Frequency based edge-texture feature using Otsu's based enhanced local ternary pattern technique for digital image splicing detection

Vikas Srivastava, Sanjay Kumar Yadav

Department of Computer Science and Information Technology, Sam Higginbottom University of Agriculture, Technology and Sciences, Prayagraj, U.P., India

Article Info	ABSTRACT
	Sharing information through images is a trend nowadays. Advancements in the technology and user-friendly image editing tool make easy to edit the image and spread fake news through different social networking platforms. Forged image has been generated through an advanced image editing tool, so it is very challenging for image forensics to detect the micro discrepancy which distorted the micro pattern. This paper proposes an image forensic detection technique, which implies multi-level discrete wavelet transform to implement digital image filtering. Canny edge detection technique is implemented to detect the edge of the image to implement Otsu's based enhanced local ternary pattern (OELTP), which can detect forgery-related artifact. DWT is implemented over Cb and Cr components of the image and using edge texture to improve the Otsu global threshold, which is used to extract features using ELTP technique. Support vector machine (SVM) is used for classification to find the image is forged or not. The performance of the work evaluated on three different open available data sets CASIA v1, CASIA v2, and Columbia. Our proposed work gives better results with some of the previous states of the work in terms of detection accuracy. *This is an open access article under the [CC BY-SA](#) license.*

Corresponding Author:

Vikas Srivastava
Department of Computer Science and Information Technology
Sam Higginbottom University of Agriculture, Technology and Sciences
Prayagraj, U. P., India
Email: vikassrivasta@gmail.com

1. INTRODUCTION

Image forgery is a widespread activity in different fields by different modes like generating fake evidence, spread fake news. The digital image is a huge source of information in various areas such as disease detection in the medical field, forensic detection, electronic media, e-commerce, and social networking sites. Millions of images are uploaded daily on WhatsApp, Facebook, and other networking sites, and many are fake. They tampered with the help of advanced image editing tools and techniques. These counterfeit images negatively affect our society. So it's required to develop such forensic detection tools with the forgery detection technique to identify image forgery over the different formats of the image.

There are two types of image forensic techniques, active and passive. Digital signature and watermarking are subpart of active, and copy-move and splicing are passive subpart. We are discussing the passive image forensic technique which is applicable on both copy-move and splicing, which is trendy but not easy to implement. It's also known as the blind image forgery detection technique. In this technique, the source of the image is unknown, and only the image is present. Due to image forgery, internal statistical

information of the image gets disturbed. Detecting the forgery needs to extract disturbed internal statistics as a feature extraction, which helps to detect forgery. In this paper, we used frequency based edge texture for feature extraction technique. Through edge the performance of the optimal global threshold has been improved and the performance of the enhanced local ternary pattern (ELTP) has been improves show in result.

The tampering detection technique plays a significant role in identifying the image splicing. So many techniques were discussed last year. Some of them are discussed here, based on extraction of the various feature of the image illumination, JPEG compression, camera based property or limitations, and so on. To identify the image forgery [1], [2] the property and restrictions of the camera play an important role, it's work like a fingerprint because every camera has its own noise. They identify the differences generated by camera noise as a feature to identify the image splicing. Image forgery detected by feature fusion technique discuss in [3], where camera features and image quality are used to train them in color, quality, and frequency. The concept of color filter array (CFA) is used in [4], [5], to generate RGB through interpolation. Image tampering detected by CFA and interpolation. The best approach for pixel based feature technique is local binary pattern (LBP) [6]-[8], LBP is used for feature extraction with the help of discrete cosine transform (DCT) over the chrominance component of the image after converting the RGB image into YCbCr and derived the image into non-overlapping block. Frequency based technique is used to classified the image for forgery detection. In paper [9], [10], DCT transition probability metrics implements Markov based approach for forgery detection. Frequency-based domain generated by discrete wavelet transform (DWT) to characterize the wavelet coefficient across position, scale and orientations. Support vector machine (SVM) is used for classification. To detect blind image splicing multi-scale local binary pattern [11] is implemented over discrete cosine transform coefficient for feature extraction. K-fold cross validation technique is used to train the system. Steerable pyramid transform (SPT) [12] and LBP is implemented over the chrominance component of the image. Every texture of SPT is described by LBP histogram. Which are concatenate to generate features, and SVM is used for classification. Entropy filter and local phase quantization (LPQ) texture operator [13] is used for forgery detection. Image boundary highlighted by entropy filter and internal statistic of the image obtained by LPQ. SVM is used to classify the image. In paper [14], a traditional gray level co-occurrence material (GLCM) and LBP for texture descriptor of the image. Convolutional neural network (CNN) and multi-scale patch based recognition is used as a fisher vector. A modern hybrid frame work [15] has been proposed for existing all possible features of the image tampering to develop the best feature set. Classify the feature with the classification technique to get better result. Rotation invariant technique [16] is used to detect uniform pattern on LBP. Generalized gray scale and rotation invariant operator is used to detect the uniform reason for any quantization of angular space. It generates multiple operators for multiplex resolution. Standard deviation filter is used to highlight the image information [17]-[19], internal statistic extracted by rotation-invariant co-occurrence among adjacent local binary pattern (RIC-LBP) operator and classify to detected forgery. The concept of the ternary pattern is firstly discuss in paper [20], binary pattern (0, 1) is used for LBP and ternary pattern (0, -1, 1) used for local ternary pattern (LTP) to remove the limitations of basic LBP technique. LTP is more reliable then LBP. In paper [21], ELTP is used for enhanced the performance of the LTP technique. Features are extracted with of standard deviation filter (STD) and ELTP over chrominance component of the image. STD filter highlighted the abrupt changes of the image. SVM is used for classification to find the forgery. In paper [22] image texture features are considered to detect the edge of the image. This technique is implemented on an image where multiple faces are present. CASIA v1.0 data set for tampering detection in this data set image are stored in JPEG format. JPEG format-based technique images are compressed multiple times for tampering, quantization, and blocking artifacts. It is implemented on both frequency and special domain.

