Vol.66: e23230384, 2023
https://doi.org/10.1590/1678-4324-2023230384
ISSN 1678-4324 Online Edition

*Article - Engineering, Technology and Techniques*

# An Improved JPEG Image Blocking Artifact Detector

**Ashish Soni**[1]
https://orcid.org/0009-0000-7891-3123

**Shivani Sharma**[2]
https://orcid.org/0000-0001-6652-2651

**Dinesh Bhardwaj**[3]
https://orcid.org/0000-0003-1138-6167

**Sachin Kumar**[4*]
https://orcid.org/0000-0003-3949-0302

[1]Shri Shankaracharya Institute of Technology & Management, Department of Electrical & Electronics Engineering, Raipur, Chhattisgarh, India; [2]Dr BR Ambedkar National Institute of Technology, Department of Information Technology, Jalandhar, Punjab, India; [3]Thapar Institute of Engineering & Technology, Department of Electronics & Communication Engineering, Patiala, Punjab, India; [4]South Ural State University, Big Data and Machine Learning Lab, Chelyabinsk, Russia.

Editor-in-Chief: Alexandre Rasi Aoki
Associate Editor: Fabio Alessandro Guerra

Received: 19-Apr-2023; Accepted: 05-Jun-2023

*Correspondence: kumars@susu.ru; Tel.: +79512471669 (S.K.).

## HIGHLIGHTS

- Authentication of forged digital images posted online is very important.
- An improved JPEG image blocking artifact detector is proposed.
- The proposed artifact detector has outperformed the existing methods.
- Authenticity of digital images posted online can be verified using proposed method.

**Abstract:** Sharing digital images on social media has become very common these days. People must check for authenticity to share images on social media websites. The shared image may be forged intentionally or unintentionally and can defame someone's reputation, leading to severe events, such as public riots. Thus, authentication of digital images which are posted on social media websites is of paramount importance. Our social media should be intelligent enough to check on these forged images such that no false information spreads around society. Many image forgery detection algorithms have been used by big social groups based on JPEG compression artifacts, but these may not work well in the presence of anti-forensics. JPEG compression is the most widely used standard in social media these days. Two important artifacts, quantization and blocking artifacts, are being exploited by various experts for forensic analysis. JPEG anti-forensic techniques clear away these artifacts to fool forensic detectors. This work presents a novel technique derived from the inter-block interdependence of DCT coefficients for ferreting out JPEG-blocking artifacts in the presence of anti-forensics. In the case of JPEG images, the cropping operation shifts the blocking artifacts within the block, changing the inter-block interdependence. We propose to take advantage of this change to ferret out the blockiness in an image that will help the forensic analyst detect forgery. The proposed method can detect blocking artifacts even if anti-forensic operations are applied and take the intelligence of social media to a step up. A set of different and reproducible experiments have been conducted over a large set of images. It has been observed that the proposed detector outperformed the existing ones in ferreting out blocking artifacts in altered (anti-forensically) JPEG images.

**Keywords:** Blocking artifacts; Image-forensics; JPEG Compression.

## INTRODUCTION

Nowadays, social media is an unteachable truth of everyone's life. We all have digital cameras and phones; we click a pic from somewhere and post it on social media for fun. Sometimes, we capture images for ease of doing work too. However, in this digital era, images can be quickly tempered with evolving technology as we see in our day-to-day life. One from nowhere can take and alter these pictures to spread false information, defame someone, etc. Furthermore, this can lead to severe problems and threats to society or individuals. Therefore it is equally essential for us to be responsible while posting any image. Also, our social media should be intelligent enough to detect such images and block them before they make any undesirable impact on society. The biggest question is how we can prove the image's authenticity.

One of the primarily used compression methods is JPEG compression. Generally, a forger tempers the image and saves it in the compressed JPEG format. It is widely accepted that JPEG compression leaves behind two essential characteristics that can be used to exploit the image's authenticity. The two characteristics are quantization artifacts and blocking artifacts. Let us dig into these characteristics to understand what these artifacts mean. As the name suggests, the blocking artifacts represent the pixel discontinuities across the boundaries of different blocks. These artifacts are generated when each non-overlapping block (8 x 8 pixels) of the given image is transform-coded independently. Because of this mutually exclusive encoding of the 8 x 8 blocks of the given image, pixel discontinuities appear near the decompressed image's block boundaries. This particular blockiness is known as JPEG blocking artifacts [1]. The second characteristic, named quantization artifacts, also known as DCT histogram artifacts, is generally due to the quantization process involved in transform coding.

These artifacts appear in the histogram of a particular DCT sub-band of a given image. For any image under one JPEG compression, the corresponding coefficient DCT sub-band is gathered around the integer multiples, according to quantization step size, and a very comb-like pattern can be perceived. However, in case any image went through several JPEG compression, different patterns can be observed in the DCT-histogram depending on the values of primary and secondary quality factors [2]. This blockiness/blocking artifacts can be easily traced [1,3] and can be exploited to identify whether the image provided is JPEG compressed. In [4], the authors observed the inconsistency in the blocking artifacts in the forged area. The (BACM) matrix, i.e., blocking artifacts characteristics matrix, was developed to identify such inconsistencies and used for tempering detection.

