IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received November 23, 2020, accepted December 13, 2020, date of publication December 30, 2020,
date of current version January 8, 2021.

Digital Object Identifier 10.1109/ACCESS.2020.3048246

Digital Image Forensic Approach to Counter the JPEG Anti-Forensic Attacks

AMIT KUMAR[1], GURINDER SINGH[2], ANKUSH KANSAL[1], AND KULBIR SINGH[1]

[1]Department of Electronics and Communication Engineering, Thapar Institute of Engineering and Technology (TIET), Patiala 147004, India
[2]Department of Computer Science, IIT, Ropar, Rupnagar 140001, India

Corresponding author: Ankush Kansal (akansal@thapar.edu)

ABSTRACT Rapid advancement in digital image processing tools and software's has made it extremely simple to manipulate the digital images without leaving any footprints. It becomes a hot issue about the security and threat to society with increasing growth of social media. JPEG compression format has been widely used in most of the digital cameras. The investigation of JPEG compression footprints can play an important role in image tampering detection. In this paper, a novel method is proposed to detect the JPEG compression. The proposed forensic scheme comprises of two steps i.e. selection of target difference image and generation of second-order statistical features by evaluating the Markov Transition Probability Matrices (MTPMs) for both intra and inter-block DCT domain. Finally, the resultant feature is used to train the SVM classifier for classification purposes. The experiment results on UCID and BOSSBase datasets show that the proposed forensic technique based on MTPM is capable of detecting the JPEG compression traces even in the presence of anti-forensic attacks.

INDEX TERMS JPEG compression, digital image forensics, Markov transition probability matrices (MTPMs), discrete cosine transform (DCT).

I. INTRODUCTION

Digital images have turned into an important data carrier with the improvement of internet and rapid advancement in image processing tools and software. This development has made it extremely simple to alter the image without leaving any foot prints. Every digital image we encounter in our daily life might have gone through several processing stages to increase its quality [1]. Due to the availability of numerous softwares, it becomes easier to forge the images without leaving any footprints [2]. Probably the most significant ongoing developments in editing tools like Adobe Photoshop, Paintshop Pro or GIMP [3] and others that incorporate automatic methods for editing. These includes changing outward appearance or age with FaceApp [4], and varying visual style of images using Deep Photo Style Transfer [5]. A significant number of these procedures are not just accessible but also easier to use. However, they are also available as default applications in gadgets. This results in various issues such as, authentication of image, copyright of the image medium, individual protection regarding privacy, etc. Image validation and identifying the hints of alteration without utilizing any pre-extracted or embedded data have turned into a vital and hot research field of image processing [6]. JPEG is a regularly utilized compression standard and it has been broadly utilized in cameras and image processing software's [7]. Moreover, the JPEG image format is used by 71.1% of all the websites based on the data provided by [8] on January 01, 2020. Therefore, JPEG compression has become an important part of many image forgeries. For example, in a forgery creation scenario, when some portion of a particular image is pasted on the other image of different quality and is resaved with different quality factor, then the resultant image becomes double JPEG compressed. Thus, the detection of JPEG compression can add a great value to evaluate the authenticity of digital images [9]–[11]. The processing history of digital images is detected by using deep learning [12]. The goal of this approach is to design a scalable detector for the cases when the image captured by the camera is processed, downscaled with different scaling factors, and JPEG compressed again. In [13], a powerful machine learning based method is presented to identify single and double JPEG compressed images. Firstly, the variation between the magnitude of JPEG coefficient 2-D array of a given JPEG image and its shifted forms along different

The associate editor coordinating the review of this manuscript and approving it for publication was Varuna De Silva.

directions is utilized to enhance the artifacts of double JPEG compression. To model the difference 2-D arrays, Markov random process is applied in order to use the second-order statistics. In [14], the statistical characteristics of DCT coefficients are initially investigated based on recompression files sets. Afterwards, effect of double compression is analyzed between doctored and non-doctored region in a tampered image. Then, the DCT coefficients histograms of each block in tampered images are extracted and represented as feature vectors. The processing chain is studied in [15] which arise in the case of JPEG compression anti-forensics. In [15], the perspective of the forensic analyst has been taken to show that how it is conceivable to counter the aforementioned anti-forensic technique for uncovering the hints of JPEG compression, irrespective of the quantization matrix being used. The theoretical analysis of Benford-Fourier coefficients has been extended in [16] to present the forensic detector based on JPEG compression traces in an uncompressed format. A forensic detector based on theoretical analysis of Benford–Fourier coefficients computed on 8 × 8 block in DCT domain is presented in [17]. A feature vector for the detection of JPEG compression is presented in [18] based on Hough line, peaks, and the Harris-Stephens corner features. A modified version of densely connected convolutional networks (DenseNet) is presented in [19] to achieve the task of JPEG compression identification. A special filtering layer contains typically selected filtering kernels that can help the system to segregate the images more effectively. A technique is presented in [20] to detect the aligned double JPEG compression based on the fact that adjacent DCT coefficients correlation is enhanced due to DCT transform, and the correlation among same locations in adjacent DCT blocks is strong. The aim of the anti-forensic techniques is to create barriers in the forensic investigation process by hiding the JPEG compression artifacts. There are numerous anti-forensic techniques [21]–[27] available based on JPEG compression. The JPEG compression introduces comb like gaps in the distribution of DCT coefficients histogram of considered image [25]. Therefore, the target of the anti-forensic technique is to fill these gaps by adding noise in the DCT coefficients histogram to fool the forensic detectors. Moreover, deblocking operation is employed to suppress the blocking artifacts in spatial domain. The added noise results in the grainy noise or unnatural noise in the resultant image. Therefore, recent antiforensic technique [27] applied denoising operation to remove the unwanted grainy noise in order to improve the image visual quality.

The following new insights are revealed in this article when compared to the existing techniques:

- Most of the existing JPEG anti-forensic techniques remove the footprints based on first order statistics, but it is very difficult for these techniques to properly conceal the footprints based on second-order statistics. Therefore, a JPEG forensic technique based on second-order statistical analysis is proposed in this paper to reveal the JPEG compression artifacts even in the presence of an anti-forensic attack.
- The MTPMs based second order statistical analysis is initially employed in image steganalysis but has not been used in the existing literature for JPEG forensics for countering JPEG anti-forensics.
- Most of the efficient JPEG anti-forensic techniques are not considered during the performance evaluation of existing JPEG forensic techniques due to different strengths. Therefore, this problem of different strengths of anti-forensic techniques is resolved in this paper by designing an efficient second order statistical feature.
- The proposed second order statistical feature has smaller size in comparison to the commonly used steganalysis features such as subtractive pixel adjacency matrix (SPAM) and spatial rich model (SRM).

The organization of remaining article is as follows: Section 2 briefly describes the proposed forensic scheme based on second order statistical analysis. The experimental results for proposed forensic approach and its comparison with the existing methods are discussed in Section 3. Finally, Section 4 concludes the paper.

II. PROPOSED SCHEME

The existing JPEG compression detection techniques are based on the analysis of first order statistics based on image histogram. These detection techniques can be easily misguided by using anti-forensic techniques. Therefore, to resolve this problem, a higher order statistical analysis is required. In this paper, a second order statistical analysis is done in difference domain based on the MTPM as shown in Fig. 1. It is worth noting that when the images are transformed from spatial domain to frequency domain with DCT transformation, the correlation between the adjacent coefficients within the DCT block becomes weak to some extent. But, the correlation between the neighboring coefficients in the same block is still noticeable. Moreover, there is a strong correlation between the adjacent block DCT coefficients. Moreover, it is observed that the pixels difference is linearly dependent on the DCT coefficients difference obtained from the same locations in adjacent DCT blocks, when ignoring the quantization loss. Though the quantization loss is irreversible and expected, still it affects the dependency. Thus, the quantization loss as well as dependency is reflected due to the correlation among the same locations in the adjacent DCT blocks. Because of this fact, the intra and inter-block frequency domain features are extracted to reveal these dependencies. The proposed scheme comprises of three steps which includes selection of target difference image, evaluation of Markov transition matrices for both intra and inter-block DCT domain, and generation of mono-dimensional signal as shown in Fig.1. The resultant mono-dimensional signal is fed into SVM classifier to distinguish between the JPEG compressed and original images.

