, which have been addressed or not addressed so far. In Section 3, the details of the proposed method for solving the problem of forgery detection in the images are presented. Furthermore, the proposed method is divided into two sub-sections. The process for obtaining the phase spectrum using DCT and the Fourier transform is presented in sub-section 3.1. The phase statistics are defined in sub-section 3.2. The results to validate the proposed method are presented in Section 4. Finally, conclusions and future work are discussed in Section 5.

2. Background

Since the proposed work is relevant to document analysis and there is no particular method available for forged IMEI number and altered air ticket detection, we consider the methods which have been developed for fake or fraudulent document identification and tampered text detection in video images for reviewing here.

Elkasrawi and Shafait (2014) proposed printer source identification using supervised learning for document forgery detection. This approach explores printer parts based on noise generated by different printers for fraud document classification. Ahmed and Shafait (2014) proposed forgery detection based on intrinsic document contents. This method employs a similarity between blocks of an image to identify forged documents. Khan et al. (2015) proposed automatic ink mismatch detection for forensic document analysis. This method analyzes the ink of different pens to find fraudulent documents. Luo et al. (2015) proposed localized forgery detection in hyperspectral document images. This is an improved version of the above method, which applies ink quality under hyperspectral conditions for fraudulent document identification. Bertrand et al. (2013) proposed a system based on intrinsic features for fraudulent document detection. This approach extracts features or characters to match with the ground truth for fraud estimation. Based on mismatch scores, the method identifies fraudulent documents. da Silva Barboza et al. (2013) proposed a color-based model



(a) IMEI number images

(b) Air ticket images.

Fig. 3. Fourier Phase for IMEI number and air ticket images.

to determine document ages for forensic purposes. This approach uses the ink quality of handwritten document images captured at different intervals of time. The method in da Silva Barboza et al. (2013) helps us to identify a given image whether it is old or new. Halder and Garain (2010) proposed a color features-based approach for determining ink ages in printed documents. This method uses similar ones to the above-mentioned color features for printed text images. Recently, (Wang et al., 2017) proposed Fourier-residuals for printer identification. This method extracts features from the residual given by Fourier transforms for the identification of source printers.

It is observed from the above review of the methods on forged/fraudulent document identification that most methods focus on text with plain background images for forgery detection. Furthermore, the methods use colors or strokes of character components and distortions produced by different printers for forgery detection. However, these features may not work well for clutter background images, such as IMEI numbers and degraded air tickets due to aging and quality of the paper.

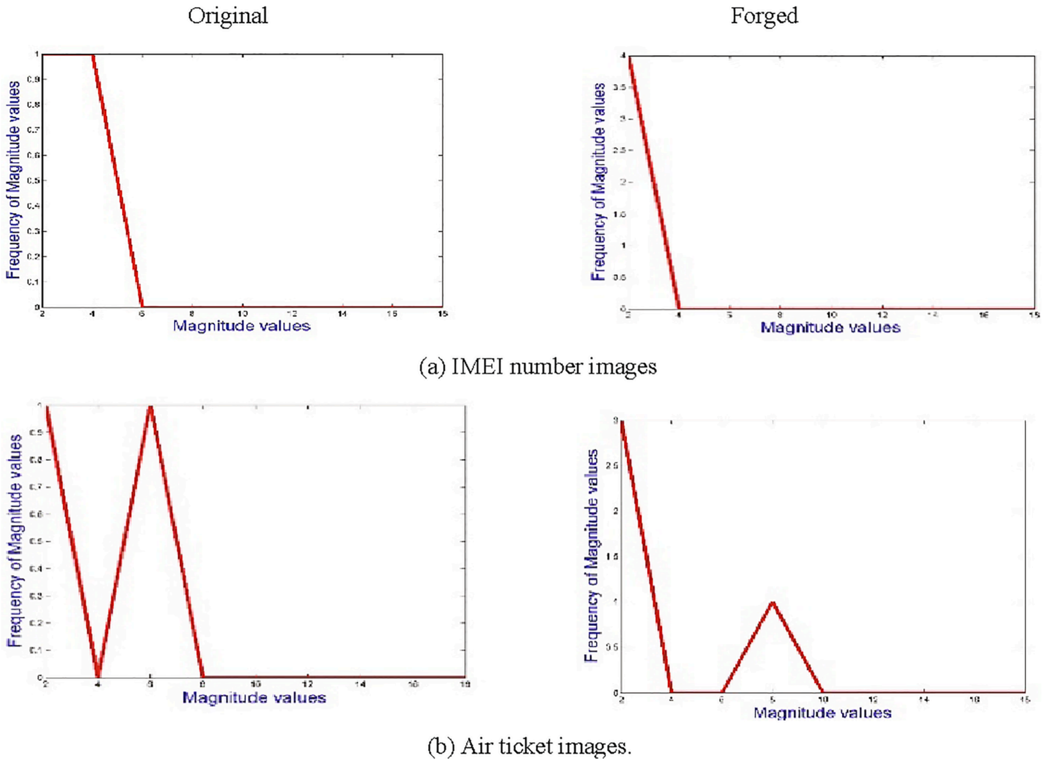
To overcome the problems of complex backgrounds, a few methods have been developed for caption text (which is edited text on video) detection in video, hence caption text is considered as tampered text (forged text) in the video. Shivakumara et al. (2014) proposed the separation of graphics and scene texts in the video. This method works based on the fact that caption text has high contrast and clarity, while scene text does not. Xu et al. (2014) proposed graphics and scene text classification in the video. This method uses the above basis for extracting distinct features through the distribution of Eigen values. Roy et al. (2016) proposed new tampered features for scene and caption text classification in video frames. This method uses DCT coefficients to differentiate caption texts from those in scenes. Bhardwaj and Pankajakshan (2016) proposed image overlay text detection based on JPEG truncation error analysis. This method extracts tampered features through truncation errors given by a color filter array for detecting caption texts in the video. However, the above methods are inadequate for forged IMEI number and altered air ticket detection because the methods require the whole tampered word or text line with good clarity.

In light of the above discussion, it is noted that none of the methods address the issue caused by IMEI numbers and text in air ticket document images, where one can expect a relatively small effect by copy-paste and insertion operations compared to forged printed and video texts. Most methods are developed based on specific properties of the text or the document. In addition, since forged texts in a plain background document images, manipulating the text is easy without introducing distortion. Therefore, it is much more difficult compared to forged IMEI number detection. Developing a single method which can deal with the above challenges is still hard. However, there has been an attempt to solve the problem of forged IMEI number detection, which uses RGB colors and a fusion method for forgery detection (Shivakumara et al., 2018). The scope of the method is limited to forged IMEI number detection but does not include altered air ticket detection as in the proposed work. Besides, the approach used in the methods is different from the proposed method. Furthermore, since the aforementioned method uses heuristics for detecting forgeries, it is not robust and accurate for large and different datasets. These factors motivated us to explore a novel method in the frequency domain for detecting forged IMEI numbers and altered air ticket detection in this work.

Hence, in this work, we propose a novel method that combines the Discrete Cosine Transform (DCT) and Fourier Transform (FT) to obtain the phase spectrum for IMEI numbers and air ticket images. The proposed method extracts phase-statistics for the phase-spectrum given by the combination of features. The features are fed to an SVM classifier for detecting forgeries in IMEI numbers and altered air ticket images. The way the proposed method uses DCT and FT coefficients along with the phase statistics for finding solutions to forgeries is new, and the key contribution in this work. Furthermore, releasing our dataset to the public is one more contribution, as it helps to set an evaluation benchmark.