2. PROPOSED METHOD

Training and testing two stages are used to detect image forgery show in Figure 1. In training, pristine and forged images are used to train the classifier to detect image forgery. In testing same classifier is used to test the image is forged or not. Many techniques are used for image forgery detection. If two are more images are combined to generate a forged image is a spliced technique. A single image is used to copy and paste somewhere in the same image, known as the copy-move forgery detection technique. Some approaches are used to find the image forgery, like image compression, camera noise, and edge detection. In this paper, we proposed a technique for image splicing detection. We implement wavelet transform for digital filtering to excess the time scale depiction. The edge detection technique is implemented over wavelet transform for detecting meaningful discontinuities in intensity value. In this proposed work, texture-based image splicing detection is used because it divides into the region of interest and classifies the region. It also helps to generate a global threshold by Otsu. The ELTP technique is implemented on the image. Forgery can be

detected with the help of a support vector machine, gives awe-inspiring results and easy to implement [23], over three different types of data set, CASIA v1, CASIA v2 [24], and Columbia.

We implement DWT to implement frequency-based digital image filtering and excess the image edge texture to produce batter global-threshold to implement ELTP and get batter feature extraction for forgery detection.

Algorithm

a.   Convert RGB image into the YCbCr image component.
b.   Chrominance component of the image is used for feature extraction.
c.   Frequency-based model is implemented to extract edge texture.
d.   Otsu-based enhanced local ternary pattern (OELTP) is used for feature extraction.
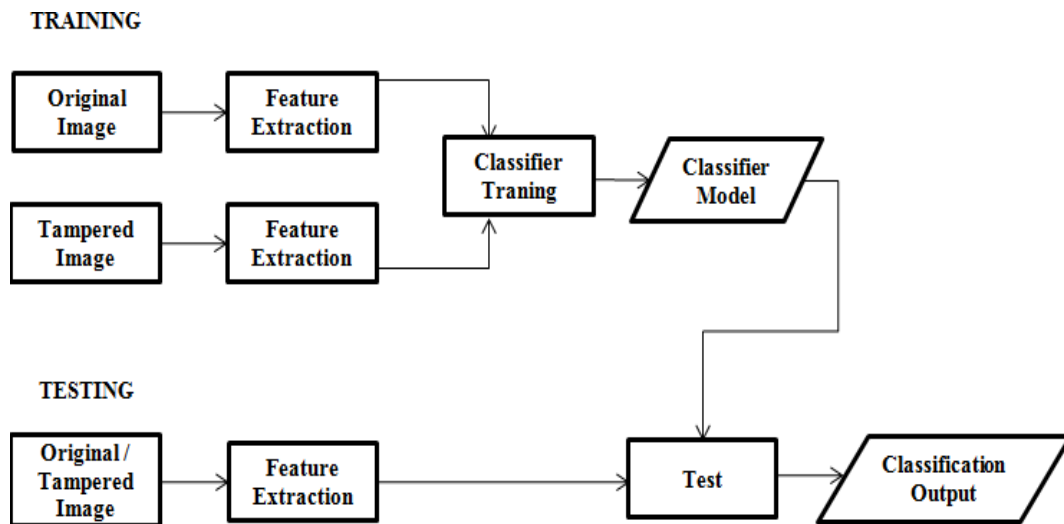e.   SVM classifier is used for forgery detection.