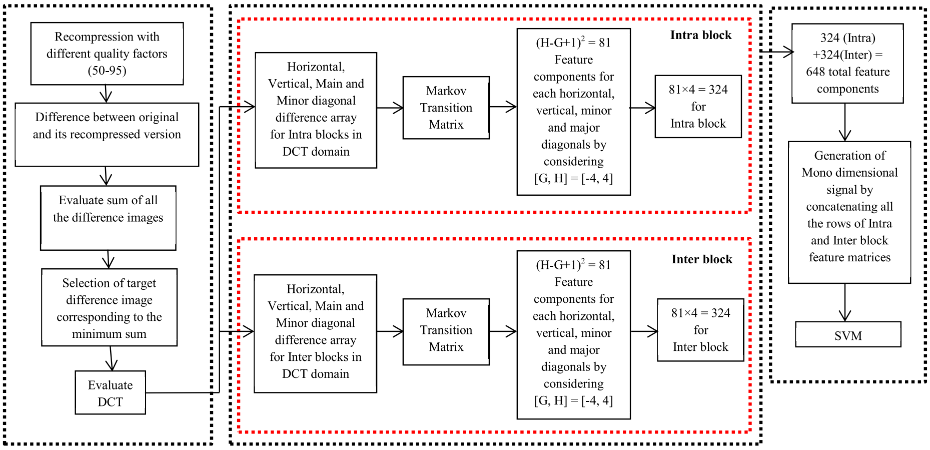

Recompression with different quality factors (50-95)
Difference between original and its recompressed version
Evaluate sum of all the difference images
Selection of target difference image corresponding to the minimum sum
Evaluate DCT
Horizontal, Vertical, Main and Minor diagonal difference array for Intra blocks in DCT domain
Markov Transition Matrix
(H-G+1)² = 81 Feature components for each horizontal, vertical, minor and major diagonals by considering [G, H] = [-4, 4]
Intra block
81×4 = 324 for Intra block
Horizontal, Vertical, Main and Minor diagonal difference array for Inter blocks in DCT domain
Markov Transition Matrix
(H-G+1)² = 81 Feature components for each horizontal, vertical, minor and major diagonals by considering [G, H] = [-4, 4]
Inter block
81×4 = 324 for Inter block
324 (Intra) +324(Inter) = 648 total feature components
Generation of Mono dimensional signal by concatenating all the rows of Intra and Inter block feature matrices
SVM

FIGURE 1. Sketch of the proposed forensic technique.

A. SELECTION OF TARGET DIFFERENCE IMAGE

The application of image processing operations such as JPEG compression, resampling, etc. results in the significant modification of original image pixel values. Therefore, it is a difficult task to preserve the intrinsic statistics (for example, adjacent pixels correlation) of the original image. The difference domain is considered rather than the spatial domain to analyze the local pixels properties for the detection of these modifications. This is due to the reason that difference domain is less dependent on the image contents. The image under investigation is initially JPEG compressed by considering various quality factors ranging from 50 to 95. Afterwards, the difference is calculated between the considered image and its recompressed versions. After calculating the difference between the considered image and its recompressed versions, the individual sum of all the difference images has been taken. After performing this step we have selected the difference image corresponding to the minimum sum i.e difference image with minimum sum has been selected which is our target image in the preprocessing of our proposed approach. Then, DCT is applied to the target image for further processing.

B. EVALUATION OF MARKOV TRANSITION PROBABILITY MATRICES IN THE DCT DOMAIN

The inter-block and intra-block correlation among the DCT coefficients are exploited by MTPM. The DCT coefficients within the same block are analyzed in different directions to reveal the intra-block correlation. On the contrary, the dependence of DCT coefficients at same position of the adjacent blocks reveals the inter-block correlation. The irregularities in the neighboring DCT coefficients correlation is exploited by using the second order statistical analysis of MTPM. The selected target difference image (I_{tar}) of size $m \times n$ is processed to obtain a 2-D DCT coefficients array of size 8×8 as shown in Fig. 2(a). The 2-D DCT coefficient array is represented by $T'(f', e')$ having $(m/8) \times (n/8)$ total number of DCT blocks. Afterwards, the inconsistencies in the neighboring DCT coefficients correlation obtained in the difference domain is further highlighted by using difference DCT coefficient 2-D arrays along horizontal, vertical, main and minor diagonal directions as shown in Fig. 3. These difference 2-D arrays are modelled by using second order statistical analysis based on Markov random process. The MTPMs can be calculated by using Eqs. (1) and (2) for the intra-block neighboring DCT coefficients along horizontal and vertical directions respectively. The MTPM features for the coefficients pair (v, u) along horizontal and vertical directions with conditional distribution probabilities $\mathcal{P}\left(T'\left(f'+1, e'\right) = v | T'\left(f', e'\right) = u\right)$ and $\mathcal{P}\left(T'\left(f', e'+1\right) = v | T'\left(f', e'\right) = u\right)$ respectively are represented by $\boldsymbol{MTPM}_{intra,h}$ and $\boldsymbol{MTPM}_{intra,v}$. The function $\partial\left(a, b\right) = 1$ for $a = b$, and $\partial\left(a, b\right) = 0$, otherwise. Similarly, the evaluation of MTPMs along main and minor diagonal difference arrays can be performed for the intra-block DCT coefficients [28].

$$\begin{aligned}\boldsymbol{MTPM}_{intra,h}\left(u, v\right) &= \mathcal{P}\left(T'\left(f'+1, e'\right) = v | T'\left(f', e'\right) = u\right) \\ &= \frac{\mathcal{P}\left(T'\left(f', e'\right) = u,\ T'\left(f'+1, e'\right) = v\right)}{\mathcal{P}\left(T'\left(f', e'\right) = u\right)} \\ &= \frac{\sum_{e'=1}^{T_{e'}-1}\sum_{f'=1}^{T_{f'}-1} \partial(T'\left(f', e'\right), u)\partial(T'\left(f'+1, e'\right), v)}{\sum_{e'=1}^{T_{e'}-1}\sum_{f'=1}^{T_{f'}-1} \partial(T'\left(f', e'\right), u)}\end{aligned} \tag{1}$$

$$\begin{aligned}\boldsymbol{MTPM}_{intra,v}\left(u, v\right) &= \mathcal{P}\left(T'\left(f', e'+1\right) = v | T'\left(f', e'\right) = u\right) \\ &= \frac{\mathcal{P}\left(T'\left(f', e'\right) = u,\ T'\left(f', e'+1\right) = v\right)}{\mathcal{P}\left(T'\left(f', e'\right) = u\right)} \\ &= \frac{\sum_{e'=1}^{T_{e'}-1}\sum_{f'=1}^{T_{f'}-1} \partial(T'\left(f', e'\right), u)\partial(T'\left(f', e'+1\right), v)}{\sum_{e'=1}^{T_{e'}-1}\sum_{f'=1}^{T_{f'}-1} \partial(T'\left(f', e'\right), u)}\end{aligned} \tag{2}$$

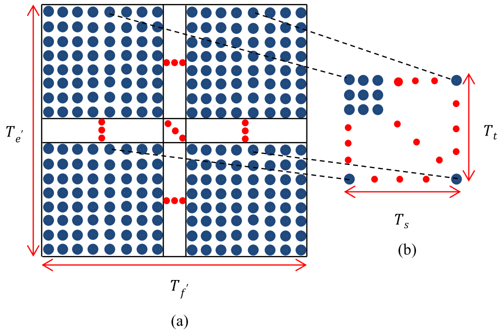


FIGURE 2. (a) 2-D array of DCT coefficients, (b) Realization of Mode (5) 2-D array.

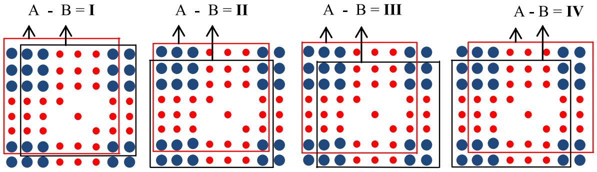


FIGURE 3. Difference DCT/Mode 2-D array in Horizontal (I), Vertical (II), Main diagonal (III), and Minor diagonal (IV) directions.

The correlation of inter-block is reflected along the modes of DCT coefficients i.e. the coefficients in the similar position of adjacent 8×8 blocks, which capture the frequency characteristics of those 8×8 blocks. Firstly, DCT coefficient 2-D array is used to form 2-D arrays. Afterwards, mode 2-D arrays of the image are used to create difference mode 2-D arrays along different directions to reveal the inter-block correlation as shown in Fig. 3. The Markov process is applied on these difference mode 2-D arrays. All the difference mode 2-D arrays are processed along each direction to evaluate the average transition probability matrix. The mode (5) 2-D array formation is shown in Fig. 2(b). Each mode 2-D array has the dimension i.e. $T_s = T_{f'}/8$ and $T_t = T_{e'}/8$ in horizontal and vertical directions respectively. The DC component (mode 1) is not considered in the evaluation because it does not affect the results significantly. Therefore, only 63 mode 2-D arrays are obtained for a given image. In a mode 2-D array, the mode coefficient is represented as as $T^{(mode)}(s, t)$, where $s \in [0, T_s - 2]$, $t \in [0, T_t - 2]$ and $mode \in [2, 64]$. The difference mode 2-D array in four different directions is evaluated as [29]:

$$T_h^{(mode)}(s,t) = T^{(mode)}(s,t) - T^{(mode)}(s+1,t) \tag{3}$$

$$T_v^{(mode)}(s,t) = T^{(mode)}(s,t) - T^{(mode)}(s,t+1) \tag{4}$$

$$T_{d'}^{(mode)}(s,t) = T^{(mode)}(s,t) - T^{(mode)}(s+1,t+1) \tag{5}$$

$$T_{d''}^{(mode)}(s,t) = T^{(mode)}(s+1,t) - T^{(mode)}(s,t+1) \tag{6}$$

The MTPMs can be calculated by using Eqs. (7) and (8) for the inter-block neighboring DCT coefficients along horizontal and vertical directions respectively. The MTPM features for the coefficients pair (v, u) along horizontal and vertical directions with conditional distribution probabilities $\mathcal{P}(T_h(s+1,t) = v | T_h(s,t) = u)$ and $\mathcal{P}(T_v(s,t+1) = v | T_v(s,t) = u)$ respectively are represented by $\boldsymbol{MTPM}_{inter,h}$ and $\boldsymbol{MTPM}_{inter,v}$. Similarly, the MTPM can also be defined for the main and minor diagonal difference arrays for inter-block DCT coefficients. Each MTPM consists of $(H - G + 1)^2$ elements, where $[G, H]$ lies in the range of u and v. The Eq. (9) is used to calculate the matrix containing $(H - G + 1)^2$ number of feature components. The inconsistencies introduced due to the modification of neighboring DCT coefficients correlation dominates near the origin. Therefore, the range of u and v is set to $[-4, 4]$, thereby providing 81 feature components for each MTPM. Consequently, all the MTPMs results into 648 feature components [29].