The DCT histogram artifacts can be used to estimate quantization step size [1,5]. One can also exploit these artifacts for the detection of image forgery [2,6]. Above mentioned JPEG compression-based forensic detectors are all old-school theories after the research proposed by Stamm. [7] in which they introduced a method for hiding the traces of DCT histogram/quantization artifacts by exploiting dither which is a particular anti-forensic noise. Later on, they also suppressed the blocking artifacts with the help of median filtering and white Gaussian noise [8].

In [9], another approach with the idea of Shrink and Zoom, also called (SAZ) attack to cheat the detectors based on double-JPEG compression artifacts. Another method proposed by Barni and coauthors [10] came into the picture to cheat manyfold JPEG compression detectors. The authors presented to reshape the histograms of various DCT-sub-bands of several corresponding images to match their statistical properties with the DCT histograms of corresponding single JPEG compressed images. Above mentioned work is further carried out by Fan and coauthors [11] in which the authors refined the visceral quality of images that are amended or modified anti-forensically while keeping the forensic undetectability intact. The technique uses four steps: first, deblocking is done mainly by agglomerating a dither noise in the frequency domain (DCT), also known as a total variation (TV) based scheme. Furthermore, total variation-based deblocking is done following then de-calibration. Further, [12] presented detectors that exploited DCT coefficients distributed based on FSD, i.e., the first significant digit. The dissemination of the first significant digit of both images, i.e., single or double JPEG compressed images, is restored to its previous state, i.e., FSD distribution of an uncompressed image. Due to the above-mentioned anti-forensic techniques, the forgery detection accuracy decreases to a large extent. Hence, it has become essential for a forensic to counter these anti-forensic techniques. First, Lai and coauthors [13] proposed two different detectors for countering the anti-forensic method [7]. The first detector exploits the fact that the DCT coefficients exhibiting high frequency tend to remain unchanged or least altered due to anti-forensic operation. The secondary detector uses the discrepancy between the variance of high-frequency DCT coefficients of a given image and the high-frequency DCT coefficients of its cropped version.

After that, Valenzise and coauthors [14] came up with a new approach to defy the scheme presented by Stamm and coauthors [7]. The authors noticed that in the spatial domain, the presence of grainy occurs because of the agglomeration of anti-forensic dither in the DCT domain. Another trending topic of the present era is machine learning. A Machine learning-based approach is used in [15] to ferret out the dithering-based anti-forensic operations. Bhardwaj and coauthors [16] introduced a technique for blocking artifacts detection by effectively utilizing the DCT coefficients-based correlation between two spatially adjoined image blocks. The authors exploited that blocking artifacts shift within the 8 x 8 block when an image is cropped. Haodong Li and coauthors [17] proposed another machine-learning approach based on reduced SRM features for classifying various image operations as well as anti-forensic operations. Recently, Kumawat and coauthors proposed a novel and robust technique [18] for identifying the JPEG images which are saved in uncompressed format (JPEG-U images). The authors exploited the change in the probability distribution of DCT coefficients due to cropping. The method also performs well in detecting JPEG-U images even if post-processing operations like median filtering, histogram equalization etc, are applied. In [19], Bhardwaj and coauthors exploited the spread of DCT coefficients around integer multiple of quantization step size for detecting dithering-based JPEG anti-forensics.

The above literature study shows that the existing methods are effective in detecting anti-forensic operations [7] and [11]. However, detecting anti-forensic operations [8] with acceptable accuracy is still an open challenge. This paper proposes an improved JPEG blocking artifact detector which detects the anti-forensically altered images [8, 11] by using a set of the total variance of differently cropped versions and their correlation to get a unique value for the original image and anti-forensically altered image. Hence, the main contribution of this paper is an improved JPEG-blocking artifact detector, which can detect blocking artifacts in the presence of different anti-forensic operations [8,11] which may further help in avoiding the spread of fake images on social media.

## BACKGROUND

This section presents various JPEG-blocking artifact detection techniques over time. First, a brief discussion of these techniques is provided, followed by a discussion on different ways of suppressing these blocking artifacts.