3. Proposed method

Since there are many methods for segmenting text from document images, and natural scene images (Shivakumara et al., 2014; Xu et al., 2014; Bhardwaj & Pankajakshan, 2016; Roy et al., 2016), we use the same method for segmenting IMEI number and altered air ticket information. For this work, segmented IMEI numbers and air ticket names, dates are used as inputs. When we perform copy-paste and insertion operations in a document, the process introduces distortions at the pixel



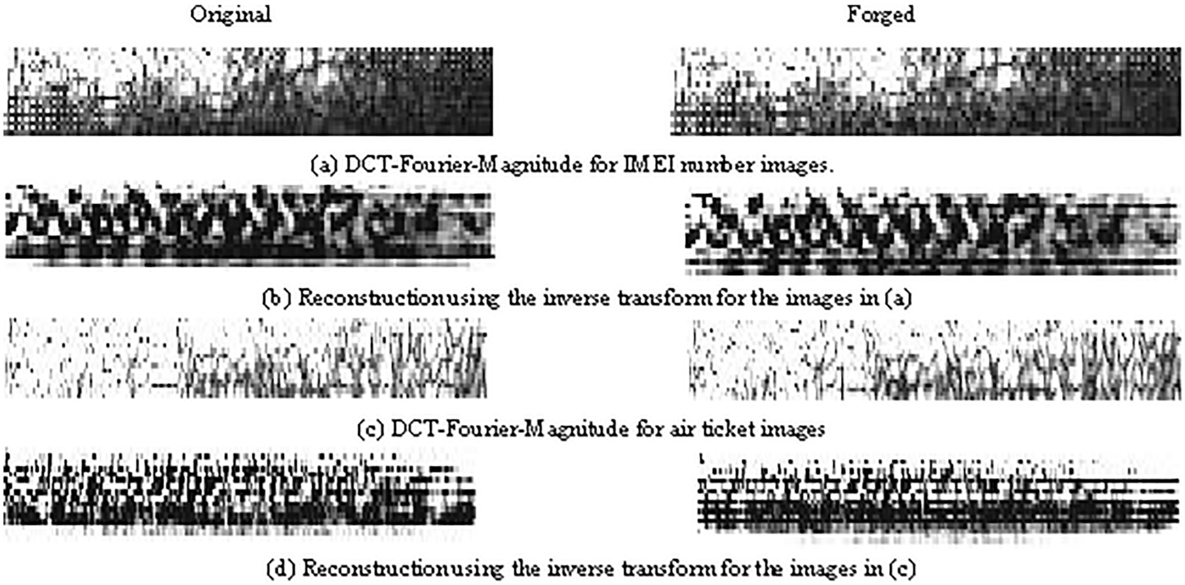
(a) IMEI number images

(b) Air ticket images.

Fig. 4. DCT Magnitude for IMEI numbers and air ticket images.

level, which may not be seen by the unaided eye (Chen et al., 2016; Feng et al., 2017; D'Amiano et al., 2018). This is the main basis for forgery detection. This is true for forgery detection in general images, videos and documents. However, the distortion effect at the pixel level might be high in the case of general images/video/documents while for IMEIs and air tickets it should be small. This is due to the advantage of editing PDF documents and a limited amount of information with less variations and a simple background. To extract such minute changes in forged images, we are inspired by the method (Kumari & Shekar, 2011) where it is noted that frequency-based features are more sensitive than spatial domain-based features. This leads to the exploration of the Discrete Cosine Transform (DCT) for the purpose of forgery detection in this work. However, DCT does not provide a complex transform like the Fourier Transform (FT). As noted, the phase-spectrum has the ability to provide fine details for edges in images irrespective of contrast variations compared to the magnitude (Kumari & Shekar, 2011).

However, the phase-spectrum given by FT alone is not effective because of the power spectrum, which does not consider time variations of phase and magnitude, hence noise cannot be removed from the phase-spectrum (Park & Joh, 2009). It is evident from Fig. 3(a) and (b), where it is noted that there are small differences between the phase histogram of the original and forged IMEI numbers, and altered air ticket images. Similarly, the same conclusion can be drawn from Fig. 4(a) and (b), where DCT-magnitude histograms are shown for the original and forged



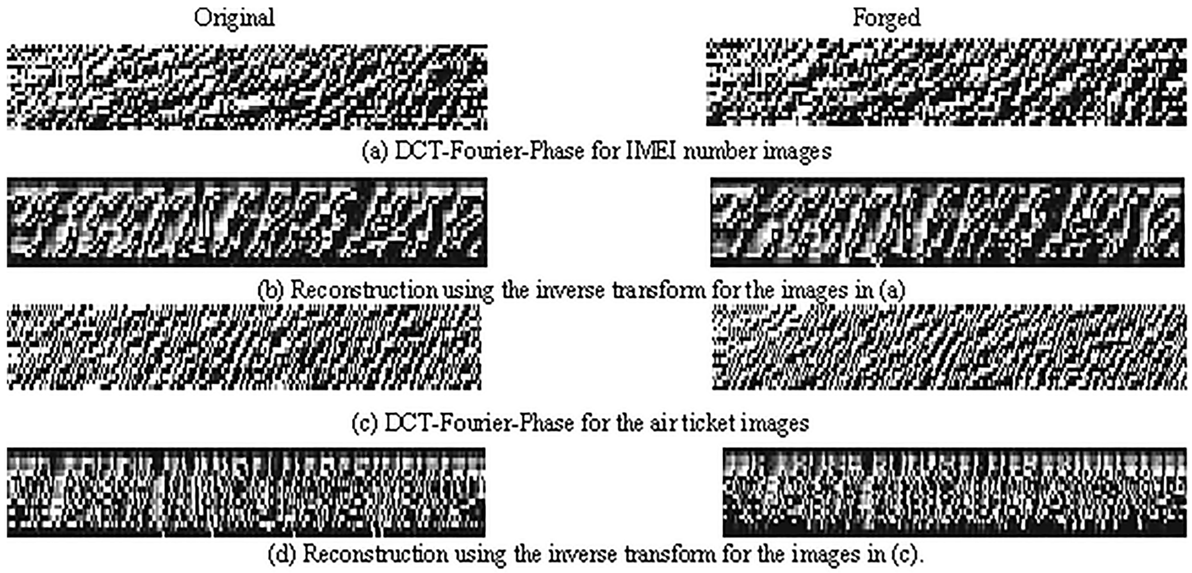
(a) DCT-Fourier-Magnitude for IMEI number images.

(b) Reconstructionusing the inverse transform for the images in (a)

(c) DCT-Fourier-Magnitude for air ticket images

(d) Reconstructionusing the inverse transform for the images in (c)

Fig. 5. DCT-Fourier-Magnitude and the respective reconstructed images for IMEI and Air ticket images.



(a) DCT-Fourier-Phase for IMEI number images

(b) Reconstruction using the inverse transform for the images in (a)

(c) DCT-Fourier-Phase for the air ticket images

(d) Reconstruction using the inverse transform for the images in (c).

Fig. 6. DCT-Fourier-Phase images and the respective reconstructed images for IMEI and air ticket images.

IMEI numbers and air ticket images. But the small differences given by Fourier-phase and DCT-magnitude can be magnified by integrating DCT and Fourier-phase for forgery detection. This motivated us to combine DCT and FT to generate the phase-spectrum in a new way in this work.

It is noted from Fig. 3 that the phase-spectrum obtained by the combination of DCT and FT provides clues for discriminating the original and forged images. To extract such a difference from the phase-spectrum, we propose to extract phase-statistics to form feature vectors (Salwa & Mohammed, 2017). Since phase is circular data, we propose circular statistics, namely, the circular mean which describes where the center of the data is, and circular variance, which describes how the data is spread around the center. Due to the complexity of the problem, sometimes, one can expect that different distributions may share the same mean and variance. To overcome this issue, the proposed method extracts higher-order statistics, namely, circular skewness and circular kurtosis, which describe how the shape of the distribution is. In this way, the proposed method extracts the above-mentioned four features from the input image. Then the feature vector is applied to an SVM classifier for detecting forged IMEI numbers and altered air ticket images. In this work, we prefer to use well-known and simple SVM classifiers for forgery detection because our intention is to make a contribution at the feature extraction level. Detailed steps of obtaining the phase spectrum and the extraction of phase statistics will be presented in subsequent sections.

