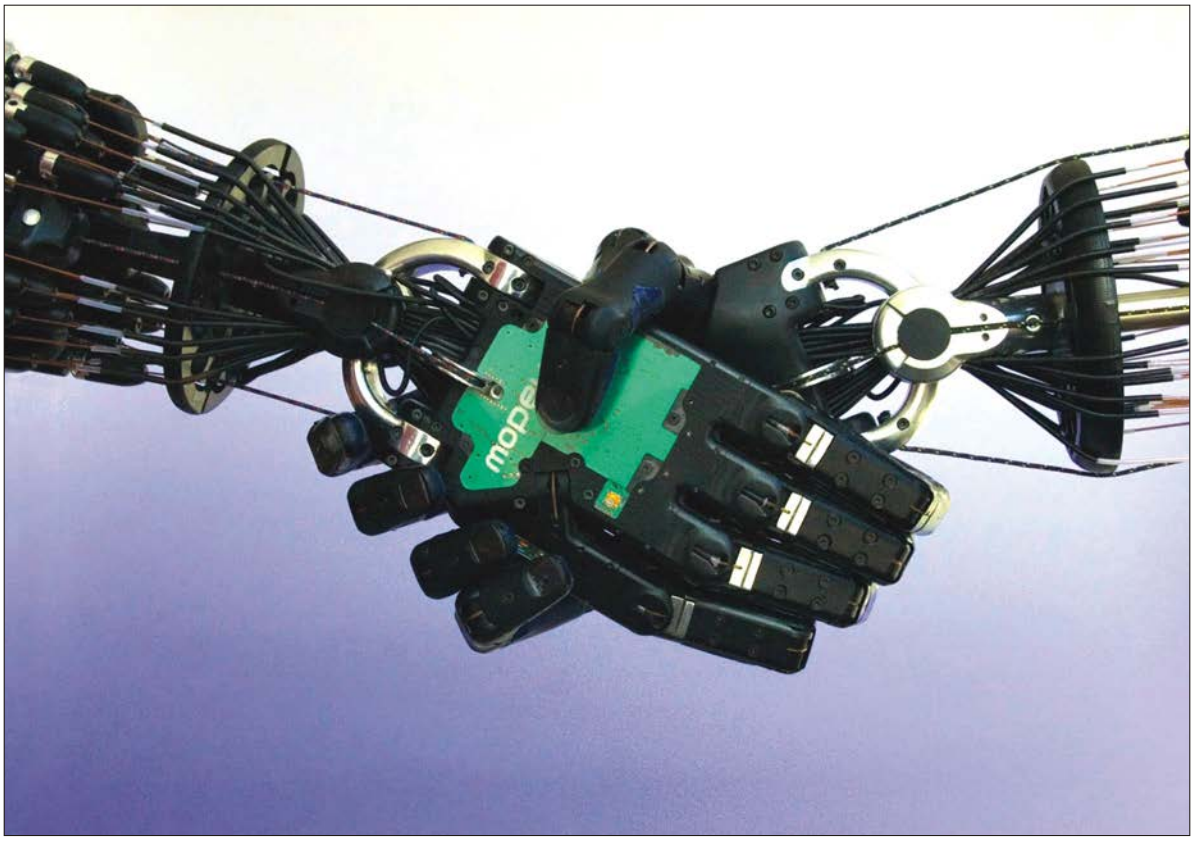

# Journal of Artificial Intelligence

ISSN 1994-5450

science alert

ANSInet
an open access publisher
http://ansinet.com

OPEN ACCESS Journal of Artificial Intelligence

ISSN 1994-5450
DOI: 10.3923/jai.2017.66.75

# Research Article
# Image Tamper Detection using Energy Deviation Measure

Surbhi Gupta and Neeraj Mohan

Computer Science and Engineering, Inder Kumar Gujral Punjab Technical University, Kapurthala, India

## Abstract

**Background and Objective:** Digital imaging, image forgery and its forensics has become an emerging field for research now days. Digital imaging is used to enhance and restore images to make them more meaningful whereas image forgery produces tampered fake images. Digital forensics is required to examine the questioned images and classify them as authentic or tampered. This study aimed to introduce an image tamper detection method using statistical features extracted from Energy Deviation Measure. **Materials and Methods:** Energy Deviation Measure is a measure of Energy Deviation in pixel neighbourhood in tampered and recompressed images. It is extracted by measuring the inter pixel intensity difference across and inside the DCT block boundary. Features from Energy Deviation Measure have been used to classify the authentic and tampered images. Support Vector Machine is used for classification. **Results:** The experimental results have shown that the proposed method performs better with fewer dimensions as compared to other state of art methods. It gives improved accuracy and area under curve while classifying images and it is robust to noise and JPEG compression quality factor. **Conclusion:** The proposed Energy Deviation Measure captures the essential compression characteristics of an image and hence could be successfully utilized in classifying authentic and tampered images.

Key words: Energy deviation measure, image tampering, copy move forgery, image splicing, image forensics, compression artifacts

Received: January 16, 2017 Accepted: February 22, 2017 Published: March 15, 2017

Citation: Surbhi Gupta and Neeraj Mohan, 2017. Image tamper detection using energy deviation measure. J. Artif. Intel., 10: 66-75.