### A Method for Detecting Blocking Artifacts in JPEG Images

The technique for detecting blocking artifacts in JPEG images is proposed by Z. Fan and coauthors [1]. The discrepancy in adjacent (spatially) pixels is calculated for all inside-out pixels, i.e., 8 x 8 boundary pixels and pixels inside the block. It came into the limelight that the pixel discrepancy inside and along the block boundaries is similar for uncompressed images. It is higher across the block than within the block for compressed images; this can be represented with the mathematical expression below:

$$k_z = \sum_{n} |H_i(n) - H_{ii}(n)| \tag{1}$$

Where, $H_i(n)$ represents the normalized form of pixel's histograms discrepancy existing in the block, and $H_{ii}(n)$ represents the normalized form of histograms of pixel discrepancy between the blocks. Another method presented by W. Fan and coauthors [3], where the evaluation of weighted gradient values is done with respect to each cluster of four adjacent pixels to the other side of the block boundaries. An image as well as its tapered also called as a calibrated state $X_{cat}$, this can be expressed as:-

$$\overset{\lambda}{K_W} = \left|B_{gr}^{\lambda}(X) - B_{gr}^{\lambda}(X_{cat})\right| \tag{2}$$

Here, $B_{gr}^{\lambda}$ is gradient-aware blockiness [20].

Various observations could be recorded for different values of λ. In both mentioned techniques, we get a blocking signature measure, and we set a threshold for comparison to discriminate the uncompressed image and the modified image (JPEG compressed).

## A Method for Detecting Blocking Artifacts in JPEG Images

For Bluffing forensics detectors for JPEG compression, Stamm and coauthors [7] proposed a method to minimize the blocking artifacts in JPEG images. In this process, the image is median filtered accompanied by the incorporating white Gaussian noise; this can be expressed as

$$Y=med(X) + N \tag{3}$$

Here, X is the original image, med (.) stands for the median filtering operation, and N denotes the white Gaussian noise (zero mean).

The size of the window with respect to the median filter and Gaussian noise variance has to be chosen quite carefully by considering the JPEG image's quality. The filter window size and variance should be large enough to suppress the blocking artifacts from low-quality JPEG images (small quality factor). Note that using a large window size and high variance Gaussian noise degrades the qualitative standard of the resulting image. Similarly, W. Fan and coauthors [11] proposed a new idea to suppress blocking artifacts in JPEG images. The main focus of this technique is to obtain a better perceptual quality of the altered image (anti-forensically). This technique implies minimization based on the constraining of the total variation.

$$X^* = \underset{X\in V}{argmin}(TV_b(X) + \alpha C(X)) \tag{4}$$

Here, X denotes the input image to be processed, $X^*$ means the processed resulting image, $TV_b(.)$ represents the total variation, and C(.) Energy term used to estimate blocking in JPEG with $\alpha > 0$ as a parameter for regularisation. The projection sub-gradient method is an effective way to deal with this minimization problem. U (constraint image space) is determined as the prepared image's DCT coefficient existing in the same or neighboring bins similar to an unaltered image, which returns an image with good perceptual quality.

## Proposed Improved Blocking Artifact Detection Method

JPEG anti-forensic techniques [8, 11] primarily aim to abolish artifacts caused due to blocking and DCT histogram artifacts out from a single JPEG compressed image so that the resulting image is expected to follow all the characteristics of a genuine uncompressed image. The resulting images are known as anti-forensically altered uncompressed images.

In this work, we present an improvised version of a JPEG-blocking artifact detector to segregate the original uncompressed images from anti-forensically altered uncompressed images.