Figure 1. Framework for image splicing detection technique

3.   RESEARCH METHOD
3.1.   Proposed splicing detection system

Texture based feature extraction technique is very effective due to the highly discriminative property at the local level. In this paper, we proposed an edge-based feature extraction technique. We detect the edges to find the meaning of discontinuities in the intensity of pixels [25]. A threshold becomes better if it is tall, narrow, and separated by deep values. A most straightforward way to improve the shape of the histogram is to consider those pixels near the edge between the object and the background. We implement Otsu-based global threshold on ELTP technique for feature extraction [26], [27]. SVM is used for classification to find the image is fake are pristine. We are considering three image databases for implementing our proposed work. These are CASIA v1, CASIAv2, Columbia. Chrominance components of the image are considered. A multi-level wavelet transform is implemented over the chrominance component to get the important details in the frequency domain, the architecture of the proposed work represented by Figure 2.
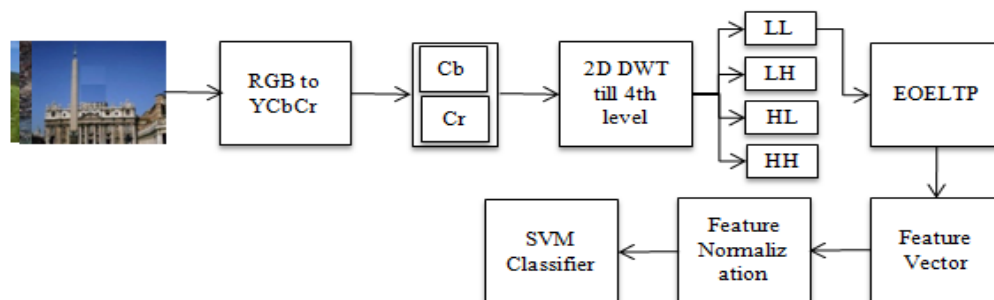

Figure 2. Architectural model of proposed work

3.2. Preprocessing

Image forgery artifacts are embedded in the form of edge discrepancy. An effective color component plays an essential role in feature extraction. We choose the YCbCr color component after converting RGB into YCbCr, RGB and luminance and chrominance relation shown in (1)-(3). We consider this color component because it does not describe the image component in detail. It's promoting a weak signal component of an image. The forgery artifacts are so effective in hiding tampering traces. Due to tampering, edge defection can be represented by the chrominance component of the image. In the proposed work, we implement defection performance through a couple of texture features, i.e. special and frequency-based.

$$Y=0.299 R + 0.587 G + 0.114 B \tag{1}$$

$$Cr=0.701 R - 0.587 G - 0.144 B \tag{2}$$

$$Cb=-0.299 R -0.587 G + 0.886 B \tag{3}$$

3.3. Feature extraction technique

To detect image forgery artifact, need to extract features of the image as per application and dataset. It is found that the operation which is used for forged the image is predicted, help to find the features.