Corresponding Author: Surbhi Gupta, Computer Science and Engineering, Inder Kumar Gujral Punjab Technical University, Kapurthala, India Tel: +91-9888659888



Competing Interest: The authors have declared that no competing interest exists.

Data Availability: All relevant data are within the paper and its supporting information files.

## INTRODUCTION

Image Tamper Detection has become an emerging image processing domain since last 2 decades. The readily available software, tools and techniques have made the image processing and forgery quite easier these days. The tools available for enhancement are being misused to manipulate or tamper the image to hide the truth and establish the fallacies. There are enormous ways to tamper or forge an image and thus a number of forensic techniques are required to fully authenticate an image prior to its use. Most common image forgery techniques are copy-move and splicing as shown in Fig. 1. Copy move forgery involves cropping, processing and then replicating some part of the same image to either hide or add some content to the image. Whereas, splicing involves using 2 different images to create a new image with new content altogether. Thus, before relying on an image we need to first check its authenticity using image forensic tools and techniques. This is done by image forensics, which aims at detecting and classifying tampered images. Image forensic techniques are based on active and passive approaches[1]. The active approach uses a watermark or signature which would get distorted if the image is tampered. The active approach is mainly used for sensitive documents and images as they are highly prone to tampering. A passive approach is used for the documents which are not already secured using active approach. Passive approach does not require any background information about the image rather it extracts features and characteristics from the available image to make a decision. Passive image forensics may be done by source identification, noise pattern analysis or other quality assessment features to identify image tampering[2].

Usually passive approaches utilize features extracted from Discrete Cosine Transform (DCT) or quantization artifacts for image forensics of .jpg, .tif and .bmp images. These features are used to train the classifier model so that it can perform classification. These techniques are fast with good performance but high false positive/negative rate has been a challenge for these techniques.

Many contributions have been made in passive image forensics domain in last 2 decades. Initially, image tamper detection is proposed using traces of image re-sampling by Popescu and Farid[3]. Then, compression characteristics based Blocking Artifact Characteristics Matrix (BACM) had been introduced by Fan and de Queiroz[4] to identify double image compression, which was further used to determine cropping and recompression by Luo *et al.*[5]. A natural image model has been proposed by Shi *et al.*[6] to investigate the periodic property of blocking artifacts. De Carvalho *et al.*[7] proposed a novel method for exposing digital image forgeries based on color illuminations. Some researchers[8-10] proposed Markov Model based features for image splice detection and achieved good accuracy. Steerable Pyramid Transform[11] (SPT) was used on chrominance channels to achieve 94.89% detection accuracy on CASIA v1.0 dataset. The GLCM was proved to be an effective texture descriptor[12-14]. In addition, texture based descriptors were applied for splice detection[15]. Furthermore, feature section based technique using Gabor filter with DCT[16] and multi-scale Weber Local Descriptors (WLD)[17] was proposed and image features were extracted which yielded very good results. Agarwal and Chand[18] proposed multi scale entropy filter for image splice detection.

Proposed methods for image forensics achieved good promising accuracy. But the complexity and dimensionality of features for existing algorithms are high and their performance varies with JPEG compression quality. The aim of presented study is to introduce and implement an Energy Deviation Measure (EDM) method for image tamper detection (copy move and splicing) with high accuracy, which is robust to the noise and JPEG compression Quality Factor (QF).


Fig. 1(a-c): (a) Authentic image, (b) Copy Move forgery and (c) Splicing forgery

## MATERIALS AND METHODS

**Proposed EDM approach:** This section elaborates the system design and algorithm for the proposed EDM approach. Figure 2 shows the main steps in system design:

- Calculation of EDM from the image
- Extraction of statistical features from EDM
- Training and testing of support vector machine

These steps taken for the proposed method are elaborated in the following algorithm.

**Step 1:** An image I is transformed to grayscale such that $I_g$ = rgb_to_gray (I)

**Step 2:** Further the image is subdivided into blocks of 8×8 pixels. For each block, for every pixel location (x, y), pixel intensity difference in immediate neighborhood D (x, y) is defined and calculated as Eq. 1 similar to Luo *et al.*[5]:

$$D(x, y) = |[F(x, y) + F(x+1, y+1)] - [F(x+1, y) + F(x, y+1)]| \quad (1)$$

where, F(x, y) represents intensity of pixel at location (x, y) and $1 \leq x, y \leq 8$ .

**Step 3:** Pixel (x+4, y+4) is considered as a distant neighbour and pixel intensity difference in distant neighbourhood is calculated as D(x+4, y+4)

**Step 4:** Absolute difference in immediate and distant neighbourhood D'(x, y) is calculated as in Luo *et al.*[5] using Eq. 2 as:

$$D'(x, y) = |D(x+4, y+4) - D(x, y)| \quad (2)$$

**Step 5:** Mean energy deviation at each pixel location (x, y) i.e., Energy Deviation Measure is calculated using Eq. 3 as:

$$EDM(x, y) = \sum_{i=1}^{n} \frac{D_i'(x, y)}{n} \quad (3)$$

where, n is total number of image blocks.