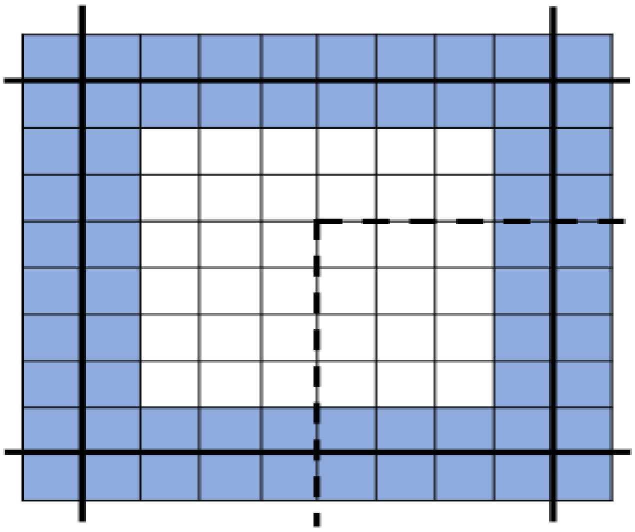

Figure 1.a

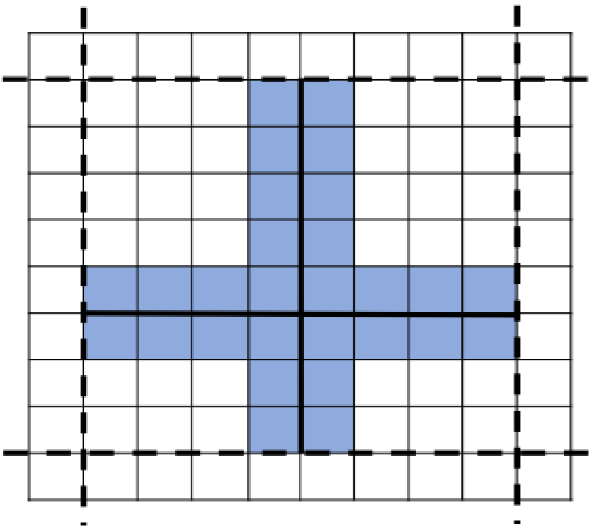

Figure 1.b

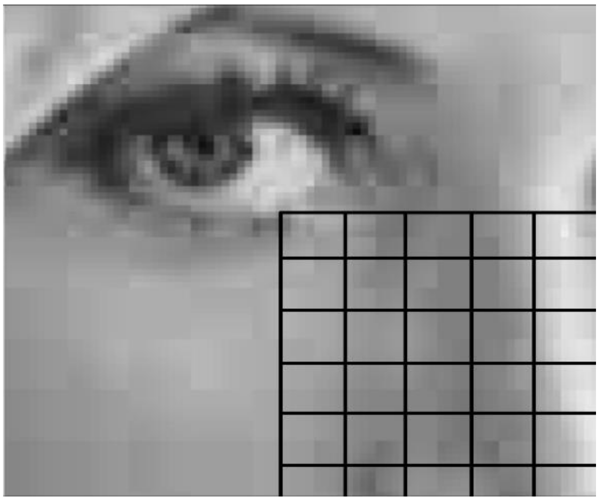

Figure 1.c

**Figure 1.** Shifting of JPEG blocking artifacts due to cropping (Figure 1a to Figure 1b to Figure 1c)

A genuine uncompressed, unaltered image does not carry any JPEG-blocking artifacts, unlike JPEG compressed, which carries JPEG-blocking artifacts. The minute traces of blocking artifacts are still present even if the JPEG compressed image undergoes another anti-forensic operation known as a deblocking step. We proposed an improved blocking artifact detector by tracing these minute remnants of the deblocking step. The proposed algorithm is described below.

Blocking artifacts of a compressed JPEG image appear in pixel discontinuities, coordinated over the edges of the 8 x 8 block boundaries. These coordinates can be altered by cropping the image. It is illustrated in Figure 1a and Figure 1b, in which the darkened lines represent the border of an 8 x 8 block within an image, whereas the dotted lines represent the cropping of an image. From this illustration, we can easily understand how the blocking artifacts near the block boundaries shift within the block after cropping. It can be further understood with the help of Figure 1c, where dark lines denote the block boundaries of an image after cropping.

A given image of dimension r x c pixels are distributed over mutually exclusive 8 x 8 pixel blocks; further, discrete cosine transform (DCT) is evaluated with respect to each block.

Let A denote the (x, y)$^{th}$ sub-band DCT coefficient in the image's (m, n)$^{th}$ block, as shown in Figure 2 where m = 1,2,….,r/8, n = 1,2,…..,c/8,  and x, y = 1,2,….,8.

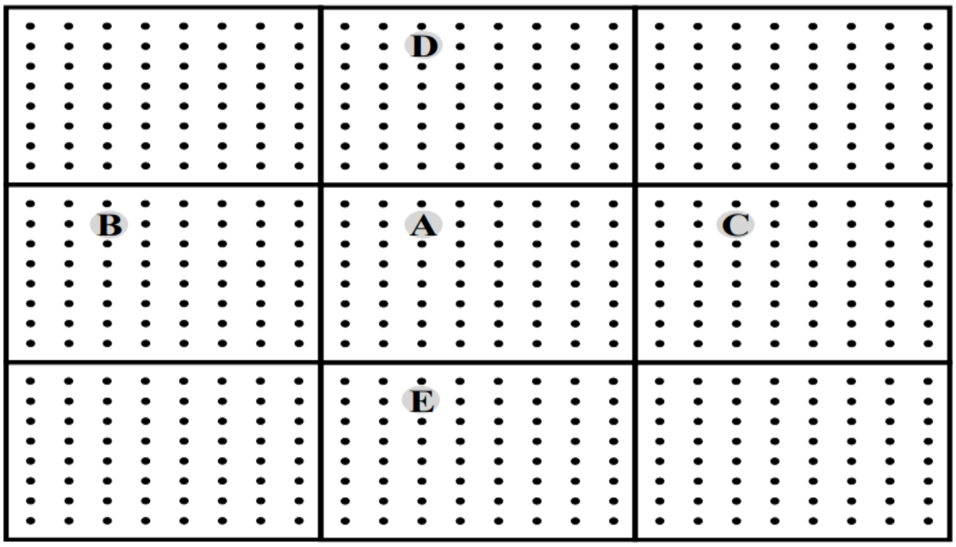

**Figure 2.** DCT coefficients in the adjacent 8 × 8 blocks

The variation in the (x, y)$^{th}$ sub-band DCT coefficient in the blocks adjacent to the (m, n)$^{th}$ block is given as

$$V_{m,n}(x,y) = ((B + C - 2A)^2 + (D + E - 2A)^2)^{1/2} \qquad (5)$$

Here notations B, C, D, and E represent the (x, y)th sub-band DCT coefficients in four spatially adjoined blocks. This variation directly depends on the correlation of DCT coefficients. The more inter-block interdependence, the less variation, and vice versa. The average variation in the (x, y)th sub-band is presented as:

$$\bar{V}(x,y) = \frac{1}{N}\sum_{m-1}^{r/8}\sum_{n-1}^{c/8} V_{m,n}(x,y) \tag{6}$$

Here, N is the number of 8 x 8 blocks.