$$\begin{aligned}
&\boldsymbol{MTPM}_{inter,h}(u,v) \\
&= \mathcal{P}(T_h(s+1,t) = v | T_h(s,t) = u) \\
&= \frac{\mathcal{P}(T_h(s,t) = u,\ T_h(s+1,t) = v)}{\mathcal{P}(T_h(s,t) = u)} \\
&= \frac{\sum_{t=1}^{T_t-2}\sum_{s=0}^{T_s-2}\sum_{mode=2}^{64}\partial(T_h^{(mode)}(s,t) = u)}{1} \\
&\quad \times \frac{\partial\left(T_h^{(mode)}(s+1,t) = v\right)}{\sum_{t=1}^{T_t-2}\sum_{s=0}^{T_s-2}\sum_{mode=2}^{64}\partial\left(T_h^{(mode)}(s,t) = u\right)}
\end{aligned} \tag{7}$$

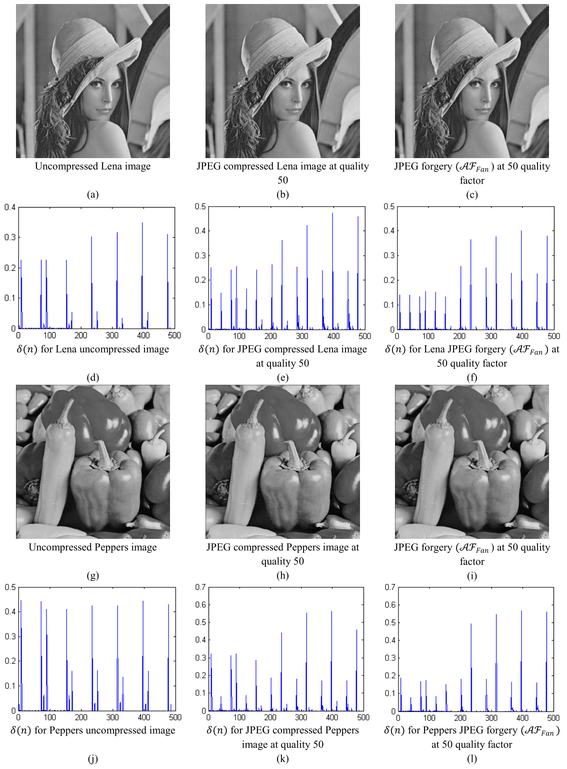
$$\begin{aligned}
&\boldsymbol{MTPM}_{inter,v}(u,v) \\
&= \mathcal{P}(T_v(s,t+1) = v | T_v(s,t) = u) \\
&= \frac{\mathcal{P}(T_v(s,t) = u,\ T_v(s,t+1) = v)}{\mathcal{P}(T_v(s,t) = u)} \\
&= \frac{\sum_{t=1}^{T_t-2}\sum_{s=0}^{T_s-2}\sum_{mode=2}^{64}\partial(T_v^{(mode)}(s,t) = u)}{1} \\
&\quad \times \frac{\partial(T_v^{(mode)}(s,t+1) = v)}{\sum_{t=1}^{T_t-2}\sum_{s=0}^{T_s-2}\sum_{mode=2}^{64}\partial(T_v^{(mode)}(s,t) = u)}
\end{aligned} \tag{8}$$

$$\begin{aligned}
&\boldsymbol{MTPM} \\
&= \begin{bmatrix}
\mathcal{P}(G|G) & \mathcal{P}(G|G+1) & \cdots & \mathcal{P}(G|H) \\
\mathcal{P}(G+1|G) & \mathcal{P}(G+1|G+1) & \cdots & \mathcal{P}(G+1|H) \\
\vdots & \vdots & \ddots & \vdots \\
\mathcal{P}(H|G) & \mathcal{P}(H|G+1) & \ldots & \mathcal{P}(H|H)
\end{bmatrix}
\end{aligned} \tag{9}$$

C. GENERATION OF SECOND ORDER STATISTICAL ANALYSIS BASED MONO-DIMENSIONAL SIGNAL

Presently, we are attempting to examine the impact of anti-forensic methodologies on MTPMs. Most of the anti-forensic methods are based on the optimization schemes with a goal of finding an optimal mapping to get back the statistics of original uncompressed image. In this procedure, pixels are shifted from one bin to another based on a maximal pixel distortion. The mapping is performed by choosing pixels in such a way that it diminishes the perceptual effect. The gaps in the histogram of JPEG compressed images can be completely removed by these anti-forensic attacks. Although, histograms of anti-forensically processed and uncompressed images are alike but there are still noticeable traces in the MTPM. We are looking for a second-order statistical feature resulting from MTPM that can differentiate the anti-forensically processed and uncompressed images efficiently.

A mono-dimensional signal is derived by analyzing various characteristics based on MTPM of the considered image. This signal is obtained by concatenation of rows of inter as well as intra-block MTPMs. It emphasizes the dithering artifacts that are introduced during image anti-forensics. Let $\delta(n)$ indicates a mono-dimensional signal of size $(1, 648)$ based on MTPMs. The investigation of signal $\delta(n)$ outlines that an uncompressed image shows a smooth behavior while the JPEG compressed and the image processed through anti-forensics demonstrates oscillating behavior as revealed in Fig. 4. It can be noticed from Fig. 4(e) and 4(k) that oscillations in JPEG compressed image are more when compared to the image processed through anti-forensics shown in Fig. 4(f) and 4(l) respectively. This is because the anti-forensic schemes are employed to hide the JPEG compression artifacts in order to fool the forensic detectors. Nevertheless, this feature is capable of detecting anti-forensically processed JPEG images efficiently. This mono dimensional signal is fed to SVM to classify the signals generated from uncompressed and anti-forensically processed JPEG compressed images.



Uncompressed Lena image
(a)

JPEG compressed Lena image at quality 50
(b)

JPEG forgery ($\mathcal{AF}_{Fan}$) at 50 quality factor
(c)

$\delta(n)$ for Lena uncompressed image
(d)

$\delta(n)$ for JPEG compressed Lena image at quality 50
(e)

$\delta(n)$ for Lena JPEG forgery ($\mathcal{AF}_{Fan}$) at 50 quality factor
(f)

Uncompressed Peppers image
(g)

JPEG compressed Peppers image at quality 50
(h)

JPEG forgery ($\mathcal{AF}_{Fan}$) at 50 quality factor
(i)

$\delta(n)$ for Peppers uncompressed image
(j)

$\delta(n)$ for JPEG compressed Peppers image at quality 50
(k)

$\delta(n)$ for Peppers JPEG forgery ($\mathcal{AF}_{Fan}$) at 50 quality factor
(l)

FIGURE 4. (a), (b), (c) and (g), (h), (i) denote the uncompressed, JPEG compressed and anti-forensically processed Lena and Peppers images respectively (d), (e), (f) and (j), (k), (l) represent the resultant signals $\delta(n)$ for the uncompressed, JPEG compressed and anti-forensically processed Lena and Peppers images respectively.