3.3.1. Discrete wavelet transform

DWTis a frequency-based model. It's reliable for texture feature classification. A digital filtering technique is implemented by discrete wavelet transform for time scale depiction of the digital signal. In DWT, the image decomposed into four frequency components, represented by LL (approximation coefficient), low-high (LH), high-high (HH), high-low (HL), shown in Figure 3 (a). The energy store in the approximation coefficient block. The effect of DWT on the image is represented by Figure 3 (b). In this proposed work, we implement DWT on the image. We again decomposed approximation coefficient into four sub-bands until the fourth level after converting RGB into YCbCr. Features are calculated through the mean of approximation coefficient and standard deviation.
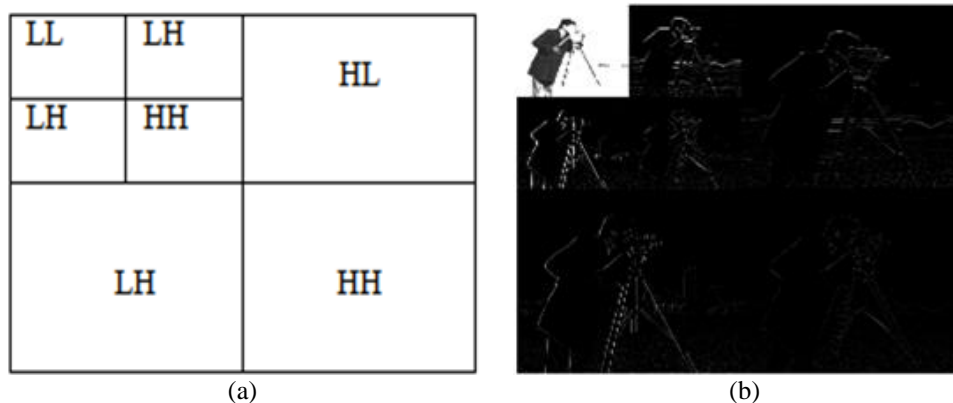

(a)   (b)

Figure 3. These figures are; (a) frequency representation of DWT, (b) multi-level DWT effect on image

3.3.2. Enhance local ternary pattern

Local binary pattern (LBP) is reliable for local feature extraction in texture. Its descriptor has some restrictions due to dependency on the central pixel. It does not perform well on random and quantization noise over uniform resigns. LBP used binary values 0 and 1 to encode the intensity between central and surrounding pixels shown by (4). Ternary value 0, 1, -1 are consider to evaluate the LTP. It's represented by (5). LTP used a fixed threshold value to find the intensity of the central pixel. The LTP is updated by an ELTP. In ELTP, the dynamic threshold value concept is used [27]. The intensity relationship between the central pixel (I_c^E) and threshold (I_s^E) of ELTP is represented by (6). M represents the image matrix of 3x3, neighbor pixels of the central pixel represented by I_c^E, and the threshold is enhanced mean absolute deviation (MAD) in the ELTP technique. The ternary matrix of ELTP is generating after implementing M, I_c^E, and T^E in (5).

$$LBP_{N,R} = \sum_{i=1}^{N} S\,(I_i - I_c)\,2^{i-1}$$
$$S(y) = \begin{cases} 1 \ , \text{if } y \geq 0 \\ 0 \ , \text{Otherwise} \end{cases} \tag{4}$$

$$S\big(I_{i,}I_{c,}T_s\big) = \begin{cases} 1 & I_i \geq I_c + T_s \\ 0 & I_c - I_c < T_s \\ -1 & I_i \leq I_c - T_s \end{cases} \tag{5}$$

where; I_i=Intensity value of the surrounding pixel.
I_c=Intensity value of the central pixel.

$$S^E\big(I_i^E, I_c^E, T_s^E\big) = \begin{cases} 1 & I_i^E \geq I_c^E + T_s^E \\ 0 & I_i - I_c^E < T_s^E \\ -1 & I_i \leq I_c^E - T_s^E \end{cases} \tag{6}$$

where; E=ELTP ternary matrix.
T_s=Static threshold value
I_i^E=Intensity of the surrounding pixel
$M=I_i^E \mid i=0, 1, 2, 3….8 \mid$
I_c^E=Mean(M)
T_s^E=MAD(M)

In ELTP, the intensity of the central pixel is obtained by the upper case and lower case ELTP matrix. We take a 3x3 matrix of the image and generate a new ternary matrix. The value assigns to surrounding pixels is based on (6). Further, it was divided into positive and negative matrices in positive matrix 0 and -1intensity represented by 0 and in negative matrix 0 and 1 intensity represented by 0 and -1 intensity represented by 1, shown in Figure 4 [27]. Central pixel intensity is evaluated by (7) of the coordinate (m, n).

$$ELTP_{m,n}=ELTP\_P_{m,n} * (m + 2) - (ELTP\_P_{m,n} * (ELTP\_P_{m,n}+ 1)) \,/\, 2 + ELTP\_N_{m,n} \tag{7}$$

