ISSN: 0067-2904

Image Forgery Detection Using Histogram-Oriented Gradients (HOG)

Iman Sedeeq
Veterinary Public Health Department, Veterinary Medicine College, Mosul University, Mosul, Iraq

Received: 25/9/2023 Accepted: 9/2/2024 Published: 30/5/2025

Abstract

Due to their capacity to influence people and their usage in news, courts, medical, and military applications, verifying the authenticity of any shared images has become crucial. Image manipulation has become so simple with modern technology. This research introduces a forgery detection method that utilizes the Histogram-Oriented Gradients (HOG) descriptor. This descriptor is established by accumulating the edge orientations caused by image manipulation by a 1D histogram over an image region. The suggested method extracts HOG features in the YCbCr color space of high-frequency discrete wavelet transform (DWT) sub-bands. Later, these features are fed to a classifier to confirm the authenticity of the image or not. Two free datasets, Casia v1.0 and Casia v2.0, were used to evaluate the proposed method. The performance evaluation showed that the HOG descriptor can be utilized to detect image forgery efficiently, with an accuracy of 91.45% for Casia v1.0 and 89.67% for Casia v2.0. The aforementioned accuracies showed that the HOG descriptor can successfully be used to detect image forgery.

Keywords: Image forgery; Histogram of oriented gradients; Discrete wavelet transform, YCbCr

الكشف عن تزييف الصورة باستعمال الرسم البياني للانحدارات الموجهة

ايمان ذنون صديق

قسم الصحة العامة البيطرية, كلية الطب البيطري, جامعة الموصل, نينوى, العراق

الخلاصة

ان للصور القدرة على التأثير في اراء الأشخاص ولأنها تستعمل في نشرات الاخبار والمحاكم والتطبيقات الطبية والعسكرية أصبح من الضرورة التحقق من صحة هذه الصور المتداولة. ومع توفر التقنيات الحديثة هذه الأيام أصبح تزييف الصور امرا في غاية السهولة. يقدم هذا البحث طريقة للكشف عن تزييف الصور تستعمل واصف الرسم البياني للانحدارات الموجهة Histogram Oriented of Gradients (HOG) . يتم انشاء هذا الواصف من خلال الرسم البياني لاتجاهات الحواف التي تنتج عن تزييف الصور. ان الطريقة المقترحة تستخرج ميزات HOG للمعاملات ذات الترددات العالية لتحويل الموجات المنفصلة Discrete Wavelet Transform (DWT) في فضاء الألوان YCbCr . بعد ذلك يتم ارسال هذه الميزات الى مصنف ليتم تحديد صحة الصورة من عدمها. تم استعمال مجموعتين من الصور متوفرة على الانترنت Casia v1.0 و Casia v2.0 لتقييم أداء الطريقة المقترحة. بلغت دقة التصنيف 91.45% لـ Casia v1.0 و89.67% لـ

*Email: imansedeeq@uomosul.edu.iq

Casia v2.0. ان الدقة المذكورة اثبتت أنه بالإمكان استعمال واصف HOG للكشف عن تزييف الصورة بنجاح.

1. Introduction

Nowadays, videos and digital images are the most common shared content on the Internet. People may forget a text, but they won't forget a picture or a video that tells a story. Also, with the prevalence of social media, people are used to documenting their everyday lives using images. As a result, images serve as the primary information carrier. Digital technologies such as smartphones, digital cameras, and the availability of free image-editing tools facilitate digital image manipulation [1]. Consequently, a surge of forged images with no visual alteration has been arising on the web. These images have become a source of fake news and fabricated evidence in many applications. This establishes a challenge about the authenticity of online shared images [2]. This challenge may consist of two steps: 1) to verify if an image is forged or not; 2) to localize the forged part. There are two commonly used ways of manipulating photos: 1) splicing, which involves creating a fake image by combining two or more images; and 2) copy-moving, which involves duplicating a portion of an image many times inside the same image to conceal information [3, 4].