3.1. Phase spectrum for DCT

We derive the equations for obtaining the phase-spectrum using DCT and Fourier operations for input IMEI number and air ticket images as defined in Eqs. (1)–(8). For each input image, the proposed method obtains the DCT-Fourier-Magnitude and DCT-Fourier-Phase spectrum as shown in Figs. 5(a-d) and 6(a-d) for IMEI number and air ticket images, respectively. It is observed from reconstructed images for the IMEI number and air ticket images in Figs. 5(b-d) and 6(b-d), the DCT-Fourier-Phase spectrum provides significant details compared to DCT-Fourier-Magnitude. Therefore, this shows that the phase-spectrum given the DCT-Fourier combination is effective compared to the DCT-Fourier-Magnitude for forgery detection in IMEI number and air ticket images.

Let f be an input image of size $p \times q$. Then DCT can be obtained for $f_{p\times q}$as follows:

$$F_{cc}(u,v) = C_1C_2\sum_{m=1}^{p}\sum_{n=1}^{q} f(m,n)cos\left[\frac{\pi u}{p}(m+0.5)\right]cos\left[\frac{\pi v}{q}(n+0.5)\right] \quad (1)$$

$$F_{cs}(u,v) = C_1C_2\sum_{m=1}^{p}\sum_{n=1}^{q} f(m,n)cos\left[\frac{\pi u}{p}(m+0.5)\right]sin\left[\frac{\pi v}{q}(n+0.5)\right] \quad (2)$$

$$F_{sc}(u,v) = C_1C_2\sum_{m=1}^{p}\sum_{n=1}^{q} f(m,n)sin\left[\frac{\pi u}{p}(m+0.5)\right]cos\left[\frac{\pi v}{q}(n+0.5)\right] \quad (3)$$

$$F_{ss}(u,v) = C_1C_2\sum_{m=1}^{p}\sum_{n=1}^{q} f(m,n)sin\left[\frac{\pi u}{p}(m+0.5)\right]sin\left[\frac{\pi v}{q}(n+0.5)\right] \quad (4)$$

where, $1 \le u \le p$ *and* $1 \le v \le q$

C_1 and C_2 are the constants and are defined as follows:

$$C_i = \begin{cases} \sqrt{\frac{2}{p}} if 2 \le u \le p & \\ & i = 1,2. \\ \sqrt{\frac{1}{p}} if u = 1 & \end{cases} \quad (5)$$

By combining the above four real transforms as:

$$\{F_{cc}(u,v) - F_{ss}(u,v)\} - j\{F_{cs}(u,v) - F_{sc}(u,v)\}$$

The complex transform for DCT is obtained as:

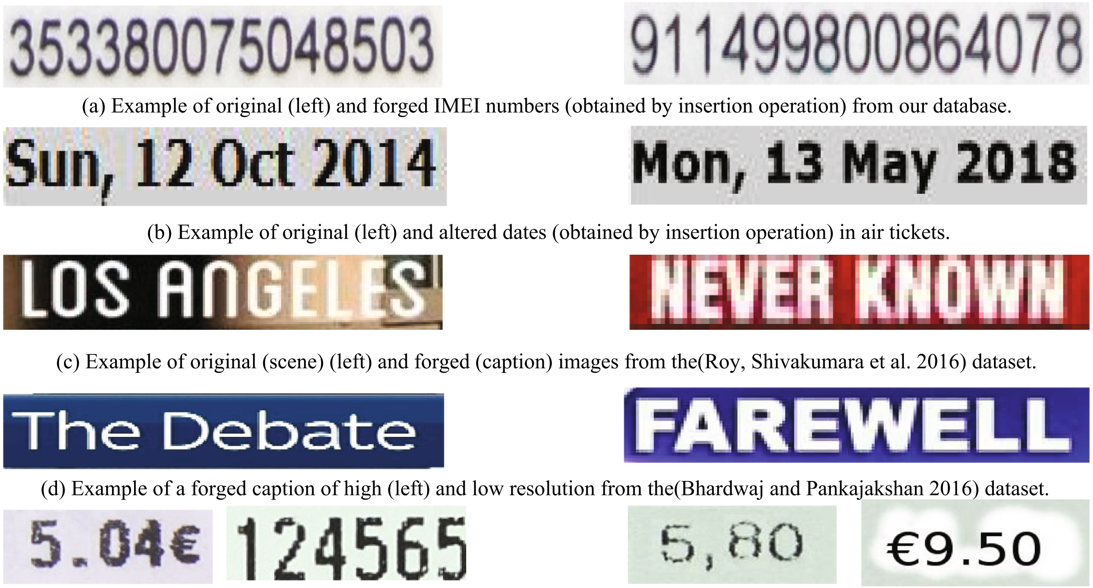
$$F(u,v) = C_1C_2\sum_{m=1}^{p}\sum_{n=1}^{q} f(m,n)e^{-j\frac{\pi u}{p}(m+0.5)}e^{-j\frac{\pi v}{q}(n+0.5)} \quad (6)$$

Eq. (6) is used for obtaining the magnitude and phase-spectrum as defined in Eqs. (7) and (8), respectively.

$$M = |F(u,v)| = \sqrt{F_r(u,v)^2 + F_i(u,v)^2} \quad (7)$$

where F_r is the real part and F_i is the imaginary part of F. The phase information is given by:

$$\theta = \angle F(u,v)| = arctan\frac{F_i(u,v)}{F_r(u,v)} \quad (8)$$



(a) Example of original (left) and forged IMEI numbers (obtained by insertion operation) from our database.

(b) Example of original (left) and altered dates (obtained by insertion operation) in air tickets.

(c) Example of original (scene) (left) and forged (caption) images from the(Roy, Shivakumara et al. 2016) dataset.

(d) Example of a forged caption of high (left) and low resolution from the(Bhardwaj and Pankajakshan 2016) dataset.

(e) Example of original (left) and forged prices chosen from the standard dataset of ICPR 2018 FDC (Artaud et al., 2018)

Fig. 7. Examples of original and forged images chosen from ours and benchmark datasets.

3.2. *Phase-Statistics for forged IMEI number and air ticket detection*

For the phase-spectrum, given by the previous step, the proposed method computes the phase-statistics as defined in Eqs. (9)–(15), which give four phase statistical features considered as the feature vector for detecting forged IMEI numbers and altered air ticket images.

Circular Mean (CM): Let θ ($\theta_1, \theta_2, \ldots, \theta_n$) be phase data defined on a circle. To compute the circular mean, it is necessary to change the coordinate system to a rectangular one as:

$$\overline{X} = \frac{\sum_{i=1}^{n} \cos\theta_i}{n}\overline{Y} = \frac{\sum_{i=1}^{n} \sin\theta_i}{n} \tag{9}$$

This allows the computation of the resultant vector as defined in Eq. (10).

$$r = \sqrt{\overline{X}^2 + \overline{Y}^2} \tag{10}$$

The direction of the resultant vector is defined as in Eq. (11).

$$\cos\overline{\theta} = \frac{\overline{X}}{r}\sin\overline{\theta} = \frac{\overline{Y}}{r} \tag{11}$$

where $\overline{\theta}$ denotes the circular mean. Then the phase-spectrum can be obtained as defined in Eq. (12) by an inverse tangent.

$$M = \overline{\theta} = \arctan\left(\frac{sin\overline{\theta}}{cos\overline{\theta}}\right) \tag{12}$$

Circular Variance (CV): This feature is established to describe the distribution of data around the mean. The variance is computed as defined in Eq. (13).

$$V = 1 - r \tag{13}$$

If CV is near to zero, then it indicates that the angles are in the same direction, and if CV is near to 1, it indicates the angles spread around the circle.

Circular Skewness (CS): Circular skewness provides information about the shape and symmetry of phase data, and it can be calculated as defined in Eq. (14).

$$S = \frac{1}{n}\sum_{i}^{n} sin2(\theta_i - \overline{\theta}) \tag{14}$$

When CS is zero, there is no skew in the phase data, which means the phase data is symmetric around CM. If CS is negative, this indicates the tail of the distribution is skewed to the left. Conversely, if CS is positive, the tail is skewed to the right.