Where

$$ELTP\_P_{m,n}=\sum_{i=0}^{N-1} e(S^E\,(I_i^E, I_c^E, T^E),\, 1)$$

$$ELTP\_N_{m,n}=\sum_{i=0}^{N-1} e(S^E\,(I_i^E, I_c^E, T^E),\, -1)$$

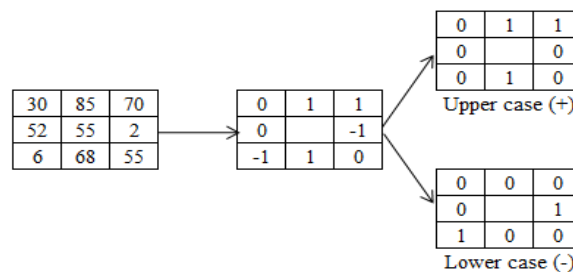$$e\,(X, Y) = \begin{cases} 1, \text{if } X = Y \\ 0, \text{if } X \neq Y \end{cases}$$

Figure 4. Positive and negative matrix representation through ELTP

3.3. Edge-Otsu based enhanced local ternary pattern

In our proposed work, we use the Edge-Otsu based enhanced local ternary pattern (EOELTP) technique for image forgery detection. In EOELTP, edge texture feature is used to implement Otsu based

enhanced local ternary pattern. We implement Canny edge detection technique, which is the most popular edge detector. Due to the implementation of the edge detection technique, the performance of the global threshold has been improved after considering the pixels which lie on or near the object and background. Before implementing the predefine ELTP technique, we implement the Canny edge detection technique to improve the performance of the global threshold by which the performance of ELTP has been improved the performance of the edge, the effect of Otsu technique represented by Figure 5.
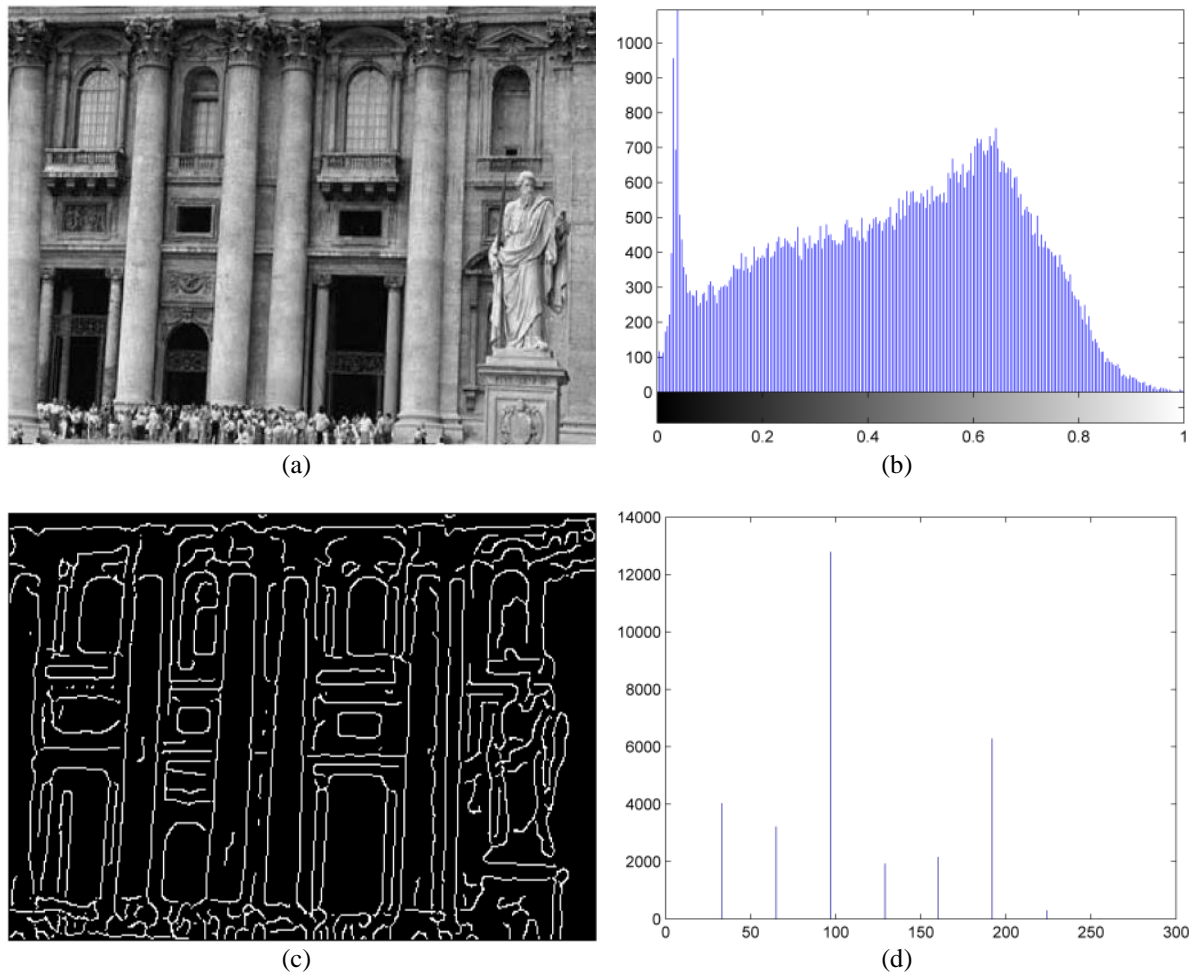