Researchers have focused on image forgery detection to develop algorithms capable of detecting image alteration. The detection techniques can be categorized as either passive or active. Passive detection algorithms are used when there is no prior information available about the analyzed image. On the other hand, active detection strategies include inserting a verification code, such as a watermark or a signature, into the image before sending it [5]. The authentication of the received image is verified when the receiver validates the presence of the verification code by comparing it with the original image.
It is critical to choose a suitable feature descriptor for detecting changes in the image caused by forgery. Histogram of Oriented Gradients (HOG) is a local descriptor that takes into consideration not only the identification of edges caused by splicing or copy-move in the image but also the direction and magnitude of these edges [6]. The discrete wavelet transform (DWT) is an effective tool to recognize these edges (high frequencies). The DWT coefficients of the image are grouped into four sub-bands: low frequencies are represented by the LL sub-band, high frequencies are represented by the LH and HL sub-bands for horizontal and vertical edges, respectively, and finally, the HH sub-band represents diagonal edges [7, 8]. Moreover, looking for a color space that always has room for data hiding or image manipulation, such as the YCbCr color space, is beneficial as well. In this color space, there are three components: luminance (component Y) and chroma (components Cb and Cr). The luminance channel (Y) is far more responsive to human eyes than the chroma channel (Cb and Cr) [9]. In this paper, the usage of HOG to describe local alterations (edges) when DWT is applied to the image in YCbCr color space is investigated. This paper is organized as follows: Section 2 presents some of the previous work with respect to image forgery detection approaches. Section 3 introduces the histogram of oriented gradients (HOG) and the required steps to obtain these features. The suggested methodology is given in Section 4. Section 5 explains in detail the performance evaluation of the proposed method. Finally, some conclusions and future work are given in Section 6.

2. Related Work

There has been a lot of research done on image forgery detection. As a result, there are numerous techniques for identifying and locating various image alterations. The detection of image forgery is a binary classification task, so a classifier is needed to determine if an image is authentic or not. These classifiers are built using machine-learning algorithms. Detection

approaches, as mentioned in Section 1, have two categories: active and passive. Active approaches employ a verification-inserted code, while passive approaches need no special equipment or software to add the verification code. In addition, passive detection approaches utilize the changes in statistical characteristics of the image that are caused by image forgery; therefore, passive approaches are more common [10]. In this section, a sample of these approaches is presented.

Wei Wong et al. [11] proposed a detection method based on a co-occurrence matrix. This matrix assists in capturing image edges by describing the relationship between any two pixels at a specific direction (vertical, horizontal, primary diagonal, and secondary diagonal) and distance. Then, these four-direction matrices are cascaded to be the input to the Support Vector Machine (SVM) classifier.

In their study, Amani A. Alahmadi et al. [12] proposed a novel technique for identifying splicing forgeries. This technique involved calculating the local binary pattern (LBP) for every overlapping image block in order to detect such forgeries. Subsequently, the discrete cosine transform (DCT) was implemented, followed by the extraction of features using the standard deviation. These features were then input into the SVM classifier. The approach attained a precision of 97%.

In their study, Davide Cozzolino et al. [13] employed a descriptor that specifically highlights edges resulting from picture alteration rather than the actual image content in order to identify instances of image forgeries. This descriptor employed a series of high-pass filters, including linear, horizontal, and nonlinear filters, to acquire the edges. Next, the co-occurrence matrix was calculated for the residuals in order to serve as an input feature for the SVM classifier. The accuracy of the proposed approach was 94%.

Han et al. [14] proposed a novel approach for extracting Markov characteristics in the frequency domain by utilizing DCT coefficients. This approach computes the disparity of discrete cosine transform (DCT) coefficients in the horizontal, vertical, and diagonal directions. Markov characteristics were extracted based on the direction with the greatest difference. The algorithm demonstrated a precision rate of 92%.