**Step 6:** Lastly, statistical features F1-F20 are extracted from the EDM of the images and Support Vector Machine is trained and tested to classify authentic and tampered images

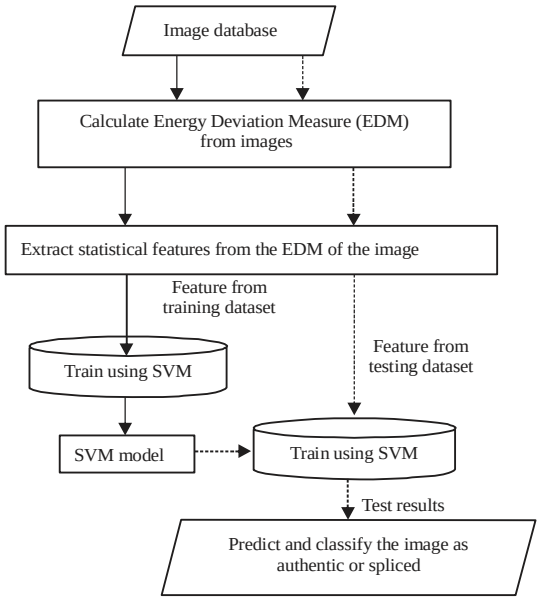


Fig. 2: Proposed System design

The algorithm works on pixel neighbouring in each block. Every pixel is considered neighbour to 4 pixels. Algorithm needs to access each block once and each pixel of the image 4 times to calculate pixel intensity difference. So, each pixel is accessed 4 times and the complexity is equivalent to O (4n) ≈ O (n). The complexity is linear with respect to the size of the image.

**Energy deviation measure and corresponding statistical feature extraction:** The EDM is a measure of Energy Deviation in pixel neighbourhood in tampered and recompressed images. It is known that the inter-pixel intensity differences across the boundary of a JPEG DCT block are similar to those inside the block in an uncompressed image[4,5]. Re-compression in an image disturbs the similarity in the pixel intensity across and inside a DCT block. This disturbance is captured as Energy Deviation Measure for every pixel location. The EDM is calculated by measuring the intensity difference of a pixel with respect to its immediate and distant neighbourhood. Figure 3 represents an 8×8 image block. Blue area represents immediate neighbourhood for pixel (1,1) and (5,5). Pixel (5,5) acts as distant neighbourhood for pixel (1,1).

The inter pixel intensity value difference in immediate neighbourhood for pixel location and was calculated using Eq. 1 as:

$$D(1,1) = |(P_{11} + P_{22}) - (P_{21} + P_{12})| \text{ and } D(5,5) = |(P_{55} + P_{66}) - (P_{65} + P_{56})|$$

where, $P_{11}$ means intensity value F(1,1):

Table 1: Energy deviation measure values of an authentic image

| EDM | y = 1 | y = 2 | y = 3 | y = 4 | y = 5 | y = 6 | y = 7 | y = 8 |
|---|---|---|---|---|---|---|---|---|
| x = 1 | 1.3134 | 1.2746 | 1.2806 | 1.3337 | 1.3448 | 1.3316 | 1.3016 | 1.3516 |
| x = 2 | 1.3141 | 1.3360 | 1.2921 | 1.2557 | 1.3377 | 1.3475 | 1.2587 | 1.3347 |
| x = 3 | 1.3148 | 1.3337 | 1.2834 | 1.3340 | 1.3381 | 1.2742 | 1.3127 | 1.2861 |
| x = 4 | 1.2746 | 1.3273 | 1.3539 | 1.3188 | 1.3104 | 1.3384 | 1.2969 | 1.2709 |
| x = 5 | 1.3404 | 1.3320 | 1.3144 | 1.3576 | 1.2817 | 1.2861 | 1.2763 | 1.2631 |
| x = 6 | 1.2969 | 1.2904 | 1.2915 | 1.3576 | 1.3279 | 1.2999 | 1.2864 | 1.3019 |
| x = 7 | 1.2958 | 1.2938 | 1.3215 | 1.3377 | 1.2388 | 1.3381 | 1.2817 | 1.3046 |
| x = 8 | 1.3215 | 1.2783 | 1.3002 | 1.2506 | 1.2874 | 1.3188 | 1.3593 | 1.3381 |