Circular Kurtosis (CK): Indicates how tall and sharp the peak is in the phase data distribution. In other words, it is a measure of the ultimate peak and can be calculated as defined in Eq. (15).

$$K = \frac{1}{n}\sum_{i}^{n} cos2(\theta_i - \overline{\theta}) \tag{15}$$

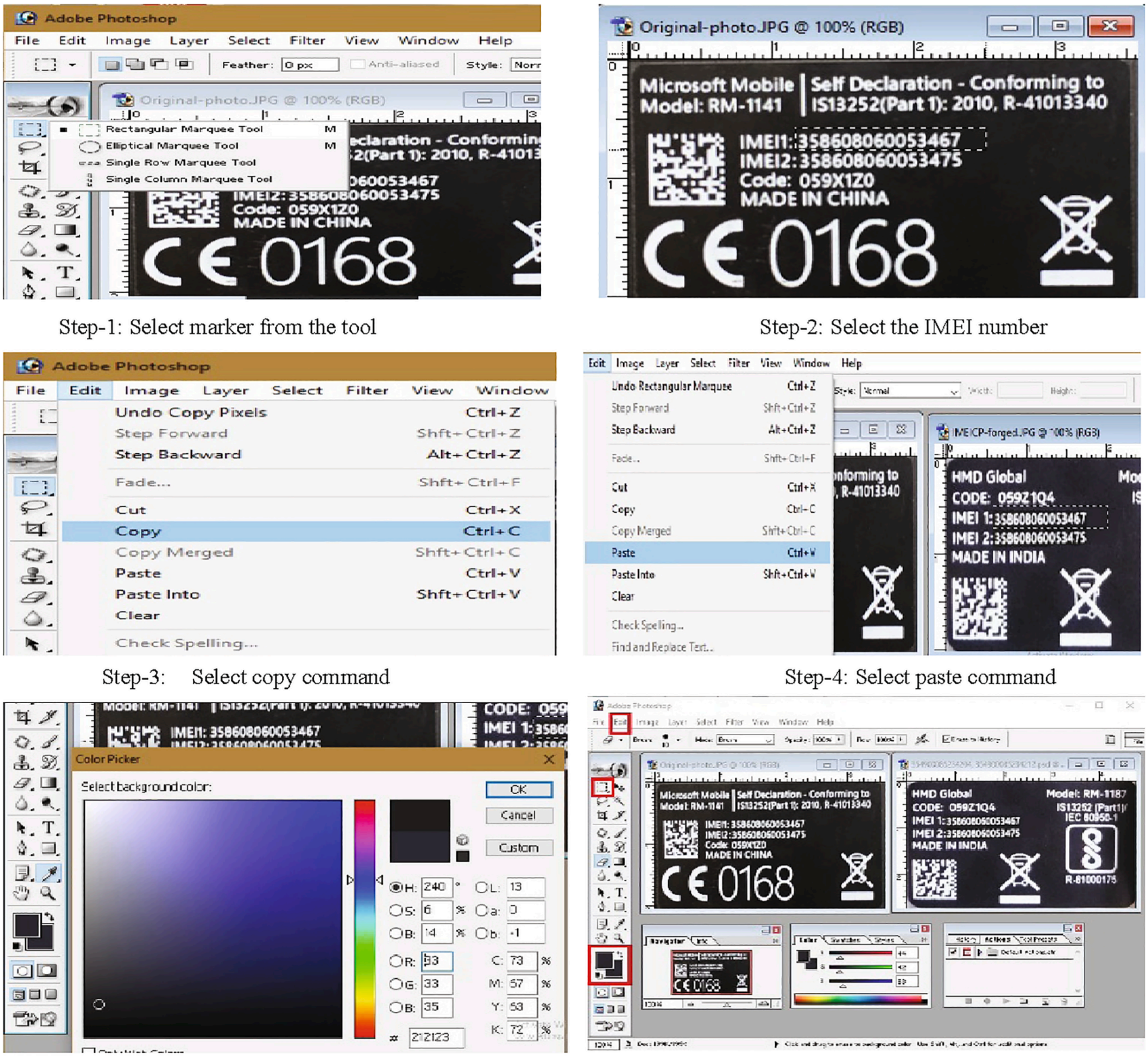
A large positive CK shows a peaked distribution.

The above extracted features are fed to the well-known SVM classifier with RBF kernel and default parameter values for forged IMEI and altered air ticket detection. The dataset is divided into the training of 75% images and testing of 25% for experimentation in this work. The values of the different parameters are determined automatically based on training samples for the detection of forged IMEI numbers and altered air tickets.

4. Experimental results

There is no benchmark dataset for evaluating the proposed method for forged IMEI number and altered air ticket detection. We created our own dataset for experimentation in this work, which includes 1000 images for the IMEI number and 1000 images for altered air tickets. Each dataset comprises two classes, namely, the original class which contains genuine images without being affected by forgery operation, and a forged class which contains the same number of tampered (forged) images. Since each class of two datasets consists of 500 images, it gives a total of 2000 images for experimentation in this work. For creating forged images, we used standard operations, namely, copy-paste and insertion. Sample images of the original, together with forged IMEI numbers and altered air tickets created by copy-paste and insertion operations, are shown in Fig. 7(a) and (b), respectively. It is noted from Fig. 7(a) and (b) that it is hard to observe the differences between the original and forged images.

Since the above-mentioned dataset is created artificially, to show a fair evaluation of the proposed method for forged IMEI number detection, we consider the standard dataset of caption and scene texts classification in videos (Roy et al., 2016). This is because the caption text in



Step-1: Select marker from the tool

Step-2: Select the IMEI number

Step-3: Select copy command

Step-4: Select paste command

Step-5: Select the color panel to change the foreground and background color, resulting in a forged image with the copy-paste operation.

Fig.8. Different steps for creating forged IMEI number images using the Photoshop tool.

the video is edited text and hence it can be considered as actual forged text such as forged IMEI numbers. Similarly, since the scene text in the video is part of the image and is natural text, it can be considered as original text like the original IMEI number. With the same notion of forged text detection, we consider one more standard dataset due to (Bhardwaj & Pankajakshan, 2016) for evaluation. (Roy et al., 2016)'s dataset provides 500 images for each class, while Bhardwaj's dataset provides 150 images with low resolution (1280 × 720 pixels), and 150 images with high resolution (1920 × 1080 pixels). In total, 1300 images are considered for experimentation in this work. The sample caption and scene text images of (Bhardwaj & Pankajakshan, 2016; Roy et al., 2016) datasets are shown in Fig. 7(c) and (d), respectively.

In the same way of choosing a standard dataset for forged IMEI number detection and for altered air ticket detection, we consider a standard dataset of altered prices listed on receipts for evaluation, which is called the ICPR 2018 Fraud Detection Contest (FDC) (Artaud et al., 2018). The altered prices are the same as altered date and names on an air ticket and therefore, the images are considered as actual forged images, and the prices that are not affected by the forgery operation are considered as the original class. The dataset provides 301 altered samples extracted from the ground truth given in the dataset, and we select 527 original (unaltered) samples, which gives a total of 828 images for experimentation. Samples of altered and original images are shown in Fig. 7(e) where we can see a plain background as in air ticket images.

To show the effectiveness of the proposed method, we implement the following methods for comparative purposes: (Roy et al., 2016) which employs tampered features for caption and scene text detection from video, Bhardwaj's method (Bhardwaj & Pankajakshan, 2016), which uses compression error in the compressed domain for detecting caption texts in video images, and the method in (Elkasrawi & Shafait, 2014), which uses noise introduced by different printers for source printer identification. The image noise generated by a printer is the same as those introduced by tampering operations in forged air ticket detection. The method in (Wang et al., 2017), which explores the Fourier residual for printer identification on the same basis as the above-mentioned approach, is also included. Shivakumara et al. (2018) proposed a method for forged IMEI number detection based on RGB color spaces and the connected component-based features. Since the scope of this method is limited to forged IMEI number detection, the features

Table 1
Studying the effectiveness of key steps for forged IMEI number and altered Air ticket detection.