A cropped version of the image can be obtained by slicing initial rows and columns (which lies in the range of 1-7), and hence the average variation $\bar{V}(x,y)$ is computed for every DCT subband of the cropped image. Due to the interdependence between the blocks in the natural image, values obtained from both original and cropped versions are similar in an uncompressed image. In contrast, in an anti-forensically altered image, JPEG blocking artifacts or their residuals are present, which in turn gives a significant difference between average variation $\bar{V}(x,y)$for the original uncompressed image and average variation $\bar{V}(x,y)$ of its cropped version. This phenomenon is resulted due to shifting of blocking artifacts or their residual. The feature proposed by Bhardwaj and coauthors [16] is given as

$$S(x,y) = \left|\frac{\bar{V_c}(x,y) - \bar{V}(x,y)}{\bar{V}(x,y)}\right| \tag{7}$$

The authors cropped the image by removing 4 rows and 4 columns to extract the residual from the image. We used three more ways of cropping to further extract the blocking artifacts or their residuals to enhance the detectability of the algorithm.

$$U(x,y) = \left|\frac{\bar{V_c}(x,y) - \bar{V}(x,y)}{\overline{V_{c12}}(x,y)}\right| \tag{8}$$

$$X(x,y) = \frac{(\overline{V_{c4}}(x,y) - \overline{V_{c8}}(x,y))^2}{\bar{V}(x,y)} \tag{9}$$

$$T(x,y) = \frac{(\overline{V_{c12}}(x,y) - \overline{V_{c16}}(x,y))}{\overline{V_{c12}}(x,y)} \tag{10}$$

Here, $V_{c4}$, $V_{c8}$, $V_{c12}$ and $V_{c16}$ are different versions of Vc with 4 x 4 pixels, 8 x 8 pixels, 12 x 12 pixels & 16 x 16 pixels sliced.

$$F = \left(\left(\left|\sum (U - (X - T))^2\right|\right)^{1/2}\right)^{1/2} \tag{11}$$

Here, $U = \sum_{x=1}^{8}\sum_{y=1}^{8} U(x,y)$, $X = \sum_{x=1}^{8}\sum_{y=1}^{8} X(x,y)$, and $T = \sum_{x=1}^{8}\sum_{y=1}^{8} T(x,y)$.

By combining U, X, and T, we have formulated a new feature, F, which gives an optimum value for detecting residuals in the image. After all this computation, finally, we combine F and S to boost our algorithm so that it can give impeccable accuracy in the detection of JPEG as well as anti-forensically altered images. Finally, the proposed blockiness measure, Z, is mathematically expressed as:

$$Z = \left|\left(\frac{3S}{F-3}\right)F\right| \tag{12}$$

Here, $S = \sum_{x=1}^{8}\sum_{y=1}^{8} S(x,y)$

This value represents the blockiness measure given by the improved blocking artifact detector, which will be low for original uncompressed images and high for JPEG/anti-forensically altered uncompressed images. Therefore, proper threshold selection can help in easily categorizing genuine uncompressed images from JPEG and anti-forensically altered uncompressed images.