(a)

(b)

(c)

(d)

Figure 5. These figures are; (a) gray image, (b) histogram of gray image, (c) image after edge detection algorithm, (d) histogram after implementing Otsu on edge image

4. RESULTS AND DISCUSSION
4.1. Evaluation matrix

To evaluate the performance of the proposed work, we use the accuracy parameter. Accuracy of the process is based on true positive (TP), true negative (TN), false positive (FP), false negative (FN) component. It's represented by (8).

$$Accuracy = 100 \times (TP + TN)/(TP + FP + TN + FN) \qquad (8)$$

where; TP: Identify fake image as a fake
TN: Original image identify as a original
FP: Original image identify as aoriginal
FN: Fake image identify as a fake

4.2. Database and classifier

The proposed work is evaluated on three open source available image databases, CASIA v1, CASIA v2, and Columbia. CASIA v1 has 1721 RGB images of different sizes 384 x 256 and 256 x 384. In this database, 800 images are pristine, and 921 are tampered. CASIA v2 has 12614 different image datasets like JPEG, BMP, and TIFF. In this, 7491 images are pristine, and 5123 are fake. In Columbia, different camera types are used for data collection, Canon G3, Canon 350D RebelXT, NikonD70, and Kodak DCS330, generating an uncompressed image of size 757 x 569 and 1152 x 768 sizes. To classify these images SVM is used, gives awe-inspiring results over the small and big datasets, and easy to implement.

4.3. Experimental results and comparison

The result of the proposed work is based on the accuracy of the forgery detection on different image datasets, CASIA v1, CASIA v2, and Columbia. We compare our work with the previous technique and previous state of work in terms of accuracy. The accuracy of the proposed work is 99.98% on CASIA v1.0, 99.03% on CASIA v2, and 98.56% on the Columbia image dataset is shown in Figure 6 and compares the proposed work accuracy with different states of work [6], [10], [12], [15], [26] is shown in Table 1.
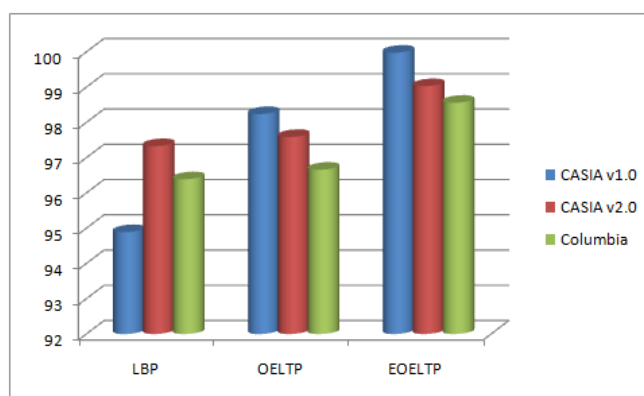

Figure 6. Accuracy result of proposed technique

Table 1. Comparison of proposed work accuracy with previous state of work

Techniques	CASIA v1.0	CASIA v2.0	Columbia
He *et al.* [10]	89.76	89.76	−
Muhammad *et al.* [12]	94.89	97.33	96.39
Goh and Thing [15]	90.18	96.21	−
Alahmadi *et al.* [6]	97.5	−	−
Kanwal, N. *et al* [26]	98.65	98.01	97.23
Proposed	99.98	99.03	98.56

5. CONCLUSION

In this paper, we discuss edge texture feature extraction using OELTP techniques for forgery detection. A multi-level wavelet transform is implemented over the chrominance component of the image to get the import details in the form of the frequency domain. The Canny edge detection technique is implemented over the frequency domain to obtain a better global threshold with the help of the Otsu technique. Extracted feature by enhanced local ternary pattern classified by SVM to get the image is forged or not. Our proposed approach obtains progress with other states of artwork in terms of accuracy. The accuracy of the proposed work is 99.98% on CASIA v1.0, 99.03% on CASIA v2, and 98.56% on the Columbia image dataset. We do not get better results when the background illumination is highly non-uniform. In the future, we need to develop such system which is reliable for highly non-uniform surface or background.