Steps	IMEI Number Dataset						Air Ticket Dataset					
	Original			Forged			Original			Forged		
	R	P	F	R	P	F	R	P	F	R	P	F
Proposed method	**0.83**	**0.78**	**0.80**	**0.76**	**0.82**	**0.79**	**0.77**	**0.81**	**0.79**	**0.82**	**0.78**	**0.80**
FT-Magnitude	0.32	0.57	0.41	0.76	0.52	0.62	0.65	0.60	0.63	0.57	0.62	0.60
FT-Phase	0.52	0.76	0.61	0.84	0.63	0.72	0.23	0.63	0.33	0.86	0.52	0.65
DCT-Magnitude	0.54	0.50	0.52	0.46	0.50	0.48	0.66	0.59	0.62	0.54	0.61	0.57
DCT-Fourier-Magnitude	0.62	0.71	0.66	0.74	0.66	0.70	0.75	0.72	0.73	0.71	0.74	0.72

The bold indicates that the method achieves the best results compared to the existing methods.

proposed in the method are not robust to handle the effect of different degrees of forgery. These five methods are the state-of-the-art in their respective fields, and the objective is the same as the proposed work. In addition, the basis that is considered in all the five existing methods is the same as the proposed method. However, the feature extraction process and the idea of the methods are different compared to the proposed method.

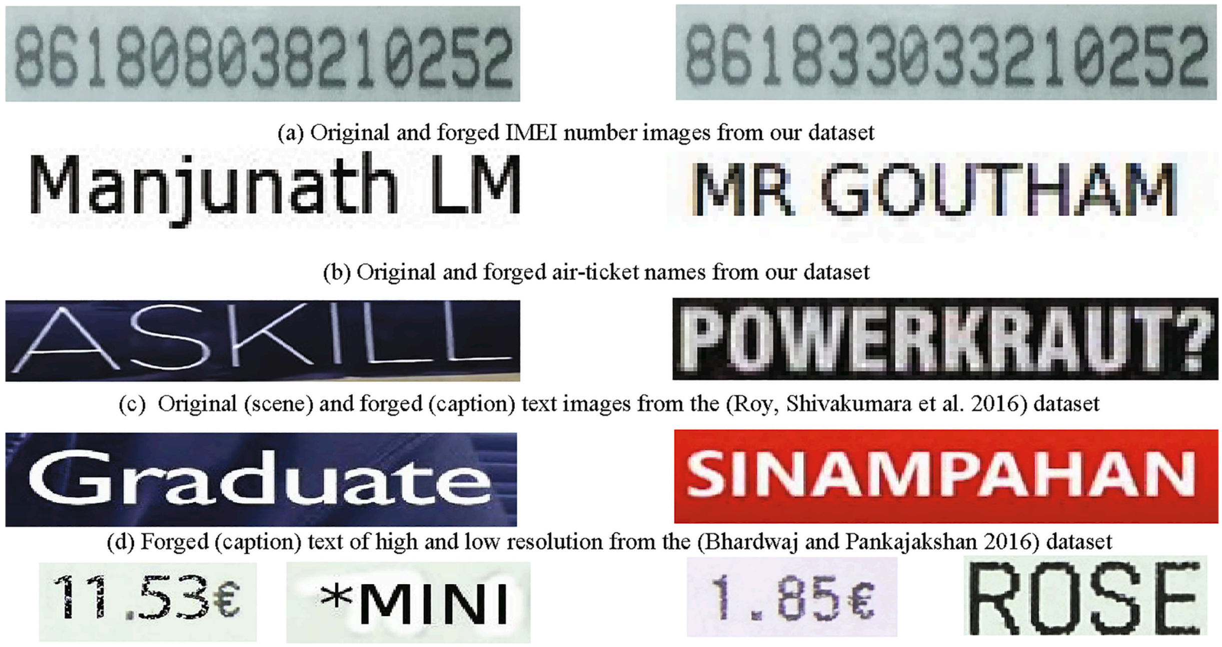
4.1. Dataset creation and evaluation

It is true that creating forged images is hard and a time-consuming task. The complexity of the task increases as the color of the background in original images changes. For instance, each forged image requires an average of 20–30 min to be created in our case. As a result, two persons spent almost 5–6 months generating 2000 images. In addition, to the best of our knowledge, this is the first dataset created containing forged IMEI numbers and altered air ticket information. We also present the procedure that we used for creating the forged dataset in this work and will release the dataset for future study or investigation. Since each IMEI number is an image, and the air ticket information is text in a plain PDF document, we used the Adobe Photoshop tool and Adobe acrobat PDF writer, respectively, for generating forged images because these two software tools are readily available and popular for editing images and text.

The different steps that we followed for creating forged IMEI numbers are shown in Fig. 8. The simple commands, namely, choosing *marker* from the Tool option menu, *selecting* the IMEI number to be forged, *copy*, *paste* command and *selecting* the *color* from the panel to change the color of the background are the same as the original, as shown in Fig. 8 for generating forged IMEI numbers. However, for the insertion operation, we choose an *eraser* from the menu to remove a part of an IMEI number, where we intend to insert different numbers and then use the *insert* option to paste it, which results in forged IMEI numbers by the insertion operation. The main difference between copy-paste and insertion operations is that the copy-paste operation changes the whole image, while the insertion operation changes a part of an image. In addition, the insertion operation involves the eraser operation as an additional operation compared to the copy-paste operation. For generating altered air ticket information, we follow the steps, namely, *select text*, *copy,* and *paste* as shown in Fig. 8. For the insertion operation, it is the same as copy-paste, except for the eraser operation.

For evaluating the performance of the proposed and existing methods, we use standard measures, namely, Recall (R), Precision (P) and F-measure (F) as defined in Equation (16)-(18). Since there is no ground truth, we count the number of forged images detected given by the proposed method manually to calculate the above-mentioned measures.

$$P = \frac{T_p}{T_p + F_p} \tag{16}$$



(a) Original and forged IMEI number images from our dataset

(b) Original and forged air-ticket names from our dataset

(c) Original (scene) and forged (caption) text images from the (Roy, Shivakumara et al. 2016) dataset

(d) Forged (caption) text of high and low resolution from the (Bhardwaj and Pankajakshan 2016) dataset

(e) Forged (altered text) and original (unaltered text) images of the ICPR 2018 FDC dataset.

Fig. 9. Samples of successful detections employing the proposed method for different datasets.

Table 2
Performances of the proposed and existing methods on the IMEI number and Air ticket datasets.

Methods	IMEI Number Dataset						Air Ticket Dataset					
	Original			Forged/Altered			Original			Forged/Altered		
	R	P	F	R	P	F	R	P	F	R	P	F
Proposed	**0.83**	0.78	**0.80**	0.76	**0.82**	0.79	**0.77**	0.81	**0.79**	0.82	0.78	**0.80**
Roy et al. (2016)	0.63	0.61	0.62	0.60	0.61	0.60	0.67	0.65	0.66	0.65	0.66	0.65
Bhardwaj and Pankajakshan (2016)	0.06	0.52	0.11	**0.94**	0.50	0.65	0.08	0.33	0.13	0.82	0.47	0.60
Wang et al. (2017)	0.44	0.39	0.41	0.33	0.38	0.35	0.65	**0.82**	0.73	**0.86**	0.71	0.78
Elkasrawi and Shafait (2014)	0.32	0.34	0.33	0.40	0.37	0.39	0.74	0.66	0.70	0.63	0.71	0.67
Shivakumara et al. (2018)	0.73	**0.82**	0.77	0.85	0.75	**0.80**	0.69	0.46	0.55	0.63	**0.80**	0.70

The bold indicates that the method achieves the best results compared to the existing methods.

$$R = \frac{T_p}{T_p + F_n} \tag{17}$$

$$F = 2*\frac{P*R}{P + R} \tag{18}$$

Here, T_p signifies the total number of correctly detected forged images, F_p signifies the total number of original images mistakenly detected as forged, and F_n is the total number of forged images, which are incorrectly missed.