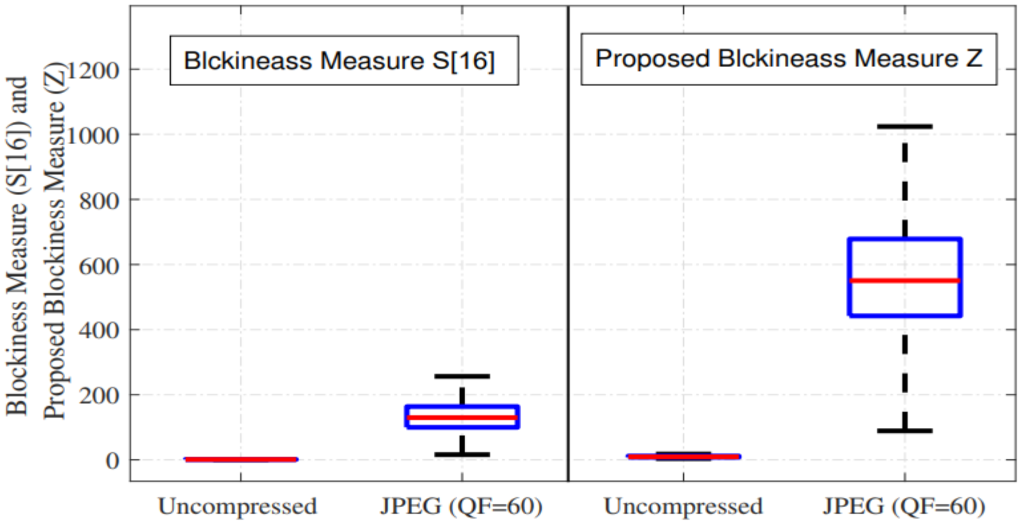

**Figure 3.** Box plot of comparative analysis

We conducted a set of experiments to claim the performance of the proposed improvised detector over the existing blocking artifact detector. For this, two different sets, each of 1338 images, are formed. The first set contains original/real uncompressed gray-scale images taken from the UCID database. The second set of images is generated by compressing the images in the first set with a quality factor 60. Then the blockiness feature S (proposed by Bhardwaj and coauthors [16] and the proposed improved blockiness feature Z is evaluated (by Eq. 12) for every image present in the datasets. The box plots for both the blockiness features (S and Z) for the considered datasets are shown in Figure 3. The figure shows that the gap between the blockiness feature for genuine uncompressed images and that of JPEG images is more in the case of proposed blockiness measure Z than the feature proposed in [16]. It confirms that the proposed blockiness measure (Z) is more potent in detecting blocking artifacts than the feature proposed in [16].

## EXPERIMENTS AND RESULTS

Several experiments were conducted to evaluate the scheme's performance proposed in this work, i.e., blocking artifact detector to differentiate original unaltered and uncompressed images from those that are anti-forensically changed and uncompressed images [8, 11]. The considered dataset and performance measuring matrix adopted for impartial differentiation is the same as explained in [16]. The dataset contains 4338 images, which are uncompressed grey-scale images. Out of these, 3000 images belong to Boss Base 1.01 [22], and others are from the UCID [21] database. The performance of the proposed detectors has been compared with two benchmark JPEG blocking artifacts detectors [1, 3]. The parameter λ = 1 is considered in the case of blocking artifact detector [3]. In the case of the detector proposed in [16], the cropping is done in horizontal and vertical directions by a factor of 4.

The JPEG compression is applied to all the images in the dataset. Five quality factors, i.e., QF={40,50,60,70,80}, are considered for performance evaluation. The anti-forensic operations [3, 8] are applied on resulting JPEG images to generate uncompressed images which are being modified anti-forensically. In the case of [8], the window size 3 x 3 is considered for the median filtering operation. The mean and variance of white Gaussian noise are zero and two, respectively. Hence, 11 different datasets are produced, each with 4338 images. Out of these 11 datasets, one set comprised original unaltered uncompressed images, whereas the remaining 10 datasets contain the modified, i.e., anti-forensically altered uncompressed images.

Initially, the proposed improved blocking artifact detector and the considered detectors are analyzed in terms of performance by plotting the receiver operating characteristic (ROC) curve. Firstly, we merged the 4330 genuine uncompressed images with an equal number of anti-forensically altered uncompressed images to create a balanced dataset. 433 images are randomly selected from ten different sets of anti-forensically altered uncompressed images to create 4330 anti-forensically altered uncompressed images.

After that, we computed the blocking artifact for the proposed and considered detectors with respect to all images present created balanced dataset, and the related ROC curves are present in Figure 4. The ROC plot distinctly shows that the proposed improved blocking artifact detector has outperformed all the considered detectors in segregating original uncompressed images from anti-forensically altered uncompressed images.