Algorithm for the Proposed JPEG Forensic Technique

```
Input:
  $I_{input}$: JPEG compressed or Anti-forensically processed JPEG image.
Output:
  $f$: Mono-dimensional feature
Parameters:
  $QF$: Quality factor
  $I_{recompressed}$: Recompressed image
  $I_{diff}$: Difference image
begin
  [x, y] = size($I_{input}$);
  QF = 50:1:95;
  $I_{difference} = zeros(x, y, length(QF))$;
  Initialize $count = 1$;
  for $i = QF$ do
    $I_{recompressed} = recompress\left(I_{input}, i\right)$; % Recompression with different quality factors
    $I_{diff}(:, :, c) = I_{input}(:, :) - I_{recompressed}(:, :)$;
    $T_{span}(:, :, c) = sum(sum(I_{diff}(:, :, c)))$;
    count = count + 1;
  end
    $[value, index] = min(T_{span})$;
    $I_{selected} = I_{diff}(:, :, index)$; %Difference image is selected corresponding to the minimum sum
    $I_{dct} = abs(dct(I_{selected}))$;
  $f1 = MTPM_{intra,h}(I_{dct})$;  $f2 = MTPM_{inter,h}(I_{dct})$;
  $f3 = MTPM_{intra,v}(I_{dct})$;  $f4 = MTPM_{inter,v}(I_{dct})$;
  $f5 = MTPM_{intra,d'}(I_{dct})$;  $f6 = MTPM_{inter,d'}(I_{dct})$;
  $f7 = MTPM_{intra,d''}(I_{dct})$;  $f8 = MTPM_{inter,d''}(I_{dct})$;
  % $MTPM$ s based on intra and inter-block of DCT domain are computed for Horizontal, Vertical, Main and Minor diagonal difference matrices
  $f = [f1; f2; f3; f4; f5; f6; f7; f8]$; % Compute the resultant feature vector
end
```

III. EXPERIMENTAL RESULTS

The performance of the proposed forensic technique is evaluated by conducting various tests on the standard databases such as Uncompressed Color Image Database (UCID) [30] and BOSSBase database [31]. UCID dataset includes 1338 TIFF images in uncompressed format having different real world scenes. The BOSSBase dataset contains 10,000 images in raw format. Initially, the JPEG images are obtained by compressing the UCID and BOSSBase database images with various quality factors ranging from $\{50, 51, 52, \ldots.95\}$. Afterwards, the JPEG forgeries datasets are created by processing these images with different anti-forensic techniques. The training dataset (UCIDTrain) is created from UCID dataset by randomly selecting 669 images and the remaining images of UCID dataset (UCIDTest) are used for testing. Various forensic techniques based on JPEG compression are as follows:

- K_V, JPEG forensic detector based on total variation [32], [15].
- K_L, JPEG detector based on calibration feature [33].
- K_U^1 and K_U^2, represents the detectors based on JPEG blocking artifacts [25].
- K_{Li}^{S100}, detector based on 100-D intra and inter block correlation feature [34], [28].
- K_{AR}^{S10}, detector based on autoregressive model [35].
- K_{SPAM}^{S686}, detector based on 686-D SPAM feature [36].
- K_{SRM}^{S714}, represents residual-based feature detector [37].
- K_{CM}, JPEG detector based on Co-occurrence matrices [38]
- K_{MTPM}, proposed MTPM based forensic approach.

The JPEG anti-forensic techniques employed to validate the performance of the proposed counter JPEG anti-forensic approach are as follows:

- $\mathcal{F}D_{S_q}$, represents the anti-forensic scheme DCT histogram smoothing [21].
- $\mathcal{F}D_{S_qS_b}$, dithering and deblocking operation based anti-forensic method [22].
- $\mathcal{F}D_V$, represents a perceptual anti-forensic dithering technique [23].
- $\mathcal{F}D_{S_u}$, anti-forensic technique with SAZ attack [24].
- $\mathcal{F}D_{Fan}$, adaptive dithering model based four-step JPEG anti-forensic scheme [26].
- $\mathcal{F}D_{Gur}$, signifies an improved TV-based deblocking operation and denoising algorithm based anti-forensic approach [27].

A. COMPARING SVM-BASED FORENSIC DETECTORS

In steganalysis methods [39], [40], minimum decision error (P_e) is considered as an evaluation parameter for measuring the performance of forgeries against various forensic detectors. Initially, ROC curve is obtained for various JPEG forensic detectors by considering positive and negative cases. Here the JPEG (anti-forensic) images are considered as positive cases, while the authentic and uncompressed images are considered as negative cases. Various periodic gaps are left during JPEG compression. These periodic gaps are filled by using anti-forensic methods. But, the dithering operation of anti-forensic technique introduced an unnatural or grainy noise in spatial domain. The presented forensic method targets to uncover the JPEG compression footprints even after the application of JPEG anti-forensic techniques. As discussed earlier, UCID dataset consisting of 1338 images is considered to evaluate the proposed technique. The images are chosen randomly for better analysis such that the images are indicated with the similar label, which is used to train the classifier. Further, the images used for the purpose of testing are not labeled and are used to authenticate the efficacy of algorithm. To evaluate the performance 70% of images are utilized for training, while 30% images are used for testing of the proposed technique. The confusion matrix for proposed approach summarizes the performance of classifier with respect to the testing data as shown in Table 1.

TABLE 1. Confusion matrices for the UCID dataset.

UCID	Predicted Negative	Predicted Positive
Actual Negative	200	1
Actual Positive	3	198

In accordance with the 70:30 proportions for training and testing, 936 images are used to train the classifier while the remaining 402 images are used for the testing purpose. Hence, the confusion matrix is formed on the basis of 402 images to envisage the accuracy of the classifier by relating actual and predicted classes. It is presumed in case of SVM based detectors that the forensic analyst possess the knowledge of forensic as well as anti-forensic approaches and can create the dataset of forged images to train the detector. This can be considered as the worst case scenario for anti-forensic techniques. The prevailing SVM based detectors K_{Li}^{S100}, K_{AR}^{S10}, K_{SPAM}^{S686} and K_{SRM}^{S714} can efficiently overcome the JPEG anti-forensic approaches. It is a challenging task to fool the machine learning based detectors by the anti-forensic approaches [41]. It is the worst case for JPEG anti-forensics but it is favorable for JPEG compression forensics. The training of SVM based detector is done with each form of JPEG anti-forensic image by considering each replacement rate for given feature vector. The SVM based forensic detectors K_{Li}^{S100}, K_{AR}^{S10}, K_{SPAM}^{S686} and K_{SRM}^{S714} used in steganalysis possess high detection accuracy along with the minimum decision error values less than 0.1. It is noticed that because of the high feature dimensionality of the existing SRM-34,671, it is rarely used in SVM [37]. SRM-714 [37] which is the modified version of SRM-34,671 performs similar to that of SRM-34,671 but with smaller feature dimensionality. Thus, in order to make the comparison feasible, the proposed approach is compared with SRM-714. The modification of DCT coefficients is done on a large scale so as to hide the JPEG compression footprints. The modification of DCT coefficients leads to the high modification rate (bits per pixel) in case of image steganalysis. The performance of proposed approach K_{MTPM} is analyzed by creating the JPEG forgeries with substitution process. This process involves replacement of the centre part of a particular uncompressed image with the image processed by JPEG anti-forensics with the replacement rate varying from 0.05 to 1. The forensic testing is done on the basis of both processed as well as uncompressed images. LIBSVM [42] with Gaussian kernel is considered for training the SVM classifier. The parameters of SVM classifier are attained from the five-fold cross validation with the multiplicative grid [36]. The SVM classifiers are trained with the uncompressed images and their corresponding JPEG (anti-forensic) images. The images created from the UCIDTest are used by these classifiers for forensic testing.

Minimum decision error values on the basis of image replacement rate against various anti-forensic techniques have been shown in Fig. 5. It is clear from Fig. 5 (e) that

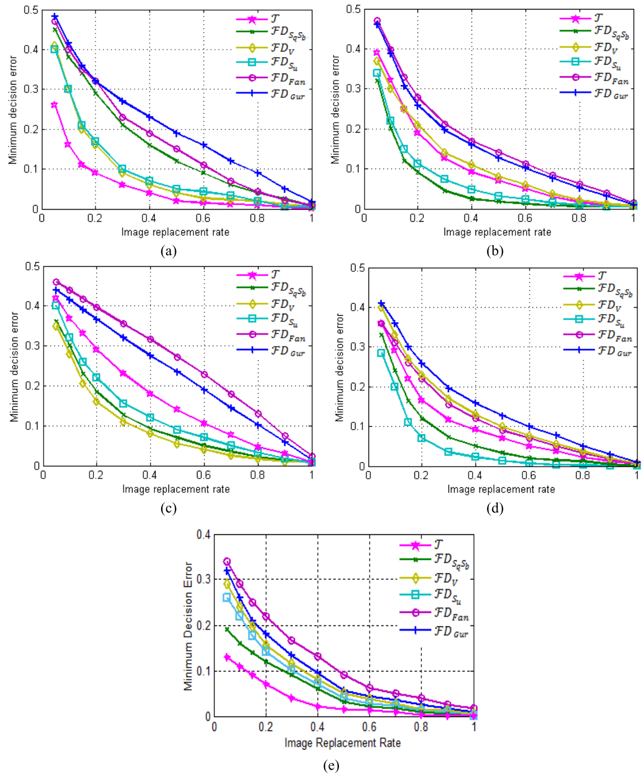


FIGURE 5. Minimum decision error based on various image replacement rates against different forgeries by considering SVM-based detectors trained on UCIDTrain dataset. The results are obtained on UCIDTest dataset. (a) K_{Li}^{S100} [34], (b) K_{SPAM}^{S686} [36], (c) K_{AR}^{S10} [35], (d) K_{SRM}^{S714} [37] (e) Proposed (K_{MTPM}).