4.2. Ablation study

To analyze the effect of the key steps used in the proposed method, we conducted experiments for the following individual steps using our dataset. The Fourier-Magnitude or Fourier-Phase, which considers magnitude and phase separately given by Fourier transform, DCT-Magnitude which considers only the magnitude given by DCT, DCT-Fourier-Magnitude which considers the magnitude given by the combination of DCT and Fourier, and DCT-Fourier-Phase which considers the phase given by the combination of DCT and Fourier (the proposed method). Note: for magnitude information, we use traditional statistics, namely, mean, variance, skew, and kurtosis but not the proposed phase-statistics to calculate measures. This is because the proposed circular phase-statistics are derived for phase-angle information but not for magnitude values. The results of the above individual steps are reported in Table 1 for IMEI and air ticket datasets. It is evident from Table 1 that Fourier-Phase is the best at F-measure for IMEI number images, while Magnitude is the best at F-measure for air ticket images. This shows that phase information is good for complex background images and magnitude is good for plain document images. The same conclusions can be drawn for both the original and forged classes of the IMEI number and air ticket datasets. However, the combination of DCT-Fourier-Magnitude is the best at F-measure for both datasets compared to the other key steps on the original and forged classes, but poorer when compared to the proposed method. This confirms that the combination of DCT and Fourier has the ability to handle diverse data. Therefore, the proposed method (DCT-Fourier-Phase) achieves the best results in terms of Recall, Precision and F-measure compared to the other individual key steps for both the IMEI numbers and the air tickets for both classes, as it integrates the advantages of DCT and the Fourier transform.

Table 4
Performances of the proposed and existing methods on the ICPR 2018 FDC dataset (Artaud et al., 2018).

Methods	Original			Forged		
	R	P	F	R	P	F
Proposed	0.78	**0.92**	0.84	**0.90**	0.75	0.81
Roy et al. (2016)	**0.88**	0.39	0.54	0.60	**0.94**	0.73
Bhardwaj and Pankajakshan (2016)	0.81	0.27	0.41	0.56	0.93	0.70
Wang et al. (2017)	0.87	0.84	**0.86**	0.85	0.88	**0.86**
Elkasrawi and Shafait (2014)	0.65	0.62	0.63	0.64	0.67	0.65
Shivakumara et al. (2018)	0.65	**0.92**	0.76	0.86	0.50	0.63

The bold indicates that the method achieves the best results compared to the existing methods.

4.3. Evaluating forged IMEI number and altered air ticket detection

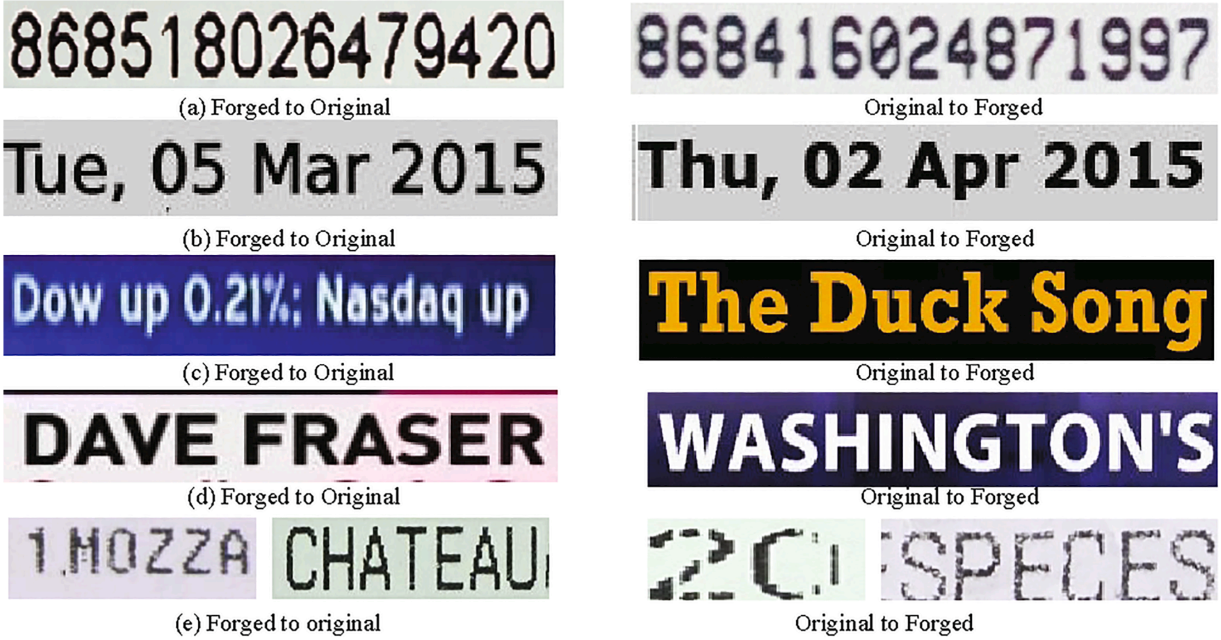
Qualitative results of the proposed method for forged IMEI numbers, altered air ticket detection, caption (forged) text detection from video images, and altered receipt detection from the ICPR 2018 FDC dataset are shown in Fig. 9(a)–(e), respectively, where it is noted that the proposed method performs accurate detection for the samples of different datasets, which exhibit different complexities. This shows that the proposed method has the ability to handle diverse data and this is due to the combination of DCT-Fourier-Phase along with the extracted Phase-statistics from the Phase-spectrum.

Quantitative results of the proposed and existing methods on our IMEI numbers, air tickets, Roy et al.'s, Bhardwaj's and the ICPR 2018 FDC datasets are reported in Tables 2–4. It is observed from Table 2 that the proposed method is the best at recall, F-measure for the original class, and the best at the precision for the forged class of the IMEI number dataset compared to the existing methods. Similarly, for original class of air ticket, the proposed method achieves the best recall and F-measure compared to the existing methods. For altered class of air ticket, the proposed method is better than existing methods in terms of F-

Table 3
Performances of the proposed and existing methods on the (Roy, 2016)dataset (Caption and scene text) and the Bhardwaj et al. dataset (2016).

Methods	Roy et al. dataset						Bhardwaj et al. dataset					
	Original (scene)			Forged (caption)			Set-1(Low resolution)			Set-2(High resolution)		
	R	P	F	R	P	F	R	P	F	R	P	F
Proposed	**0.88**	0.73	**0.80**	0.68	**0.85**	0.75	**0.82**	**0.87**	**0.84**	**0.92**	**0.88**	**0.90**
Roy et al. (2016)	0.75	0.71	0.73	0.63	0.68	0.65	0.62	0.58	0.60	0.66	0.63	0.64
Bhardwaj and Pankajakshan (2016)	0.56	0.46	0.51	0.40	0.51	0.45	0.64	0.62	0.63	0.68	0.65	0.67
Wang et al. (2017)	0.75	0.77	0.76	0.78	0.76	0.77	0.56	0.69	0.62	0.62	0.48	0.54
Elkasrawi and Shafait (2014)	0.83	0.68	0.74	0.61	0.78	0.69	0.47	0.54	0.51	0.40	0.34	0.37
Shivakumara et al. (2018)	0.54	**0.96**	0.69	**0.98**	0.68	**0.80**	0.73	0.70	0.72	0.80	0.74	0.76

The bold indicates that the method achieves the best results compared to the existing methods.



(a) Forged to Original	Original to Forged

(b) Forged to Original	Original to Forged

(c) Forged to Original	Original to Forged

(d) Forged to Original	Original to Forged

(e) Forged to original	Original to Forged

Fig. 10. Sample unsuccessful detection using the proposed method for different datasets, namely, our dataset in (a)-(b), Roy et al.'s in (c), Bhardwaj's in (d), and the ICPR 2018 FDC in (e).