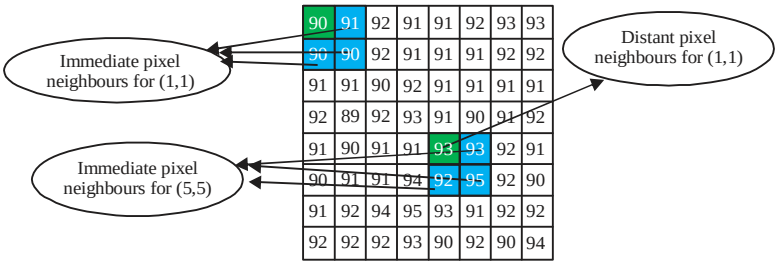


Fig. 3: Image representing immediate and distant neighbourhood

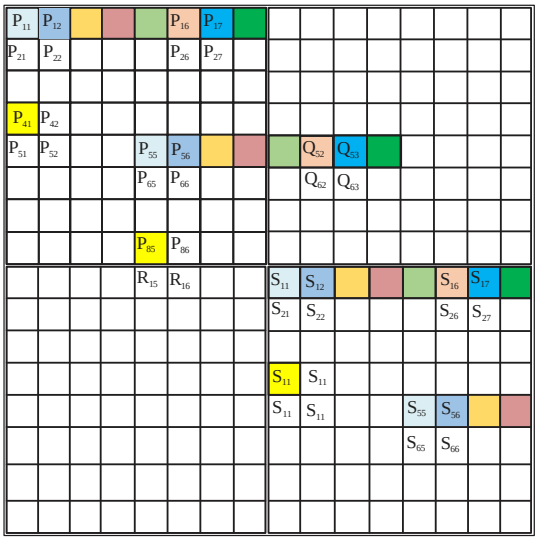

Fig. 4: Representation of immediate and distant neighbourhood in consecutive DCT blocks

$$D(1,1) = |(90+90)-(90+91)| = 1 \text{ and}$$
$$D(5,5) = |(93+95)-(92+93)| = 3$$

Further, pixel intensity difference in immediate and distant neighbourhood was calculated using Eq. 2 as:

$$D'(1,1) = |D(5,5) - D(1,1)| \text{ i.e., } D'(1,1) = 2$$

Here, all the neighbouring pixels lie inside the boundary of the block. In some cases, pixel neighbourhood may belong to other consecutive blocks. Immediate and distant neighbourhood for 4 consecutive 8×8 blocks P, Q, R and S are shown in Fig. 4. Immediate neighbourhood is highlighted with the same color text and distant neighbourhood is highlighted using same color background. For pixel location (4,1) in block P, the distant neighbourhood lies in consecutive block R as illustrated in Fig. 4. So, D(4, 1), D(8, 5) and D'(4, 1) were calculated using Eq. 1 and 2 as:

$$D(4,1) = |(P_{41} + P_{52}) - (P_{51} + P_{42})| \text{ and}$$
$$D(8,5) = |(P_{85} + R_{16}) - (R_{15} + P_{86})|$$
$$D'(4,1) = |D(8,5) - D(4,1)|$$

Further, mean energy deviation EDM (x, y) was calculated for every pixel location for n blocks by taking the mean of absolute difference in immediate and distant neighbourhood using Eq. 3.

It has been observed in experiments that for an authentic image, EDM values at all locations are similar. No significant deviation in EDM values is observed for an authentic image. This is illustrated in Table 1 which shows the EDM values of an authentic image. Similar EDM value has been observed for every pixel location.

Further, the experiments results obtained on images at different quality factors have revealed that tampering in an image causes re-compression which disturbs the EDM of the image significantly. The difference between EDM 7th and 8th row i.e., at the edge of DCT block has been calculated and illustrated for different categories of sample

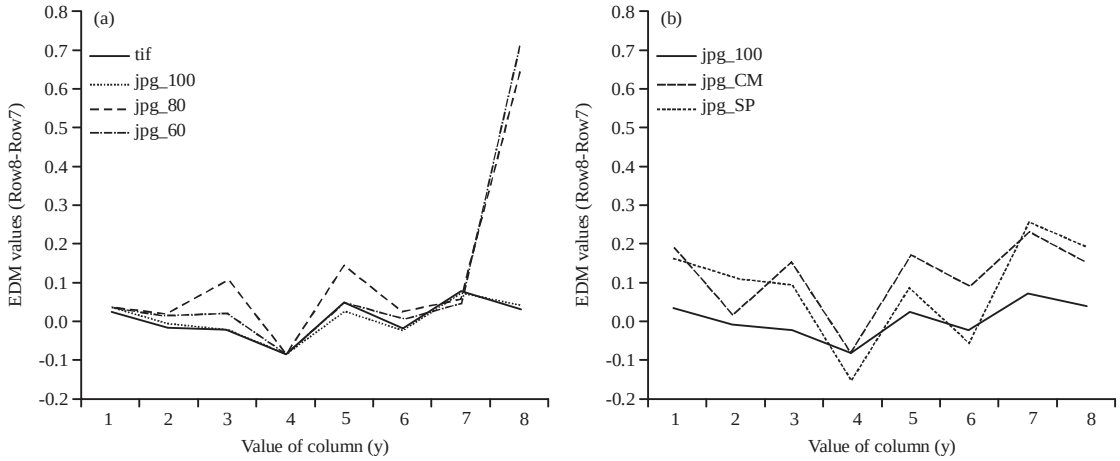


Fig. 5(a-b): Comparison of EDM difference at block boundary for (a) Authentic image at different QFs, (b) Authentic and tampered (CM and SP) images

images in Fig. 5. One can observe that EDM for .tif and .jpg image at QF100 are similar whereas significant deviation of 0.5-1.5 units can be seen at different EDM locations for QF80 and QF60 images as shown in Fig. 5a. Similar deviation can be seen at different EDM locations for tampered images created using Copy Move (CM) and splicing (SP) operations as shown in Fig. 5b.