the proposed technique K_{MTPM} has outperformed the existing forensic detectors (a) K_{Li}^{S100}, (b) K_{SPAM}^{S686}, (c) K_{AR}^{S10} and (d) K_{SRM}^{S714} by giving lower values of minimum decision error against various anti-forensic techniques. The purpose of the proposed forensic method is to identify the JPEG compressed as well as anti-forensically processed JPEG images. In terms of forensic undetectability, the technique $\mathcal{FD}_{Fan}$ and $\mathcal{FD}_{Gur}$ outperforms the other anti-forensic techniques. This is due to the fact that explicit DCT histogram smoothing is employed to create JPEG forgeries in JPEG anti-forensic methods [26] and [27]. This smoothing prompts further alteration in the statistics of image. In the case of existing SVM-based detectors, the anti-forensic technique presented in [15] gives high minimum decision error when the replacement rate is 0.10. Thus, it is easy for someone to create a forgery by substituting a block of size 112 × 160 in the UCID dataset images of size 384 × 512. Various sorts of forgeries can be made by substituting the block of size 112 × 160, for example, the forger without any difficulty can substitute the head of one individual in the image. While, it is extremely hard task for the anti-forensic schemes to trick the machine learning detectors when attempting to disguise the whole JPEG image as uncompressed. The JPEG anti-forensics still amazingly applied in various circumstances, for example, concealing double JPEG compression footprints and image splicing. But the efficiency of suggested counter JPEG anti-forensic approach is improved in terms of low minimum decision error values for all anti-forensic approaches for each replacement rate including 0.10 as shown in Fig. 5. It can be noticed that the minimum decision error is high for the anti-forensic techniques $\mathcal{FD}_{Gur}$, $\mathcal{FD}_v$, $\mathcal{FD}_{Fan}$ when compared to other techniques. This is because of the explicit histogram smoothing. It is worth noting that higher value of minimum decision error signifies less forensic detectability. On the other hand, smaller values of minimum decision error indicate better forensic detectability.

The objective of the proposed work is to detect the forgeries present in an image by revealing the JPEG compression artifacts. The two classes i.e. original and forged images are considered for classification on the basis of SVM. True Positive Rate (TPR) indicates the tampered images correctly classified as tampered images. False Positive Rate (FPR) indicates the tampered images incorrectly classified as original image. Numerous existing approaches for analyzing JPEG compression artifacts are based on single scalar feature. Hence, in order to make the comparison feasible, separate ROC curves are provided for scalar-based and SVM-based machine learning detectors as illustrated in Fig. 6. The ROC curve as shown in Fig. 6 for proposed forensic algorithm (K_{MTPM}) is closer to the upper left corner in comparison to the other (scalar or SVM-based) existing techniques which depicts the highest accuracy. The accuracy achieved by the proposed approach for the UCID dataset is 99.004%. Therefore, the proposed approach provides improved forensic detectability as compared to the existing approaches upon conducting test against the JPEG anti-forensic approach FD_{Gur}.

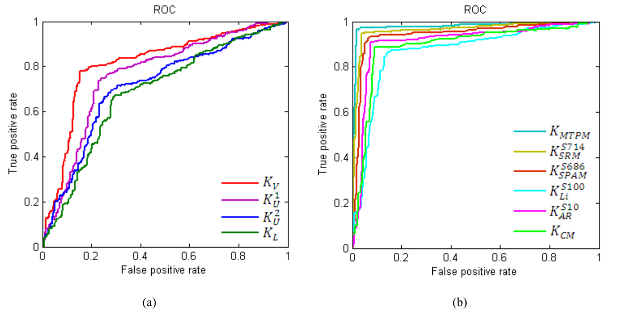


FIGURE 6. ROC curves for (a) Scalar-based forensic detectors, (b)SVM-based forensic detectors, when tested against the JPEG anti-forensic approach FD_{Gur}. It is worth noting that forensic detectability rises as the ROC curve approach to the upper left corner.

B. EXPERIMENTAL RESULTS OBTAINED ON BOSSBASE DATASET

The performance of the presented forensic approach is further validated on the BOSSBase image dataset [31]. Initially, the conversion of original raw images of BOSSBase dataset is done into 8-bit grayscale PGM images after converting them into PPM format with *UFRaw* utility. The forensic testing is done by cropping a sub-image of 512 × 512 from the center of each original high-resolution grayscale

BOSSBase image. For testing SVM-based detectors, we choose 5000 test images named as BOSSBaseTest and rest as training images named as BOSSBaseTrain from BOSSBase image database. Afterwards, these images are processed with various anti-forensic techniques in order to create the processed image datasets for evaluation. The SVM-based detectors are tested on BOSSBaseTest dataset and training is performed on the BOSSBaseTrain dataset. The strategy as used for UCID images is followed to prepare the training and testing datasets for BOSSBase images.

Fig. 7 shows the minimum decision error values for various types of JPEG anti-forensic techniques on BOSSBase dataset by considering different image replacement rates against SVM-based detectors K_{Li}^{S100}, K_{AR}^{S10}, K_{SPAM}^{S686}, K_{SRM}^{S714}, and K_{MTPM}. The proposed forensic scheme (K_{MTPM}) based on second order statistical analysis provide better results in the detection of all the considered JPEG anti-forensic techniques by providing smaller minimum decision error values. It can be observed from Fig. (5) and Fig. (7) that the results obtained on UCID dataset are quite similar with the results obtained on BOSSBase dataset. Furthermore, the SVM classifier is less sensitive to curse of dimensionality problem [43]. So, the number of dataset images has smaller effect on the efficiency of SVM classifier. Moreover, it can be observed that the minimum decision error values achieved by BOSSBase dataset are almost at equal level as that of the UCID dataset images.

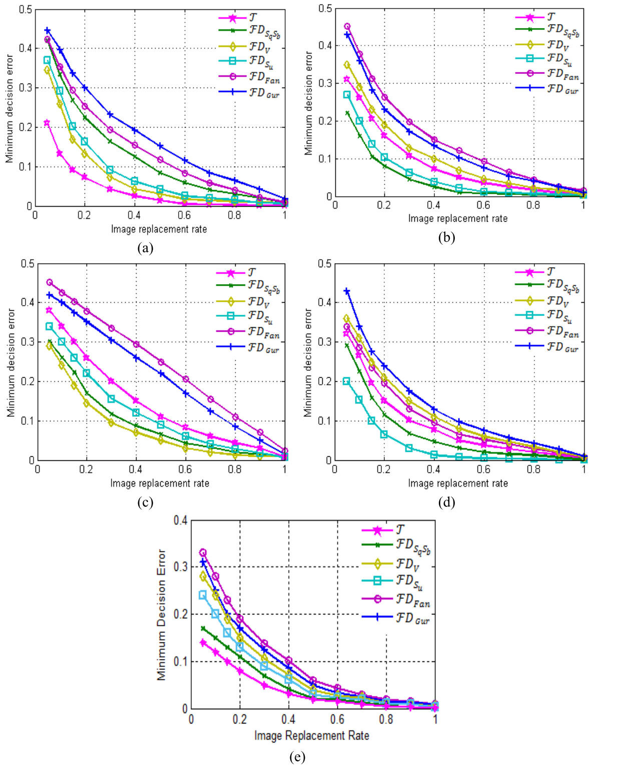


FIGURE 7. Minimum decision error based on various image replacement rates against different forgeries by considering SVM-based detectors trained on Bossbase dataset. The results are obtained on Bossbase dataset. (a) K_{Li}^{S100} [34], (b) K_{SPAM}^{S686} [36], (c) K_{AR}^{S10} [35], (d) K_{SRM}^{S714} [37] (e) Proposed (K_{MTPM}).

C. EVALUATION ON ALIGNED AND NON-ALIGNED JPEG COMPRESSED IMAGES

The further authentication of the ability of suggested forensic technique has been done by conducting a test on anti-forensically processed double JPEG compressed images. The various existing anti-forensic schemes are considered to compute the efficiency of the existing state-of-the-art double JPEG compression forensic detectors [44] and [45] and presented forensic approach.

In double JPEG compression, initially images are compressed with the quality factor QF_1 and the obtained images are further compressed with quality factor QF_2. Image cropping and alteration of content can occur during double JPEG compression. The existing anti-forensic approaches are applied on the JPEG images compressed with quality factor QF_1. The forged JPEG image obtained after applying the anti-forensic approach can be untouched or cropped with the random grid shift as per the testing conditions. Finally, the resultant image is compressed again with quality factor QF_2 to obtain the anti-forensic double JPEG compressed image.

The non-uniformity of integer periodicity map of DC coefficients is calculated by using efficient threshold detector as presented in [45]. Initially, the image is selected from UCID dataset and compressed with quality factor QF_1. Afterwards, the image is cropped by employing random shift (i, j) $\neq$ (0, 0) with $0 \leq$ i, j ≤ 7. Further, the cropped image is again compressed with QF_2 thus providing NA-DJPG compressed image. Here, the anti-forensics is done after the first compression with quality factor QF_1. Thus, various types of JPEG forgeries are created from the images of UCID dataset using the approach of [45]. Since the anti-forensic approach [27] required high computational time so approximately half of the images from the UCID Test dataset are considered by taking into account all the 100 possible combinations of quality factors QF_1 and $QF_2 \in \{50, 55, 60, 65, 70, 75, 80, 85, 90, 95\}$.