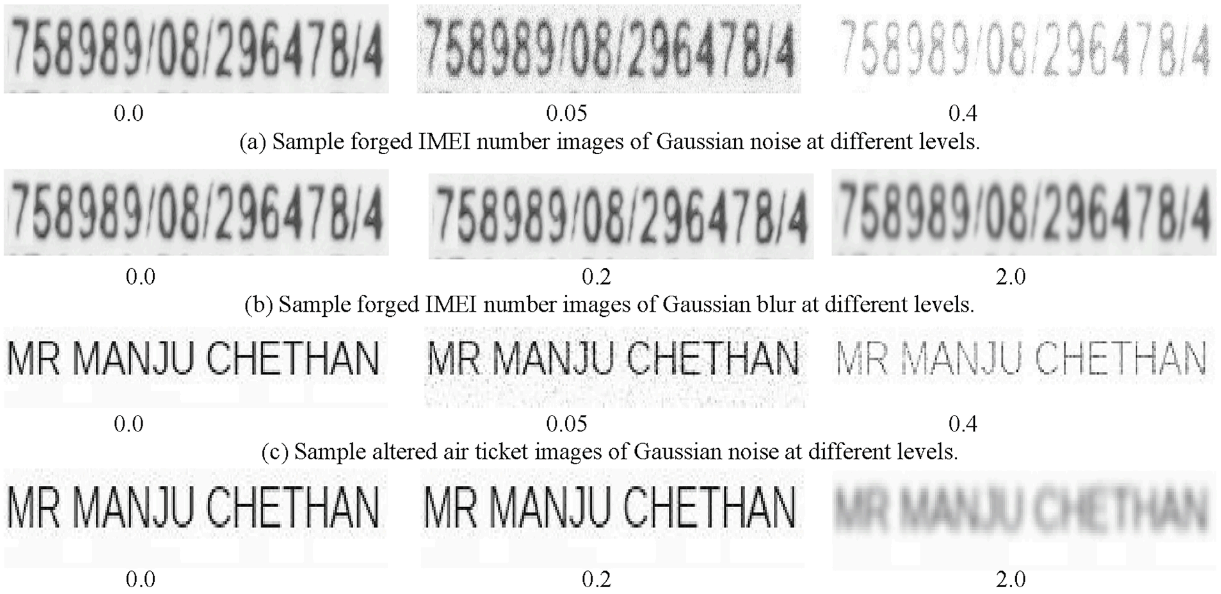
measure. However, the existing method (Shivakumara et al., 2018) achieves the best precision for the original class and the best F-measure for the forged class in IMEI numbers, and the best precision for the altered air ticket class compared to the proposed method. Since the existing method (Shivakumara et al., 2018) was developed for forged IMEI number detection from the same dataset with a different approach and features, it reports better precision for the original class of IMEI dataset while it performs the worst for the forged class of IMEI dataset compared to the proposed method. It is noted from the Table 2 that Bhardwaj et al. scores the best recall and the worst precision for the forged class of IMEI number dataset compared to the proposed method. Wang et al. (2017) scores the best precision and recall for original and altered classes, respectively for air ticket dataset compared to the proposed method. However, the proposed method is best at F-measure for original and altered classes of air ticket dataset compared to the existing methods. Table 2 shows that the existing methods (Bhardwaj & Pankajakshan, 2016; Roy et al., 2016; Elkasrawi & Shafait, 2014; Wang et al., 2017) were developed with a specific objective and different approaches for forged text detection in video and documents but not for IMEI number and altered air ticket detection. Therefore, the existing methods do not score better results for all the classes compared to the proposed and Shivakumara et al. (2018)'s method for both the datasets.

For Roy et al. and Bhardwaj et al. datasets, the results reported in Table 3 show that the proposed method achieves better recall, F-measure for the original class and better precision for the forged class of Roy et al.'s dataset while it is the best at all the three measures for Bhardwaj et al.'s dataset compared to the existing methods. However, the Shivakumara et al. (2018) method scores the highest precision for the original class and the highest recall as well as the F-measure for the forged class of Roy et al.'s dataset compared to the proposed method. This shows that Shivakumara et al. (2018)'s method is accurate for forged classes of Roy et al.'s dataset compared to the proposed method. However, it misses many images of the original class of Roy et al.'s dataset and hence the recall is lower than the proposed method. When we compare the results of the proposed and existing methods on Bhardwaj et al.'s dataset, all the existing methods report poor results compared to the proposed method. This is because the images of Bhardwaj et al.'s dataset are of good quality compared to the images of Roy et al.'s dataset. The reason for the poor results of the existing methods is the limitation of the features proposed in the respective methods. i.e., the features are sensitive to images of different resolutions. On the other hand, the proposed method is robust to different resolution.

For the ICPR 2018 FDC dataset, the results reported in Table 4 show that the proposed method is better at precision for the original class and better at recall for forged classes compared to the existing methods. But the precision is same for both the proposed and Shivakumara et al. (2018) method. However, Wang et al. (2017)'s approach is better at F-measure for the original and forged classes compared to the proposed and the other existing methods. This is because Wang et al. (2017)'s method is developed for document images and hence it works well for altered receipts from the ICPR 2018 FDC dataset. But Wang et al. (2017)'s approach is not as accurate as the proposed method for original classes for the ICPR 2018 FDC dataset. Similarly, Roy et al. (2016)'s approach is the best at recall for the original class and precision for the forged class of the ICPR 2018 FDC dataset compared to all other methods including the proposed method. However, it misses the images of forged classes when compared to the proposed method.

Overall, when we look at the discussion on the results of the proposed and existing methods on the IMEI number, altered air ticket, forged text in video and altered receipts from the ICPR 2018 FDC datasets (Artaud et al., 2018), the proposed method achieves the best results in terms of at least one measure out of the three measures for all different datasets whilst the existing methods do not. Therefore, one can infer that the proposed method is robust across different datasets and is effective in achieving better results compared to the existing methods. This shows that the proposed combination of the DCT-Fourier-Phase spectrum with phase statistics has the ability to deal with the challenges of different datasets. Note that in Table 3, Bhardwaj et al.'s dataset does not have the original classes because this dataset provides only caption texts (forged text) with different resolutions.

However, it is observed from Fig. 10 that the proposed method sometimes misclassifies original as forged and vice-versa across the four datasets. The reason is that during the forgery process, if the operation does not introduce noticeable errors, the proposed method fails to detect it well. In the case of Roy et al.'s and Bhardwaj's datasets, when an image contains fancy (ornamental) texts affected by blur distortion, the proposed method does not perform well. In addition, if texts share the same properties, such as contrast, shapes, and texture, the proposed



(a) Sample forged IMEI number images of Gaussian noise at different levels.

(b) Sample forged IMEI number images of Gaussian blur at different levels.

(c) Sample altered air ticket images of Gaussian noise at different levels.

(d) Sample altered air ticket images of Gaussian blur at different levels.

Fig. 11. Examples of forged IMEI number and altered air ticket images with Gaussian noise and blur effects at different levels.

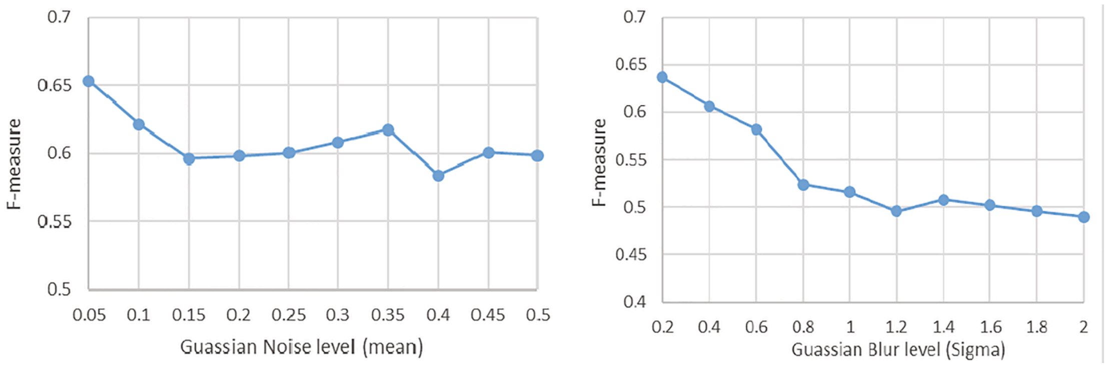


Fig. 12. Performance of the proposed method on different noise and blurred images from our dataset.

method tends to misclassify them. For the ICPR 2018 FDC dataset, when the images suffer from poor quality, the degradation has a conflict with the distortion introduced by the forgery operation. It is difficult to deal with this situation with the proposed method.