These deviations are captured in terms of statistical features extracted from EDM of the image. Similar to Luo *et al.*[5], twenty such features are defined statistically in Eq. 4-23 as follows:

$$F1 = \sum_{y=1}^{3} |EDM(4,y) - EDM(4,8-y)| \quad (4)$$

$$F2 = \sum_{x=1}^{3} |EDM(x,4) - EDM(8-x,4)| \quad (5)$$

$$F3 = \sum_{x=1}^{3}\sum_{y=1}^{3} EDM(x,y) - EDM(x,8-y) \quad (6)$$

$$F4 = \sum_{x=5}^{7}\sum_{y=1}^{3} EDM(x,y) - EDM(x,8-y) \quad (7)$$

$$F5 = \sum_{x=1}^{3}\sum_{y=1}^{3} EDM(x,y) - EDM(8-x,y) \quad (8)$$

$$F6 = \sum_{x=1}^{3}\sum_{y=5}^{7} EDM(x,y) - EDM(8-x,y) \quad (9)$$

$$F7 = \sum_{x=1}^{3}\sum_{y=1}^{3} EDM(x,y) - EDM(8-x,8-y) \quad (10)$$

$$F8 = \sum_{x=1}^{3}\sum_{y=5}^{7} EDM(x,8-y) - EDM(8-x,y) \quad (11)$$

$$F9 = \frac{EDM(4,4)}{\sum_{x=1}^{3}\sum_{y=1}^{3} EDM(x,y)} \quad (12)$$

$$F10 = \frac{EDM(4,4)}{\sum_{x=1}^{3}\sum_{y=5}^{7} EDM(x,y)} \quad (13)$$

$$F11 = \frac{EDM(4,4)}{\sum_{x=5}^{7}\sum_{y=1}^{3} EDM(x,y)} \quad (14)$$

$$F12 = \frac{EDM(4,4)}{\sum_{x=5}^{7}\sum_{y=5}^{7} EDM(x,y)} \quad (15)$$

$$F13 = \frac{EDM(4,4)}{\sum_{y=1}^{7} EDM(4,y) - EDM(4,4)} \quad (16)$$

$$F13 = \frac{EDM(4,4)}{\sum_{x=1}^{7} EDM(x,4) - EDM(4,4)} \quad (17)$$

$$F15 = \sum_{i=1}^{4}\sum_{j=1}^{4} EDM(i,j) \quad (18)$$

$$F16 = \sum_{i=5}^{8}\sum_{j=1}^{4} EDM(i,j) \quad (19)$$

$$F17 = \sum_{i=1}^{4}\sum_{j=5}^{8} EDM(i,j) \quad (20)$$

$$F18 = \sum_{i=5}^{8}\sum_{j=5}^{8} EDM(i,j) \quad (21)$$

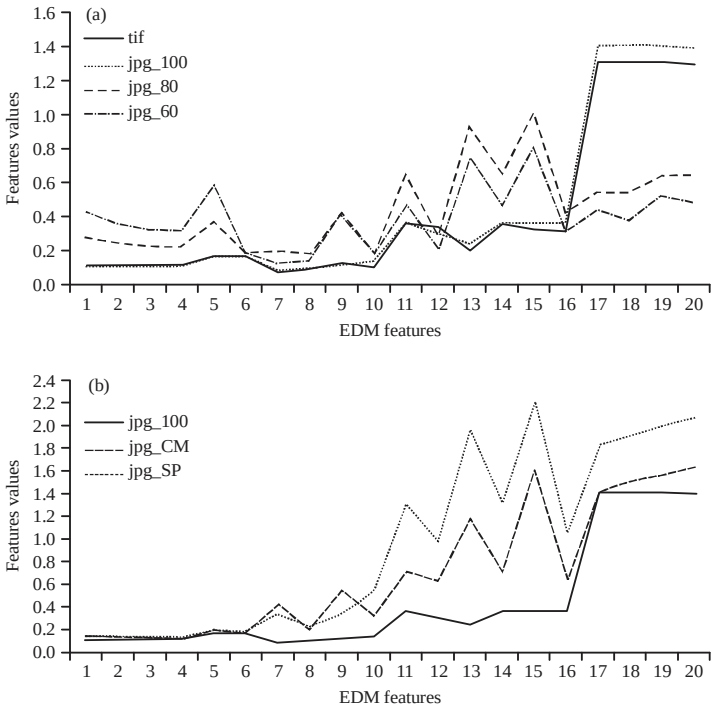


Fig. 6(a-b): Comparison of EDM feature values for (a) Authentic image at different QFs, (b) Authentic and tampered (CM and SP) images

$$F19 = \sum_{y=1}^{3} |EDM(8,y) - EDM(8,8-y)| \quad (22)$$

$$F20 = \sum_{x=1}^{3} |EDM(x,8) - EDM(8-x,8)| \quad (23)$$

A sample of feature values for authentic images at various quality factors (QF100, QF80 and QF60) and tampered images (created using copy move and splicing operations for sample images shown in Fig. 1) are represented in Fig. 6a, b respectively. It is evident that the EDM features are efficient enough in classifying authentic and tampered images at various Qfs.