The proposed forensic detector (K_{MTPM}) and NA-DJPG detector [45] are used for testing single and double compressed JPEG images simultaneously. Further, computation of minimum decision error P_e is done for various types of JPEG forgeries. Fig. 8 shows the average of minimum decision error with respect to quality factor QF_1 with fixed value of QF_2. It can be observed that the anti-forensic approaches FD_{Gur} and FD_{Fan} shows good forensic undetectability due to explicit DCT histogram smoothing when tested against NA-DJPG detector [45]. Most of the existing JPEG forensic detectors are fooled effectively with the anti-forensic approach FD_{Fan} presented in [26]. FD_{Fan} successfully fools the NA-DJPG detector [45] with minimum decision error value near to 0.5. This is due to the fact that NA-DJPG detector is unable to sense the integer periodicity. This shows that there is need of second order statistical analysis to counter the JPEG anti-forensics. Furthermore, the proposed forensic

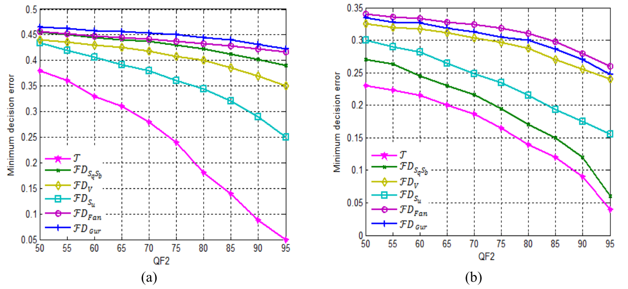


FIGURE 8. Minimum decision error based on different QF_2 values against various types of forgeries, when test is conducted on (a) NA-DJPG detector and (b) Proposed scheme K_{MTPM} on UCID dataset.

technique can also expose the gaps that are partially filled in DCT domain. It is perceived from Fig. 8 that the proposed forensic technique K_{MTPM} provides lesser values of minimum decision error for different values of quality factor QF_2. This shows that the proposed approach outperforms the existing double compression forensic approach [45] against various anti-forensic approaches.

The A-DJPG compressed images dataset is made by compressing the images of UCIDTraindataset with QF_1 and then again compressing it with quality factor QF_2 where $QF_1 \neq QF_2$. Consequently, this case consists of 90 combinations for which different sorts of JPEG forgeries are made by considering half of the UCIDTestdataset images. Fig. 9 exhibits that the introduced JPEG forensic approach provides lower values of minimum decision error as compared to A-DJPG forensic detector [44] against several existing anti-forensic techniques. The proposed forensic technique has outperformed other techniques in terms of minimum decision error. It is worth noting that lower values of minimum decision error represent a better forensic technique.

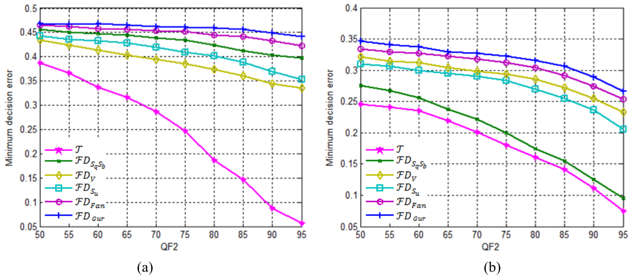


FIGURE 9. Minimum decision error based on different QF_2 values against various types of forgeries, when test is conducted on (a) A-DJPG detector and (b) proposed scheme K_{MTPM}, UCIDTest dataset.

D. EVALUATION OF PROPOSED SCHEME ON SPLICED IMAGES

The performance of the proposed scheme is evaluated on the realistic scenarios by considering spliced images. The proposed scheme comprises of three steps which includes selection of target difference image, evaluation of Markov transition matrices for both intra and inter-block DCT domain, and generation of mono-dimensional signal as shown in Fig. 1. The pixels co-relation gets disturbed during the creation of a forgery. Therefore, a second order statistical analysis based on Markov Transition Probability Matrices (MTPMs) is performed to analyse these inconsistencies. Further a mono-dimensional signal is derived by analyzing various characteristics based on MTPM of the considered image. This signal is obtained by concatenation of rows of inter as well as intra-block MTPMs. Let $\delta(n)$ indicates a mono-dimensional signal of size $(1, 648)$ based on MTPMs. This resultant mono-dimensional signal is fed into SVM classifier to distinguish between spliced and original images. Most of image splicing techniques are based on the optimization schemes with a goal of finding an optimal mapping to get back the statistics of authentic image. In the case of the spliced images, the inconsistencies occur due to variation in the intensity level at the edges by a significant value. Due to these inconsistencies there exists a relation between the spliced part and authentic part. This relation can differentiate the spliced and authentic image. The proposed approach based on second order statistical analysis is capable to evaluate these inconsistencies in the altered images.

The monodimensional signal for various spliced and original images is shown in Fig. 10. The investigation of signal $\delta(n)$ as shown in Fig. 10 outlines that an authentic image shows a smooth behavior while the spliced image processed through splicing technique demonstrates oscillating behavior as revealed in Fig. 10. (f), (h), (n), (p), (v) and (x). It can also be noticed from Fig. 10 that there is clear difference in the oscillations of mono-dimensional signal $\delta(n)$ between authentic and spliced images. Therefore, it is clear that the proposed feature is capable of detecting spliced images efficiently.

The evaluation of proposed forensic method is done by conducting numerous tests on the standard datasets such as CASIA v1.0 [46] and Columbia database [47]. The CASIA image tampering detection evaluation dataset (CITDE) provides various kinds of image for tampering detection which includes 800 authentic and 921 tampered images [46]. The Columbia dataset comprises 363 total images in formats i.e. BMP and TIFF, out of which 183 are authentic images, remaining is tampered [47]. However, the number of tampered images is more in comparison to the authentic images in both the datasets. Therefore, in order to balance the authentic and tampered images, images are randomly selected for the detection. In the proposed work, 70% of images are used for training while 30% images are used for testing. A confusion matrix summarizes the performance of classifier with respect to the testing data.

For instance, there are 800 authentic and 921 tampered images in the CASIA v1.0 dataset. In order to keep the balance, 800 authentic and 800 tampered images are considered for the experimentation, thus there are 1600 images in total for CASIA v1.0. In accordance with the 70:30 proportions for training and testing, 1120 images are used to train the classifier while the remaining 480 images are used for the

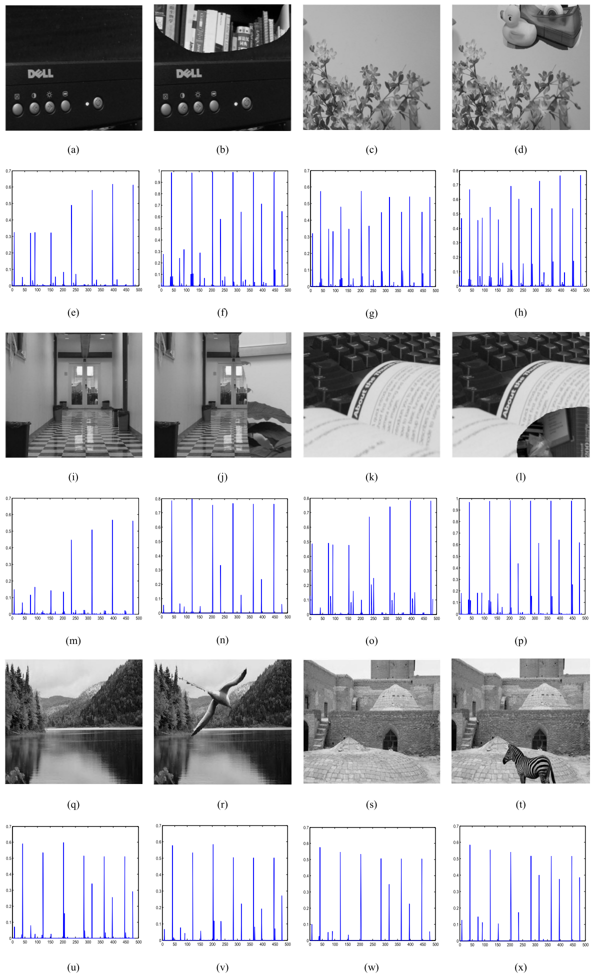


FIGURE 10. (a), (c), (i), (k), (q), (s) denote the uncompressed authenticate images and (b), (d), (j), (l), (r), (t) denote the spliced images respectively. (e), (g), (m), (o), (u), (w) and (f), (h), (n), (p), (v), (x) represent the resultant signals $\delta(n)$ for the uncompressed authenticate and spliced images respectively.

testing purpose. In a similar manner, the Columbia dataset 252 images are used to train the classifier and 108 images are used for the testing purpose. Hence, the confusion matrix is formed on the basis of 480 and 108 images to envisage the accuracy of the classifier by relating actual and predicted classes. The confusion matrix for testing images of both datasets CASIA v1.0, Columbia is shown in Table 2.

TABLE 2. Confusion matrices for the respective datasets.

CASIA v1.0	**Predicted Negative**	**Predicted Positive**	**Columbia**	**Predicted Negative**	**Predicted Positive**
Actual Negative	236	4	Actual Negative	53	1
Actual Positive	2	238	Actual Positive	1	53

The efficiency of the proposed scheme is further confirmed on the basis of ROC curve by considering various existing techniques such as Alahmadi *et al.* [48], Muhammad *et al.* [49], Hussain *et al.* [50], Aggarwal *et al.* [51] and Alahmadi *et al.* [52]. The ROC curve is plotted to depict the performance of the classifier. The ROC curve close to the upper left corner depicts the highest performance of the proposed scheme. The comparison of ROC curves for CASIA v1.0 dataset is done with [48], [49], [50] as presented in Fig. 11 (a) and with [51], [52] for Columbia dataset as presented in Fig. 11 (b).