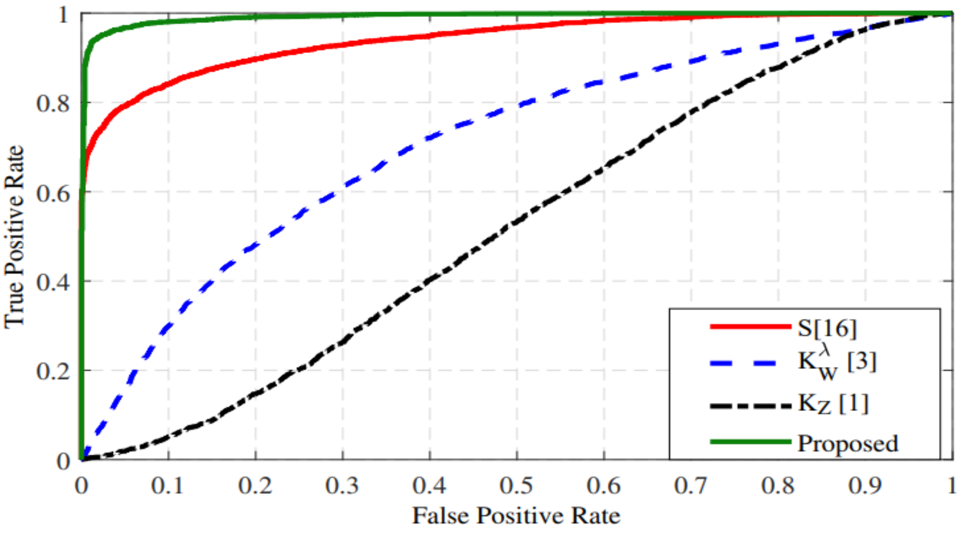

**Figure 4.** Receiver operating characteristic (ROC) curves for various blocking artifacts detectors

Next, the performance of all the blocking artifact detectors is examined in detail in terms of a parameter known as true positive rate (TPR). Thresholds corresponding to false-positive rate (FPR) equal to 0.1 are computed for the four considered detectors.

Here, TPR shows the ratio of anti-forensically altered uncompressed images identified as containing blocking artifacts to the total number of anti-forensically altered uncompressed images (4338). It should be as high as possible. The FPR represents the ratio of genuine uncompressed images that contain blocking artifacts to the total available (4338) of genuine uncompressed images. The TPR is computed for all the 10 datasets of anti-forensically altered images using the calculated thresholds. The PSNR values (in dB) in the table represent the average peak signal-to-noise ratio of the anti-forensically altered images w.r.t. the corresponding JPEG images. It indicates the perceptual degradation of an image due to the application of anti-forensic operations.

It is distinctly observed from the corresponding TPR values depicted in Table 1 and Table 2 that the anti-forensic methods [8, 11] dupe the detector in [1]. Other detectors in [3] and [16] give an average performance in correspondence of the compressed images with small quality factors (QF = 40 and 50) and degrade more and more as the JPEG quality factor increases. The proposed method outperforms all the considered blocking artifact detectors and performs consistently across all quality factors.

**Table 1.** TPR and PSNR values for considered blocking artifact detectors mentioned in [8]

| Quality Factor | PSNR (dB) | $K_z$[1] | $K_w^\lambda$[3] | S[16] | Proposed Method |
|---|---|---|---|---|---|
| 40 | 32.05 | 0.09 | 0.88 | 0.97 | 0.99 |
| 50 | 32.25 | 0.04 | 0.73 | 0.91 | 0.99 |
| 60 | 32.32 | 0.02 | 0.50 | 0.78 | 0.98 |
| 70 | 32.37 | 0.01 | 0.22 | 0.51 | 0.98 |
| 80 | 32.51 | 0.02 | 0.08 | 0.22 | 0.96 |

**Table 2.** TPR and PSNR values for considered blocking artifact detectors mentioned in [11]

| Quality Factor | PSNR (dB) | $K_z$[1] | $K_w^\lambda$[3] | S[16] | Proposed Method |
|---|---|---|---|---|---|
| 40 | 37.02 | 0.09 | 0.10 | 0.99 | 0.99 |
| 50 | 37.43 | 0.08 | 0.13 | 0.99 | 0.98 |
| 60 | 37.75 | 0.08 | 0.15 | 0.99 | 0.97 |
| 70 | 38.25 | 0.07 | 0.14 | 0.98 | 0.96 |
| 80 | 38.97 | 0.07 | 0.13 | 0.98 | 0.94 |

In the case of anti-forensic methods [11], the proposed and [16] are the only robust detectors that produce good concordant results for all the considered quality factors of JPEG compression. The performance of the proposed detector is almost consistent with an increase in the quality factor. It slightly decreases in the proposed method and significantly decreases in other considered detectors in the case of

Stamm and coauthors anti-forensic operation [8]. This may be due to the more aggressive deblocking operation applied in the case of [8] to remove the JPEG-blocking artifacts.

To the best of our knowledge, other than the machine learning-based method [17], none of the detectors reported in the literature can identify the traces of blockiness in those images which are altered anti-forensically with either of the techniques presented in [8] or [11] with the accuracy offered by the proposed detector.

## CONCLUSION

This paper presented a blocking artifact detector for determining the traces of blocking artifacts in JPEG images, especially when processed using anti-forensic methods. The detector is elicited from the inter-block interdependence of DCT coefficients. The proposed detector performed superior to previous detectors during experimental analysis. Another finding from the study of this detector is that it is efficient in ferreting out images altered with JPEG anti-forensic techniques. It will support the forensic analyst in designing a robust image forgery detection technique for social media images in an anti-forensics presence. The limitation of the proposed detector is that it does not consider the possibility of the presence of a shrink and zoom (SAZ) attack.

**Funding**: This research received no external funding.
**Acknowledgments:** Not Applicable
**Conflicts of Interest:** The authors declare no conflict of interest.