## RESULTS AND DISCUSSION

Correct classification of authentic and tampered images in their respective classes is very crucial. A good classification method always aims at high accuracy with low complexity for all the possible scenarios. The advantage of proposed EDM method is that it achieved high accuracy for images for all types of spliced images at different quality factors with less dimensionality of features, which has not been illustrated by many recent existing techniques[15-17]. Proposed method achieved an accuracy of 96.38% with low dimensionality of 20 features. The results obtained for proposed method demonstrate its effectiveness in classifying authentic and tampered images for different Quality factor, splice area and presence of noise.

The results have been obtained using a popular image dataset CASIA V2.0[19]. This dataset consist of 7491 authentic and 5123 tampered images. Images are categorised as nature, architecture, art, plants, animals, indoors and character classes to cover all possible types of images. Tampered images are produced using crop-paste and spliced image region(s). These images are pre-processed with resizing, rotation or other distortions. Images are post-processed with operations such as blurring to finish crop-and-paste operations. Different size (small, medium and large) of spliced region has been considered. Another set of images has been generated to further test the robustness of proposed method at various image compression quality factors, Gaussian blur and white noise.

A 'n' fold cross validation approach is used to train and test the support vector machine for the proposed method. This approach divides the dataset in 'n' subsets. Then, (n-1)/n proportion of the set is taken as training and 1/n proportion is taken as testing set. Most of the state of art methods uses 10 fold or 6 fold cross validation. So, the experimentation has been conducted for both 10 and 6 fold cross validation to evaluate the performance of proposed method. LIBSVM[20]

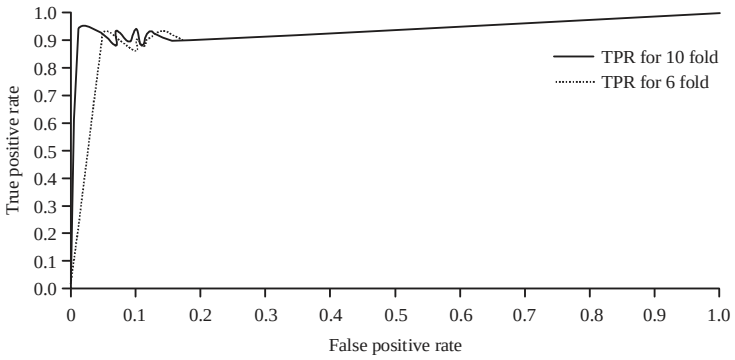


Fig. 7: Receiver Operator Characteristics Curve for proposed EDM method

Table 2: Performance comparison with existing methods

| Parameters | Proposed method | Natural image model based method | Multi scale WLD | GF+DCT | Proposed method | Markov features based method | Textural feature based method |
|---|---|---|---|---|---|---|---|
| Cross validation | 10 fold | 10 fold | 10 fold | 10 fold | 6 fold | 6 fold | 6 fold |
| Accuracy | 96.38 | 84.86 | 96.61 | 97.90 | 95.98 | 89.76 | 97.73 |
| Dimensionality | 20.00 | 266.00 | 960.00 | 70.00 | 20.00 | 100.00 | 96.00 |
| Need for feature selection | Not required | Not required | Not required | Required | Not required | Required | Not required |

classifier with Radial Basis Function kernel is used as it is well known for its performance for binary classification. The penalty parameter C is chosen by Grid Search method. The performance for proposed method was investigated as follows:

- Performance evaluation and comparison with existing methods
- Performance evaluation for small, medium and large spliced area
- Performance evaluation at different JPEG Compression Quality Factors, Gaussian Blur and White Noise

**Performance evaluation and comparison with existing methods:** The proposed EDM method has been evaluated using 10 fold and 6 fold cross validation approach. Images are selected randomly for each test and each experiment has been repeated for 15 times to avoid the effect of randomness of selection. It is evident that performance of proposed EDM method is excellent for both 10 and 6 fold cross validation. The performance parameters considered are True Positive Ratio (TPR), True Negative Ratio (TNR), Accuracy (ACC) and Area Under Curve (AUC). TPR and TNR mean the correct classification of authentic and tampered images in their classes respectively. Overall correct classification is indicated by ACC and AUC represents area under Receiver Operator Characteristics (ROC) curve. The TPR, TNR, ACC and AUC achieved for 6-fold cross validation are 96.24, 95.69, 95.98 and 0.9698 respectively. The TPR, TNR, ACC and AUC achieved for 10-fold cross validation improved slightly as 97.36, 95.23, 96.38 and 0.9733 respectively. The AUC in both cases is $\geq$ 0.96 which is very near to ideal value i.e., 1. It demonstrated that proposed method is fairly effective. The ROC curve for both the approaches is shown is Fig. 7.