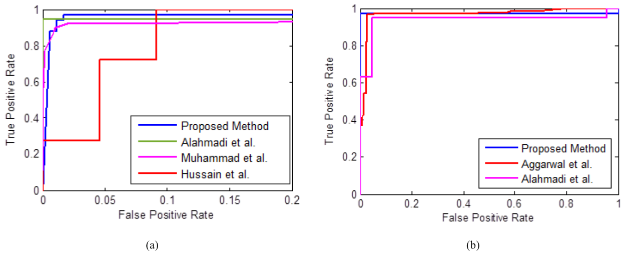


FIGURE 11. ROC curves for the various techniques evaluated on (a) CASIA v1.0 (b) Columbia datasets.

It is observed from Fig. 11 (a) and (b) that the ROC curve of the proposed approach is closer to the upper left corner for both the datasets which indicates that it achieves more accuracy as compared to the existing techniques. Moreover, it is perceived from the experimental results that the second-order statistical feature resulting from MTPM for both intra and inter-block DCT domain, outperforms the existing techniques with accuracy of 98.75% and 98.15% on CASIA v1.0 and Columbia datasets respectively. Thus the proposed method differentiates the authentic and spliced images efficiently.

Moreover, majority of methods do not implement run time analysis, as they, are not robust against post-processing operations. Instead, the proposed work overcomes these downsides by authenticating the performance with run time analysis as shown in Table 3.

TABLE 3. Run time analysis of the proposed technique on both datasets.

Datasets	**Image Size**	**Total number of images**	**Running Time (secs/image)**
CASIA v1.0	384×256	1721	0.438
Columbia	757×568 to 1152×768	363	2.364 to 2.839

IV. CONCLUSION

The first order statistical analysis based forensic detectors can be easily misguided by applying some anti-forensic techniques. Therefore, higher order statistical analysis is required to counter these anti-forensic techniques. In this paper, a higher order statistical analysis based on MTPM is performed to detect the footprints left by the dithering operation of various anti-forensic techniques. It is observed that it is difficult to hide the traces of JPEG compression completely. The proposed second order feature is capable of detecting the grainy noise introduced by dithering operation of the anti-forensic techniques. The capability of the proposed forensic technique is confirmed from the extensive experimental analysis. The proposed technique provides better detection results against various anti-forensic techniques in terms of minimum decision error, when compared to the existing techniques. This work can be further extended to design a general purpose forensic technique in order to detect various image tampering operations.

REFERENCES

[1] R. Montasari and R. Hill, "Next-generation digital forensics: Challenges and future paradigms," in *Proc. IEEE 12th Int. Conf. Global Secur., Saf. Sustainability (ICGS)*, Jan. 2019, pp. 205–212, doi: 10.1109/ICGS3.2019.8688020.

[2] O. M. Al-Qershi and B. E. Khoo, "Enhanced block-based copy-move forgery detection using k-means clustering," *Multidimensional Syst. Signal Process.*, vol. 30, no. 4, pp. 1671–1695, Oct. 2019, doi: 10.1007/s11045-018-0624-y.

[3] X. Y. Wang, C. Wang, L. Wang, L. X. Jiao, H. Y. Yang, and P. P. Niu, "A fast and high accurate image copy-move forgery detection approach," *Multidim. Syst. Sign. Process.*, vol. 31, pp. 1–27, Nov. 2019, doi: 10.1007/s11045-019-00688-x.

[4] (Apr. 2017). *FaceApp*. [Online]. Available: https://www.faceapp.com/

[5] F. Luan, S. Paris, E. Shechtman, and K. Bala, "Deep photo style transfer," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Jul. 2017, pp. 4990–4998, doi: 10.1109/CVPR.2017.740.

[6] C. Pasquini, G. Boato, and R. Bohme, "Teaching digital signal processing with a challenge on image forensics [SP Education]," *IEEE Signal Process. Mag.*, vol. 36, no. 2, pp. 101–109, Mar. 2019, doi: 10.1109/MSP.2018.2887214.

[7] G. Hudson, A. Léger, B. Niss, I. Sebestyén, and J. Vaaben, "JPEG-1 standard 25 years: Past, present, and future reasons for a success," *J. Electron. Imag.*, vol. 27, no. 4, pp. 1–19, Aug. 2018, doi: 10.1117.JEI.27.4.040901.

[8] A. W3techs.com. *Usage of Image File Formats for Websites*. Accessed: Jan. 1, 2020. [Online]. Available: http://.com/technologies/overview/image_format/all

[9] Y. Kim, J. W. Soh, and N. I. Cho, "AGARNet: Adaptively gated JPEG compression artifacts removal network for a wide range quality factor," *IEEE Access*, vol. 8, pp. 20160–20170, Jan. 2020, doi: 10.1109/ACCESS.2020.2968944.

[10] T. Bianchi and A. Piva, "Image forgery localization via block-grained analysis of JPEG artifacts," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 3, pp. 1003–1017, Jun. 2012, doi: 10.1109/TIFS.2012.2187516.

[11] E. A. A. Vega, E. G. Fernandez, A. L. S. Orozco, and L. J. G. Villalba, "Passive image forgery detection based on the demosaicing algorithm and JPEG compression," *IEEE Access*, vol. 8, pp. 11815–11823, 2020, doi: 10.1109/ACCESS.2020.2964516.

[12] M. Boroumand and J. Fridrich, "Deep learning for detecting processing history of images," *Electron. Imag.*, vol. 2018, no. 7, pp. 1–9, 2018, doi: 10.2352/ISSN.2470-1173.2018.07.MWSF-213.

[13] C. Chen, Y. Q. Shi, and W. Su, "A machine learning based scheme for double JPEG compression detection," in *Proc. 19th Int. Conf. Pattern Recognit.*, Dec. 2008, pp. 1–4, doi: 10.1109/ICPR.2008.4761645.

[14] Z. Ting and W. Rangding, "Doctored JPEG image detection based on double compression features analysis," in *Proc. ISECS Int. Colloq. Comput., Commun., Control, Manage.*, Aug. 2009, pp. 76–80, doi: 10.1109/CCCM.2009.5267984.

[15] G. Valenzise, M. Tagliasacchi, and S. Tubaro, "Revealing the traces of JPEG compression anti-forensics," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 2, pp. 335–349, Feb. 2013, doi: 10.1109/TIFS.2012.2234117.

[16] C. Pasquini, F. Perez-Gonzalez, and G. Boato, "A benford-Fourier JPEG compression detector," in *Proc. IEEE Int. Conf. Image Process. (ICIP)*, Oct. 2014, pp. 5322–5326, doi: 10.1109/ICIP.2014.7026077.

[17] C. Pasquini, G. Boato, and F. Perez-Gonzalez, "Statistical detection of JPEG traces in digital images in uncompressed formats," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 12, pp. 2890–2905, Dec. 2017, doi: 10.1109/TIFS.2017.2725201.

[18] Y. Choi, D. Kang, J. J. Hwang, and K. H. Rhee, "JPEG compression detection based on edge-corner features using SVM," in *Proc. Int. Conf. Mach. Learn. Data Sci. (MLDS)*, Dec. 2017, pp. 80–84, doi: 10.1109/MLDS.2017.25.

[19] X. Zeng, G. Feng, and X. Zhang, "Detection of double JPEG compression using modified DenseNet model," *Multimedia Tools Appl.*, vol. 78, no. 7, pp. 8183–8196, Apr. 2019, doi: 10.1007/s11042-018-6737-3.

[20] J. Li, W. Lu, J. Weng, Y. Mao, and G. Li, "Double JPEG compression detection based on block statistics," *Multimedia Tools Appl.*, vol. 77, no. 24, pp. 31895–31910, Dec. 2018, doi: 10.1007/s11042-018-6175-2.

[21] M. C. Stamm, S. K. Tjoa, W. S. Lin, and K. J. R. Liu, "Anti-forensics of JPEG compression," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process.*, Mar. 2010, pp. 1694–1697, doi: 10.1109/ICASSP.2010.5495491.

[22] M. C. Stamm, S. K. Tjoa, W. S. Lin, and K. J. R. Liu, "Undetectable image tampering through JPEG compression anti-forensics," in *Proc. IEEE Int. Conf. Image Process.*, Sep. 2010, pp. 2109–2112, doi: 10.1109/ICIP.2010.5652553.

[23] G. Valenzise, M. Tagliasacchi, and S. Tubaro, "The cost of JPEG compression anti-forensics," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, May 2011, pp. 1884–1887, doi: 10.1109/ICASSP.2011.5946874.

[24] P. Sutthiwan and Y. Q. Shi, "Anti-forensics of double JPEG compression detection," in *Proc. Int. Workshop Digit. Watermarking*, Oct. 2011, pp. 411–424, doi: 10.1007/978-3-642-32205-1_33.