REFERENCES

[1] Y. Hsu and S. Chang, "Detecting Image Splicing using Geometry Invariants and Camera Characteristics Consistency," *2006 IEEE International Conference on Multimedia and Expo*, 2006, pp. 549-552, doi:

       10.1109/ICME.2006.262447.

[2]   H. Yao, S. Wang. X. Zhang, C. Qin and J. Wang, "Detecting image splicing based on noise level inconsistency," *Multimedia Tools Applications*, vol. 76, no. 10, pp. 12457-12479, 2017, doi: 10.1007/s11042-016-3660-3.

[3]   P. Zhang and X. Kong, "Detecting Image Tampering Using Feature Fusion," *2009 International Conference on Availability, Reliability and Security*, 2009, pp. 335-340, doi: 10.1109/ARES.2009.150.

[4]   G. Chierchia, G. Poggi, C. Sansone and L. Verdoliva, "A Bayesian-MRF Approach for PRNU-Based Image Forgery Detection," in *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 4, pp. 554-567, April 2014, doi: 10.1109/TIFS.2014.2302078.

[5]   M. Chen, J. Fridrich, M. Goljan and J. Lukas, "Determining Image Origin and Integrity Using Sensor Noise," in *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 1, pp. 74-90, March 2008, doi: 10.1109/TIFS.2007.916285.

[6]   A. Alahmadi, M. Hussain, H. Aboalsamh, M. Ghulam, G. Bebis and H. Mathkour, "Passivedetectionof image forgery using DCT and local binary pattern," *Signal, Image and Video Processing*,vol. 11, no. 1, 81-88, 2016, doi: 10.1007/s11760- 016-0899-0.

[7]   M. Hariri and F. Hakimi, "Image-splicing forgery detection based on improved LBP and K- nearest neighborsalgorithm," *Electronic information and planning*, vol. 3, 2015.

[8]   F. Hakimi, M. Hariri and F. G. Baghi, "Image splicing forgery detection using local binary pattern and discrete wavelet transform," *2015 2nd International Conference on Knowledge-Based Engineering and Innovation (KBEI)*, 2015, pp. 1074-1077, doi: 10.1109/KBEI.2015.7436195.

[9]   Z. He, W. Sun, Z. Wei and H. Lu, "Digital image splicing detection based on approximate run length," *Pattern Recognition Letters*, vol. 32, no. 12, pp. 1591-1597, 2011, doi: /10.1016/j.patrec.2011.05.013.

[10] Z. He, W. Lu, W. Sun and J. Hwang, "Digital image splicing detection based on Markov features in DCT and DWT domain," *Pattern Recognition*, vol. 45, no. 12, pp. 4292-4299, 2012, doi: 10.1016/j.patcog.2012.05.014.

[11] A. Shah and E. El-Alfy, "Image Splicing Forgery Detection Using DCT Coefficients with Multi-Scale LBP*," 2018 International Conference on Computing Sciences and Engineering (ICCSE)*, 2018, pp. 1-6, doi: 10.1109/ICCSE1.2018.8374214.

[12] M. Ghulam, M. Al-Hammadi, M. Hussain and G. Bebis, "Image forgery detection using steerable pyramid transform and local binary pattern," *Machine Vision and Applications*, vol. 25, no. 4, pp. 985-995, 2014, doi: 10.1007/s00 138-013-0547-4.

[13] S. Agarwal and S. Chand, "Image Forgery Detection using Multi-Scale Entropy Filter and Local Phase Quantization*," International Journal of image, Graphics and Signal Processing*, vol. 10, no. 10, pp. 78-85, 2015, doi: 10.5815/ijigsp.2015.10.08

[14] P. Cavalin and L. S. Oliveira, "A Review of Texture Classification Methods and Databases," *2017 30th SIBGRAPI Conference on Graphics, Patterns and Images Tutorials (SIBGRAPI-T)*, 2017, pp. 1-8, doi: 10.1109/SIBGRAPI-T.2017.10.