The success of forgery detection, irrespective of images and datasets, depends on the distortion introduced during the forgery operation. However, there is a possibility of introducing noise due to faults in the acquisition process or devices, and blur due to defocusing. In these situations, the distortions caused due to noise and blur have a conflict with the features extracted for forgery detection in the images. Therefore, the performance of the method degrades for those images affected by noise and blur. To analyze the performance of the proposed method in a noisy and blurred environment, we choose 500 samples from the original and 500 from forged classes across IMEI numbers and the altered air ticket datasets randomly for conducting experiments. For these images, we use the Gaussian function to add noise and blur at a different level as shown in the sample images from Fig. 11(a)–(d), where we can see that as noise and blur increases, the vital edge information is lost and hence the extracted feature loses discriminative power for separating forged information from actual information in the images.

In Fig. 12 the line graphs are drawn for varying noise and blur levels (on the X axis) and the corresponding average F-measure (on the Y axis). It is observed from Fig. 12 that the F-measure of the proposed method decreases as the level of noise and blur increases. This is the limitation of the proposed forgery detection approach. In this case, one should not consider abrupt changes in the forged images, rather we should consider the pattern or sequence of abrupt changes to study the consistency/inconsistency of the pattern. If the method is able to find an inconsistency, it is considered as forged text. This is beyond the scope of the proposed work. Thus, there is a scope for extension of the proposed work to overcome the above limitations in the near future.

5. Conclusions and future work

In this work, we have proposed a new combination of the DCT and Fourier transform for forged IMEI number and altered air ticket detection. The magnitude of DCT and the phase of the Fourier transform are combined in a new way for generating a phase-spectrum. Since the phase-spectrum contains angle information, we have proposed circular phase-statistics, which accept angle information from the phase spectrum. The phase statistics are formed as a vector and the vector is supplied to an SVM classifier for the detection of forged IMEI numbers and altered air tickets. Experimental results on our dataset of IMEI numbers, altered air tickets dataset, a benchmark dataset of video text, and altered receipts dataset from the ICPR 2018 FDC show that the proposed method has the ability to cope with the challenges of different datasets. A comparative study with the existing methods demonstrates the effectiveness of the proposed method in achieving better results on different datasets. However, it is noted from the Experimental Section that the proposed method misclassifies images when they lose vital edge information due to distortion. It is also evident from the experiments on noisy and blurred images that the performance of our method decreases as the level of noise and blur increases. Therefore, there is scope for extending the proposed work in the near future. To deal with this situation, we need to study the pattern of noise created by the forgery operation and distortions at the component level, rather than at the pixel level. It is expected that the noise pattern created by distortions may exhibit a uniform pattern throughout the text whilst the noise created by the forgery operation may not exhibit uniformity throughout the text due to variations in the forgery operation itself. In order to study this observation, in the future, we plan to adopt a learning approach, which includes multi-level deep learning to improve the performance of the proposed method.

CRediT authorship contribution statement

Lokesh Nandanwar: Methodology. **Palaiahnakote Shivakumara:** . **Swati Kanchan:** Methodology. **V. Basavaraja:** Investigation. **D.S. Guru:** Investigation. **Umapada Pal:** . **Tong Lu:** . **Michael Blumenstein:** .

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgement

The work is supported by the Natural Science Foundation of China under Grant No. 6167227. The authors would like to thank J. Divyashree, DDU, GKY Institute, Karnataka, India for her help in creating the dataset.

References

Ahmed, A. G. H., & Shafait, F. (2014). Forgery detection based on intrinsic document contents. *2014 11th IAPR international workshop on document analysis systems (DAS)*. IEEE.

Artaud, C., et al. (2018). Find it! Fraud detection contest report. In *International Conference on Pattern Recogniton* (pp. 13–18).

Behera, S. K., et al. (2018). Fast recognition and verification of 3D air signatures using convex hulls. *Expert Systems With Applications, 100*, 106–119.

Bertrand, R., et al. (2013). A system based on intrinsic features for fraudulent document detection. *2013 12th International conference on document analysis and recognition (ICDAR)*. IEEE.

Bhardwaj, D., & Pankajakshan, V. (2016). Image overlay text detection based on JPEG truncation error analysis. *IEEE Signal Processing Letters, 23*(8), 1027–1031.

Bouamra, W., et al. (2018). Towards the design of an offline signature verifier based on a small number of genuine samples for training. *Expert Systems With Applications, 107*, 182–195.

Chen, S., et al. (2016). Automatic detection of object-based forgery in advanced video. *IEEE Transactions on Circuits and Systems for Video Technology, 26*(11), 2138–2151.

D'Amiano, L., et al. (2018). A patchmatch-based dense-field algorithm for video copy-move detection and localization. *IEEE Transactions on Circuits and Systems for Video Technology*.

da Silva Barboza, R., et al. (2013). A color-based model to determine the age of documents for forensic purposes. *2013 12th International conference on document analysis and recognition (ICDAR)*. IEEE.

Elkasrawi, S., & Shafait, F. (2014). Printer identification using supervised learning for document forgery detection. *2014 11th IAPR international workshop on document analysis systems (DAS)*. IEEE.

Feng, C., et al. (2017). Motion-adaptive frame deletion detection for digital video forensics. *IEEE Transactions on Circuits and Systems for Video Technology, 27*(12), 2543–2554.

Gupta, A., et al. (2016). Synthetic data for text localisation in natural images. In Proceedings of the IEEE conference on computer vision and pattern recognition 2016.

Halder, B., & Garain, U. (2010). Color feature based approach for determining ink age in printed documents. *2010 20th International conference on pattern recognition (ICPR)*. IEEE.

Hou, J.-U., & Lee, H.-K. (2017). Detection of Hue modification using photo response nonuniformity. *IEEE Transactions on Circuits and Systems for Video Technology, 27*(8), 1826–1832.

Khan, Z., et al. (2015). Automatic ink mismatch detection for forensic document analysis. *Pattern Recognition, 48*(11), 3615–3626.

Kho, J. B., et al. (2019). An incremental learning method for spoof fingerprint detection. *Expert Systems with Applications, 116*, 52–64.

Kumari, M. S. & Shekar, B. (2011). On the use of phase of the discrete cosine transform for text detection in document images and video frames under variations in illumination. IICAI.

Luo, Z., et al. (2015). Localized forgery detection in hyperspectral document images. *2015 13th International conference on document analysis and recognition (ICDAR)*. IEEE.

Park, H.-C., & Joh, S.-E. (2009). Determination of phase spectrum using harmonic wavelet transform. *NDT & E International, 42*(6), 534–542.

Roy, S., et al. (2016). New tampered features for scene and caption text classification in video frame. *2016 15th International conference on frontiers in handwriting recognition (ICFHR)*. IEEE.

Salwa, L., & Mohammed, R. (2017). Novel phase-based descriptor using bispectrum for texture classification. *Pattern Recognition Letters, 100*, 1–5.

Sharma, A., & Sundaram, S. (2018). On the exploration of information from the DTW cost matrix for online signature verification. *IEEE Transactions on Cybernetics, 48*(2), 611–624.

Shivakumara, P., et al. (2014). Separation of graphics (superimposed) and scene text in video frames. *2014 11th IAPR international workshop on document analysis systems (DAS)*. IEEE.

Shivakumara, P., et al. (2018). A new RGB based fusion for forged IMEI number detection in mobile images. *2018 16th International conference on frontiers in handwriting recognition (ICFHR)*. IEEE.

Wang, Z., et al. (2017). Fourier-residual for printer identification. *2017 14th IAPR international conference on document analysis and recognition (ICDAR)*. IEEE.

Xu, J., et al. (2014). Graphics and scene text classification in video. *2014 22nd International conference on pattern recognition (ICPR)*. IEEE.

Yue, Y., et al. (2019). *An automatic system for generating artificial fake character images*. Springer.