The performance of proposed EDM method has been compared with five different existing methods in Table 2. Accuracy, Dimensionality and Need for features selection are the parameters considered for comparison. Most of the existing methods have high dimensionality ranging from 70-960 which increased their processing time. Further, feature selection also resulted in extra processing time which is avoided is proposed EDM method. The proposed method has low dimensionality (number of features) i.e., 20 and achieved an accuracy of 96.38% without using feature selection.

Accuracy obtained for proposed method is higher as compared to methods based on Natural model[6] and Markov features[8]. Multi scale Weber Local Descriptor (WLD) methods[17] has achieved similar accuracy of 96.61% but with very high dimensionality i.e., 960. Similarly, Gabor filter and DCT based method[16] and Texture based method[15] achieved marginally higher accuracy of 97.90% with higher dimensionality. Further, GF+DCT and Markov feature based methods require feature selection too.

**Performance evaluation for small, medium and large spliced area:** The classification accuracy of proposed method is also evaluated for small, medium and large splicing area. It

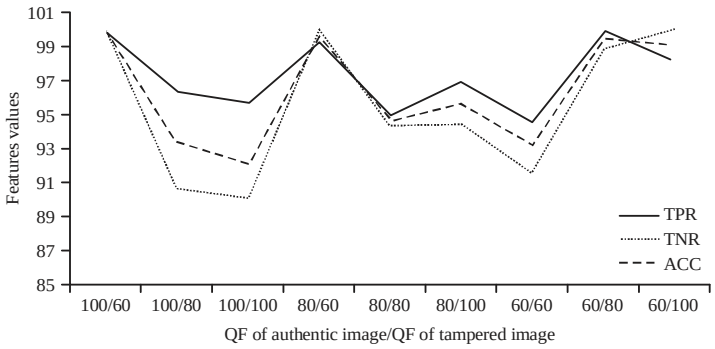


Fig. 8: Classification accuracy at different JPEG quality factors of authentic and tampered images

Table 3: Performance variation at different JPEG compression quality factors

| Authentic image Quality factor | Spliced image Quality factor | True positive ratio | True negative ratio | Accuracy | Area under curve |
|---|---|---|---|---|---|
| QF100 | QF60 | 100.00 | 100.00 | 100.00 | |
| | QF80 | 96.40 | 90.70 | 93.40 | 0.9300 |
| | QF100 | 95.70 | 90.10 | 92.12 | 0.9200 |
| QF80 | QF60 | 99.30 | 100.00 | 99.70 | 0.9900 |
| | QF80 | 95.00 | 94.40 | 94.70 | 0.9500 |
| | QF100 | 97.00 | 94.40 | 95.70 | 0.9600 |
| QF60 | QF60 | 94.60 | 91.60 | 93.20 | 0.9300 |
| | QF80 | 100.00 | 98.90 | 99.50 | 1 |
| | QF100 | 98.20 | 100.00 | 99.10 | 0.9900 |
| Average | | 97.36 | 95.23 | 96.38 | 0.9633 |

was observed that the proposed method gives better accuracy in classifying images with small spliced area as compared to images with medium and large spliced area. The accuracy of proposed method for images with large spliced area is 92.6, which improves to 93.5 for medium spliced area and 96.7 for small spliced area. It is evident that accuracy is better for images with small spliced area.

**Performance evaluation at different JPEG compression quality factors, gaussian blur and white noise:** As images splicing is usually followed by post-processing, it is important to test the robustness of proposed method in presence of noise. Experiments for images at different compression Quality Factors, Gaussian Blur and White Noise have been conducted. Images from CASIA 2.0 have been post processed to evaluate the results.

As the quality factor of an image is a direct measure of its compression ratio, a thorough experimentation has been conducted to evaluate its impact on proposed EDM method. The recompressed authentic and tampered images at various JPEG Quality Factors i.e. 60, 80 and 100 were tested using proposed EDM method. Results have been tabulated in Table 3.

It is evident that classification accuracy of proposed method is better while classifying authentic and tampered images at different QFs as compared with authentic and tampered images at same QFs. Figure 8 shows the parameter values for different combinations of authentic and tampered images at QF 100, 80 and 60. QF_100_80 represents authentic image at QF100 and tampered image at QF80.

The classification accuracy of proposed method is studied in presence of Gaussian Blur at =0.05 and White noise at mean=0 and variance=0.00005 in the images. The classification accuracy obtained is 93.6 and 92.3 respectively.

The above experiments infer that proposed EDM classifier outperforms in terms of accuracy and dimensionality without using feature selection. Moreover, it is robust to compression quality factor and gives good accuracy for all the scenarios. It performs well even in the presence of Gaussian blur and white noise in spliced image.

## CONCLUSION

A novel Energy Deviation Measure based method for detecting tampered images has been proposed and implemented. The statistical differentiating features based on EDM have been extracted as mentioned in algorithm and

system design. Authentic and tampered images at various quality factors i.e., QF60, QF80, QF100 with copy move and splicing operation have been considered to train and test Support Vector Machine. The main advantage of proposed EDM method is that it performs well with fewer dimensions and irrespective of the image compression quality factor. It can be used to detect copy move and spliced tampered images undergone any kind of pre-processing operation as cropping, re-sampling and rotation etc. as well as any post-processing operation such as blurring or added noise. It supports .jpg, .bmp and .tif images. The receiver operating characteristic curve and area under the curve demonstrated that proposed EDM method achieves high accuracy as compared to existing methods with lesser dimensionality and no feature selection. The proposed EDM method may be extended to make an integrated forensic tool for detecting and classifying splicing, copy move, seam carving, steganography and other types of tampering in images.