[25] K. Singh, A. Kansal, and G. Singh, "An improved median filtering anti-forensics with better image quality and forensic undetectability," *Multidimensional Syst. Signal Process.*, vol. 30, no. 4, pp. 1951–1974, Oct. 2019, doi: 10.1007/s11045-019-00637-8.

[26] W. Fan, K. Wang, F. Cayre, and Z. Xiong, "JPEG anti-forensics with improved tradeoff between forensic undetectability and image quality," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 8, pp. 1211–1226, Aug. 2014, doi: 10.1109/TIFS.2014.2317949.

[27] G. Singh and K. Singh, "Improved JPEG anti-forensics with better image visual quality and forensic undetectability," *Forensic Sci. Int.*, vol. 277, pp. 133–147, Aug. 2017, doi: 10.1016/j.forsciint.2017.06.003.

[28] C. Chen and Y. Q. Shi, "JPEG image steganalysis utilizing both intrablock and interblock correlations," in *Proc. IEEE Int. Symp. Circuits Syst.*, May 2008, pp. 3029–3032, doi: 10.1109/ISCAS.2008.4542096.

[29] Y. Q. Shi, C. Chen, and W. Chen, "A Markov process based approach to effective attacking JPEG steganography," in *Proc. Int. Workshop Inf. Hiding*, Jul. 2006, pp. 249–264, doi: 10.1007/978-3-540-74124-4_17.

[30] G. Schaefer and M. Stich, "UCID: An uncompressed color image database," *Proc. SPIE*, vol. 5307, pp. 472–480, Dec. 2003, doi: 10.1117/12.525375.

[31] P. Bas, T. Filler, and T. Pevny, "Break our steganographic system: The ins and outs of organizing BOSS," in *Proc. Int. Conf. Inf. Hiding*, May 2011, pp. 59–70, doi: 10.1007/978-3-642-24178-95.

[32] G. Valenzise, V. Nobile, M. Tagliasacchi, and S. Tubaro, "Countering JPEG anti-forensics," in *Proc. 18th IEEE Int. Conf. Image Process.*, Sep. 2011, pp. 1949–1952, doi: 10.1109/ICIP.2011.6115854.

[33] S. Lai and R. Bohme, "Countering counter-forensics: The case of JPEG compression," in *Proc. Int. Workshop Inf. Hiding*, May 2011, pp. 285–298, doi: 10.1007/978-3-642-24178-920.

[34] H. Li, W. Luo, and J. Huang, "Countering anti-JPEG compression forensics," in *Proc. 19th IEEE Int. Conf. Image Process.*, Sep. 2012, pp. 241–244, doi: 10.1109/ICIP.2012.6466840.

[35] H. Zeng, X. Kang, and A. Peng, "A multi-purpose countermeasure against image anti-forensics using autoregressive model," *Neurocomputing*, vol. 189, pp. 117–122, May 2016, doi: 10.1016/j.neucom.2015.12.089.

[36] T. Pevny, P. Bas, and J. Fridrich, "Steganalysis by subtractive pixel adjacency matrix," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 2, pp. 215–224, Jun. 2010, doi: 10.1109/TIFS.2010.2045842.

[37] H. Li, W. Luo, X. Qiu, and J. Huang, "Identification of various image operations using residual-based features," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 28, no. 1, pp. 31–45, Jan. 2018, doi: 10.1109/TCSVT.2016.2599849.

[38] G. Singh and K. Singh, "Counter JPEG anti-forensic approach based on the second-order statistical analysis," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 5, pp. 1194–1209, May 2019, doi: 10.1109/TIFS.2018.2871751.

[39] T. Pevný, T. Filler, and P. Bas, "Using high-dimensional image models to perform highly undetectable steganography," in *Proc. Int. Workshop Inf. Hiding*, Jun. 2010, pp. 161–177, doi: 10.1007/978-3-642-16435-4_13.

[40] V. Holub and J. Fridrich, "Digital image steganography using universal distortion," in *Proc. 1st ACM workshop Inf. Hiding Multimedia Secur. IH&MMSec*, 2013, pp. 59–68, doi: 10.1145/2482513.2482514.

[41] R. Böhme, and M. Kirchner, "Counter-forensics: Attacking image forensics," in *Digital Image Forensics*. New York, NY, USA: Springer, 2013, pp. 327–366, doi: 10.1007/978-1-4614-0757-712.

[42] C.-C. Chang and C.-J. Lin, "LIBSVM: A library for support vector machines," *ACM Trans. Intell. Syst. Technol.*, vol. 2, no. 3, pp. 1–27, Apr. 2011, doi: 10.1145/1961189.1961199.

[43] V. Vapnik, *The Nature of Statistical Learning Theory*. New York, NY, USA: Springer, Jun. 2013, doi: 10.1007/978-1-4757-3264-1.

[44] T. Pevny and J. Fridrich, "Detection of double-compression in JPEG images for applications in steganography," *IEEE Trans. Inf. Forensics Security*, vol. 3, no. 2, pp. 247–258, Jun. 2008, doi: 10.1109/TIFS.2008.922456.

[45] T. Bianchi and A. Piva, "Detection of nonaligned double JPEG compression based on integer periodicity maps," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 842–848, Apr. 2012, doi: 10.1109/TIFS.2011.2170836.

[46] J. Dong, W. Wang, and T. Tan, "CASIA image tampering detection evaluation database," in *Proc. IEEE China Summit Int. Conf. Signal Inf. Process.*, Jul. 2013, pp. 422–426, doi: 10.1109/ChinaSIP.2013.6625374.

[47] Y.-F. Hsu and S.-F. Chang, "Detecting image splicing using geometry invariants and camera characteristics consistency," in *Proc. IEEE Int. Conf. Multimedia Expo*, Jul. 2006, pp. 549–552, doi: 10.1109/ICME.2006.262447.

[48] A. Alahmadi, M. Hussain, H. Aboalsamh, G. Muhammad, G. Bebis, and H. Mathkour, "Passive detection of image forgery using DCT and local binary pattern," *Signal, Image Video Process.*, vol. 11, no. 1, pp. 81–88, Jan. 2017, doi: 10.1007/s11760-016-0899-0.

[49] G. Muhammad, M. H. Al-Hammadi, M. Hussain, and G. Bebis, "Image forgery detection using steerable pyramid transform and local binary pattern," *Mach. Vis. Appl.*, vol. 25, no. 4, pp. 985–995, May 2014, doi: 10.1007/s00138-013-0547-4.

[50] M. Hussain, S. Q. Saleh, H. Aboalsamh, G. Muhammad, and G. Bebis, "Comparison between WLD and LBP descriptors for non-intrusive image forgery detection," in *Proc. IEEE Int. Symp. Innov. Intell. Syst. Appl. (INISTA)*, Jun. 2014, pp. 197–204, doi: 10.1109/INISTA.2014.6873618.

[51] S. Agarwal and S. Chand, "Texture operator based image splicing detection hybrid technique," in *Proc. 2nd Int. Conf. Comput. Intell. Commun. Technol. (CICT)*, Feb. 2016, pp. 116–120, doi: 10.1109/CICT.2016.31.

[52] A. A. Alahmadi, M. Hussain, H. Aboalsamh, G. Muhammad, and G. Bebis, "Splicing image forgery detection based on DCT and local binary pattern," in *Proc. IEEE Global Conf. Signal Inf. Process.*, Dec. 2013, pp. 253–256, doi: 10.1109/GlobalSIP.2013.6736863.

AMIT KUMAR received the B.Tech. degree in electronics and communication engineering from the Amritsar College of Engineering and Technology, Amritsar, in 2011, and the M.Tech. degree in electronics and communication engineering from Uttar Pradesh Technical University, in 2015. He is currently pursuing the Ph.D. degree with the Department of Electronics and Communication Engineering, Thapar Institute of Engineering and Technology, Patiala. His research interests include signal processing and image processing.

GURINDER SINGH received the Ph.D. degree in electronics and communication engineering from the Thapar Institute of Engineering and Technology, Patiala, India. He is currently a Postdoctoral Fellow with IIT, Ropar. His research interests include digital image forensics and anti-forensics.

ANKUSH KANSAL received the B.Tech. and M.Tech. degrees in electronics and communication engineering from PTU, Jalandhar, and the Ph.D. degree in wireless communication from the Thapar Institute of Engineering and Technology, Patiala. He is currently working as an Associate Professor with the Thapar Institute of Engineering and Technology. He has published 45 research articles in refereed international journals, international conference, and national conference. His research interests include networking, wireless communication, image processing, and embedded systems. He is a Life Time Member of ISTE.

KULBIR SINGH was born in Batala, Punjab, India. He received the B.Tech. degree from PTU, Jalandhar, in 1997, and the M.E. and Ph.D. degrees from the Thapar Institute of Engineering and Technology, Patiala, in 2000 and 2006, respectively. He is currently working as a Professor with the Department of Electronics and Communication Engineering, Thapar Institute of Engineering and Technology. He has published more than 70 research articles in national and international journals/conference proceedings. His research interests include fractional transforms, signal processing, image processing, and image forensics. He was a recipient of the Best Paper Award for the IETE Journal of Education, in 2008.