[15] J. Goh and V. L. L. Thing, "A hybrid evolutionary algorithm for feature and ensemble selection in image tampering detection," *International journal of electronic security and digital forensic*, vol. 7, no. 1, pp. 76-104, 2015, doi:10.1504/IJESDF.2015.067996.

[16] T. Ojala, M. Pietikainen and T. Maenpaa, "Multiresolution gray-scale and rotation invariant texture classification with local binary patterns," in *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 24, no. 7, pp. 971-987, July 2002, doi: 10.1109/TPAMI.2002.1017623.

[17] V. Srivastavaven and S. K. Yadav, "Digital Image splicing Detection Using RIC-LBP Feature Extraction Technique," *2020 Sixth International Conference on Parallel, Distributed and Grid Computing (PDGC)*, Waknaghat, India, 2020, pp. 84-87, doi: 10.1109/PDGC50313.2020.9315812.

[18] R. Nosaka, C. H. Suryanto and K. Fukui, "Rotation invariant co-occurrence among adjacent LBPs," in *Proceedings of the Asian Conference on Computer Vision*, Korea, 2012, pp.15-25, doi: 10.1007/978-3-642-37410-4_2.

[19] S. Agarwal and S. Chand, "Texture Operator Based Image Splicing Detection Hybrid Technique," *2016 Second International Conference on Computational Intelligence & Communication Technology (CICT)*, 2016, pp. 116-120, doi: 10.1109/CICT.2016.31.

[20] X. Tan and B. Triggs, "Enhanced Local Texture Feature Sets for Face Recognition Under Difficult Lighting Conditions," in *IEEE Transactions on Image Processing*, vol. 19, no. 6, pp. 1635-1650, June 2010, doi: 10.1109/TIP.2010.2042645.

[21] V. Srivastava and S. K. Yadav, "Texture Operator based Digital Image Splicing Detection using ELTP Technique," *2020 9th International Conference System Modeling and Advancement in Research Trends (SMART)*, 2020, pp. 345-348, doi: 10.1109/SMART50582.2020.9337095.

[22] T. J. de Carvalho, C. Riess, E. Angelopoulou, H. Pedrini and A. de Rezende Rocha, "Exposing Digital Image Forgeries by Illumination Color Classification," in *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 7, pp. 1182-1194, July 2013, doi: 10.1109/TIFS.2013.2265677.

[23] C. Cortes and V. Vanik, "Support-vector networks," *Machine Learning*, vol.20, no. 3, pp. 273-297, 1995, doi: 10.1007/BF00994018.

[24] J. Dong, W. Wang and T. Tan, "CASIA Image Tampering Detection Evaluation Database," *2013 IEEE China Summit and International Conference on Signal and Information Processing*, 2013, pp. 422-426, doi: 10.1109/ChinaSIP.2013.6625374.

[25] K. Asghar, X. Sun, P. L. Rosin, M. Saddique, M. Hussain and Z. Habib, "Edge–texture feature-based image forgery detection with cross-dataset evaluation," *Machine Vision and Applications*, vol. 30, pp. 1243–1262, 2019, doi: 10.1007/s00138-019-01048-2.
[26] N. Kanwal, A. Girdhar, L. Kaur and J. S. Bhullar, "Digital image splicing detection technique using optimal threshold based local ternary pattern," *Multimedia Tools and Applications*, vol. l79, pp. 12829-12846, 2020, doi: 10.1007/s11042-020-08621-2.
[27] J.-H. Yuan, H.-D. Zhu, Y. Gan and L. Shang, "Enhanced local ternary pattern for texture classification," In: *International conference on intelligent computing, Springer*, vol. 8588, pp. 443–448,2014, doi: 10.1007/978-3-319-09333-8_48.

BIOGRAPHIES OF AUTHORS

Vikas Srivastava has received his B.Tech from VBS Purvanchal university, Jaunpur in Computer Science and Engineering and his M.tech from RGPV, Bhopal in CTA. He is pursuing Ph.D in Department of Computer Science and Information Technology from Sam Higginbottom University of Agriculture, Technology and Sciences, Prayagraj, U.P., India.

Sanjay Kumar Yadav did his MCA from Lucknow University, Lucknow, and M.Tech. in Computer Science from Motilal Nehru National Institute of Technology, Allahabad, and Ph.D from SHIATS-DU, Allahabad. Presently working as aAssociate Professor in Department of Computer Science and Information Technology, Sam Higginbottom University of Agriculture, Technology and Sciences, Prayagraj, U.P., India.