## SIGNIFICANCE STATEMENTS

This study discovers the Energy Deviation Measure to determine tampering in digital images. This method is based on utilizing compression artifacts for image forensics. The proposed method has high accuracy in classifying authentic and tampered images. It is a significant contribution in image forensics as proposed method can detect both copy-move and splicing at any compression quality factor and is robust to pre and post processed operations in the image. Thus, a new method for image forensics has been proposed and implemented successfully.

## REFERENCES


1. Birajdar, G.K. and V.H. Mankar, 2013. Digital image forgery detection using passive techniques: A survey. Digital Invest., 10: 226-245.
2. Asghar, K., Z. Habib and M. Hussain, 2017. Copy-move and splicing image forgery detection and localization techniques: A review. Aust. J. Forensic Sci., 49: 281-307.
3. Popescu, A.C. and H. Farid, 2005. Exposing digital forgeries by detecting traces of resampling. IEEE Trans. Signal Process., 2: 758-767.
4. Fan, Z. and R.L. de Queiroz, 2003. Identification of bitmap compression history: JPEG detection and quantizer estimation. IEEE Trans. Image Process., 12: 230-235.
5. Luo, W., Z. Qu, J. Huang and G. Qiu, 2007. A novel method for detecting cropped and recompressed image block. Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing, Volume 2, April 15-20, 2007, Honolulu, HI., USA., pp: 217-220.
6. Shi, Y.Q., C. Chen and W. Chen, 2007. A natural image model approach to splicing detection. Proceedings of the 9th Workshop on Multimedia and Security, September 20-21, 2007, Dallas, TX., USA., pp: 51-62.
7. De Carvalho, T.J., C. Riess, E. Angelopoulou, H. Pedrini and A. de Rezende Rocha, 2013. Exposing digital image forgeries by illumination color classification. IEEE Trans. Inform. Forensics Secur., 8: 1182-1194.
8. He, Z., W. Lu, W. Sun and J. Huang, 2012. Digital image splicing detection based on Markov features in DCT and DWT domain. Pattern Recognit., 45: 4292-4299.
9. El-Alfy, E.S.M. and M.A. Qureshi, 2015. Combining spatial and DCT based Markov features for enhanced blind detection of image splicing. Pattern Anal. Applic., 18: 713-723.
10. Su, B., Q. Yuan, S. Wang, C. Zhao and S. Li, 2014. Enhanced state selection Markov model for image splicing detection. EURASIP J. Wireless Commun. Networking. 10.1186/1687-1499-2014-7.
11. Muhammad, G., M.H. Al-Hammadi, M. Hussain and G. Bebis, 2014. Image forgery detection using steerable pyramid transform and local binary pattern. Mach. Vision Applic., 25: 985-995.
12. Chen, G.C., B. Su, S.L. Wang and S.H. Li, 2011. Blind detection of splicing image based on gray level co-occurrence matrix of image DCT domain. J. Shanghai Jiaotong Univ., 45: 1547-1551.
13. De Siqueira, F.R., W.R. Schwartz and H. Pedrini, 2013. Multi-scale gray level co-occurrence matrices for texture description. Neurocomputing, 120: 336-345.
14. Nanni, L., S. Brahnam, S. Ghidoni and E. Menegatti, 2015. Improving the descriptors extracted from the co-occurrence matrix using preprocessing approaches. Expert Syst. Applic., 42: 8989-9000.
15. Shen, X., Z. Shi and H. C hen, 2016. Splicing image forgery detection using textural features based on the grey level co-occurrence matrices. IET Image Process., 11: 44-53.
16. Muhammad, G., M.S. Dewan, M. Moniruzzaman, M. Hussain and M.N. Huda, 2014. Image forgery detection using Gabor filters and DCT. Proceedings of the International Conference on Electrical Engineering and Information and Communication Technology, April 10-12, 2014, Dhaka, Bangladesh, pp: 1-5.

17. Hussain, M., S. Qasem, G. Bebis, G. Muhammad, H. Aboalsamh and H. Mathkour, 2015. Evaluation of image forgery detection using multi-scale Weber local descriptors. Int. J. Artif. Intell. Tools, Vol. 24, No. 4. 10.1142/s0218213015400163.
18. Agarwal, S. and S. Chand, 2015. Image forgery detection using multi scale entropy filter and local phase quantization. Int. J. Image Graph. Signal Process., 10: 78-85.
19. Dong, J. and W. Wang, 2011. CASIA 2.0. CASIA Tampered Image Detection Evaluation Database. http://forensics .Idealtest.org/casiav2/.
20. Chang, C.C. and C.J. Lin, 2011. Libsvm: A library for support vector machines. ACM Trans. Intell. Syst. Technol., Vol. 2, No. 3. 10.1145/1961189.1961199.