## REFERENCES

1. Fan Z, De-Queiroz RL. Identification of bitmap compression history: JPEG detection and quantizer estimation. IEEE Trans. Image Proc. 2003 Feb; 12(2):230-5.
2. Lin Z, He J, Tang X, Tang CK. Fast, automatic and fine-grained tampered JPEG image detection via DCT coefficient analysis. Patt. Recogn. 2009 Nov; 42(11):2492-501.
3. Fan W, Wang K, Cayre F, Xiong Z. A variational approach to JPEG anti-forensics. In: 2013 IEEE International Conference on Acoustics, Speech and Signal Processing. 2013 May 26-31; Vancouver, BC, Canada: IEEE; 2013. p.3058-3062.
4. Luo W, Qu Z, Huang J, Qiu G. A novel method for detecting cropped and recompressed image block. In: 2007 IEEE International Conference on Acoustics, Speech and Signal Processing. 2007 Apr 15-20; Honolulu, HI, USA: IEEE; 2007. p. 217-220.
5. Luo W, Huang J, Qiu G. JPEG error analysis and its applications to digital image forensics. IEEE Trans. Inform. Foren. Sec. 2010 Sep; 5(3):480-91.
6. Bianchi T, Piva A. Image forgery localization via block-grained analysis of JPEG artifacts. IEEE Trans. Inform. Foren. Sec. 2012 Jun; 7(3):1003-17.
7. Stamm MC, Tjoa SK, Lin WS, Liu KJR. Anti-forensics of JPEG compression. In: 2010 IEEE International Conference on Acoustics, Speech and Signal Processing. 2010 Mar 14-19; Dallas, TX, USA: IEEE; 2010. p.1694-7.
8. Stamm MC, Liu KJR. Anti-forensics of digital image compression. IEEE Trans. Inform. Foren. Sec. 2011 Feb; 6(3):1050-65.
9. Sutthiwan P, Shi YQ. Anti-forensics of double JPEG compression detection. In: 10th International Workshop Digital Forensics and Watermarking. 2011 Oct 23-26; Atlantic city, NJ, USA: Springer; 2011.p. 411-424.
10. Barni M, Fontani M, Tondi B. Universal counterforensics of multiple compressed JPEG images. In: 13th International Workshop Digital Forensics and Watermarking. 2014 Oct 1-4; Taipei, Taiwan: Springer; 2015. p.31-46.
11. Fan W, Wang K, Cayre F, Xiong Z. JPEG anti-forensics with improved tradeoff between forensic undetectability and image quality. IEEE Trans. Inform. Foren. Sec. 2014 Apr; 9(8):1211-26.
12. Pasquini C, Comesana-Alfaro P, Perez-Gonzalez F. Transportation-theoretic image counterforensics to first significant digit histogram forensics. In: IEEE International Conference Acoustics, Speech and Signal Processing. 2014 May 04-09. Florence, Italy: IEEE; 2014. p. 2699-703.
13. Lai S, Bohme R. Countering counter-forensics: The case of JPEG compression. In: 13th International Conference on Information Hiding. 2011 May 18-20. Prague, Czeck Republic: Springer; 2011. p.285–98.
14. Valenzise G, Tagliasacchi M, Tubaro S. Revealing the traces of JPEG compression anti-forensics. IEEE Trans. Inform. Foren. Sec. 2013 Feb; 8(2):335-49.
15. Li H, Luo W, Huang J. Countering anti-JPEG compression forensics. In: 19th IEEE International Conference on Image Processing; 2012 Sep 30- Oct 03; Orlando, FL, USA: IEEE; 2013. p.241-244.
16. Bhardwaj D, Pankajakshan V. A JPEG blocking artifact detector for image forensics. Sig. Proces.: Image Comm. 2018 Oct; 68:155-61.

17. Li H, Luo W, Qiu X, Huang J. Identification of various image operations using residual-based features. IEEE Trans. Circuits Sys. Video Tech. 2018 Dec; 28:31–45.
18. Kumawat C., Pankajakshan V. A robust JPEG compression detector for image forensics. Sig. Proces.: Image Comm. 2020, 89, 116008.
19. Bhardwaj D, Pankajakshan V. An approach to expose dithering-based JPEG anti-forensics. Foren. Sci. Intern. 2021, 328, 111040.
20. Ullerich C, Westfeld A. Weaknesses of MB2. In: 6th International Workshop on Digital Watermarking. 2007 Dec 3-5; Guangzhou, China: Springer; 2008. p.127-142.
21. Schaefer G, Stich M. UCID - an uncompressed colour image database. In: Proceedings of the SPIE. 2003 Dec 18. San Jose, California, USA: Online; 2004. p. 472480. https://doi.org/10.1117/12.525375
22. Bas P, Filler T, Pevny T. Break our steganographic system: The ins and outs of organizing boss. In: 13th International Conference on Information Hiding. 2011 May 18-20. Prague, Czech Republic: Springer; 2011. p.59-70.

© 2023 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY NC) license (https://creativecommons.org/licenses/by-nc/4.0/).