Mahale Vivek Hilal et al. [15] employed histograms of oriented gradients for feature extraction in order to identify instances of copy-move forgeries. The process commenced with partitioning the image into overlapping blocks, followed by the extraction of HOG features from each block. Subsequently, the Euclidean distance was employed, using the determined threshold, to detect duplicate regions through a matching process.
Chandhany Shyan Prakash et al. [16] proposed a technique that employed both the discrete cosine transform (DCT) and Zernike moments to identify instances of both copy-move and splicing. To detect splicing, the image was divided into non-overlapping blocks and subjected to a discrete cosine transform (DCT) to extract distinctive features. Furthermore, Zernike seconds were utilized for the purpose of identifying instances of copy-move forgeries. The proposed method attained a 99% accuracy in detecting picture splicing and an 87.5% accuracy in detecting copy-move forgery.

In their study, Mohammed Hazim Alkawaz et al. [17] demonstrated the impact of various DCT block sizes on the detection of forgeries, namely copy-move manipulation. Initially, the image underwent a transformation to grayscale and was thereafter divided into overlapping pieces. The dimensions of these blocks were 4x4 and 8x8 pixels. Next, the discrete cosine transform (DCT) was utilized on each block to acquire the DCT coefficients. Then, these

blocks were sorted using lexicographic order to find blocks with the same features so duplicate regions could be recognized.

Hamid A. Jalab et al. [18] suggested a methodology that started by transforming the examined image to YCbCr color space. Then, DWT was applied to the luminance (Y) and chroma (Cb and Cr) channels. Next, a non-overlapping block-based method of 8x8 was utilized per channel. This method calculates the fractional entropy per block to be combined later to construct the feature vector for the classifier.

Muhammad Hameed Siddiqi et al. [19] utilized a technique that applied DWT to non-overlapping blocks. The local changes were then captured by extracting weighted local binary patterns for each pixel using a 3x3 window. The input feature vector for the classifier was created by joining the histograms of these binary patterns. The best accuracy recorded was 98.9%.

Kurshid Asghar et al. [20] used a scheme that found the noise patterns of forged images were no more like those of authentic images. The researchers estimated these patterns using Fast Fourier Transform FFT and high-pass filters. Later, a descriptor of local binary patterns (LBP) was used to analyze the texture region to detect forgeries. Their scheme achieved an accuracy of 99.21%.

Dalia S. Sulaiman et al. [21] employed a second version of the classic Neural Network (NN) algorithm to build a classifier. The algorithm has two differences: a) it does not use gradient, and b) all parameters are set at once (no need to iteratively learn these parameters). It is known as an Extreme Learning Machine (ELM). Thus, ELM is much faster than classic NN. The input to ELM is the LBP of non-overlapped blocks of 3x3 pixels in YCbCr color space. The obtained accuracy was 99.7%.

The work in this paper utilized extracted HOG features of the image in YCbCr color space to detect image alteration. These discriminative features were obtained using high-frequency sub-bands of DWT of luminance (Y) and chroma (Cb and Cr) channels to form a feature vector for a multilayer perceptron classifier in the Weka environment [22] to decide whether the examined image is forged or not. Later, a performance evaluation of the proposed methodology is given in detail in this paper.

3. Histogram of Oriented Gradients

In this section, an introduction to HOG is given. HOG is a feature descriptor that is utilized in computer vision to detect objects. Basically, its process starts by counting instances of gradient orientation within a specific part of an image [23]. The HOG descriptor emphasizes an object's structure or shape by ignoring irrelevant information. The main goal of HOG is to record local intensity changes and their directions, which are crucial for describing the forms and structures of objects. In subsection 3.1, steps for generating HOG features are presented.

3.1 Generation of HOG Features

The process to acquire HOG features can be shown in Fig. 1. These steps can be summarized as follows [24]:

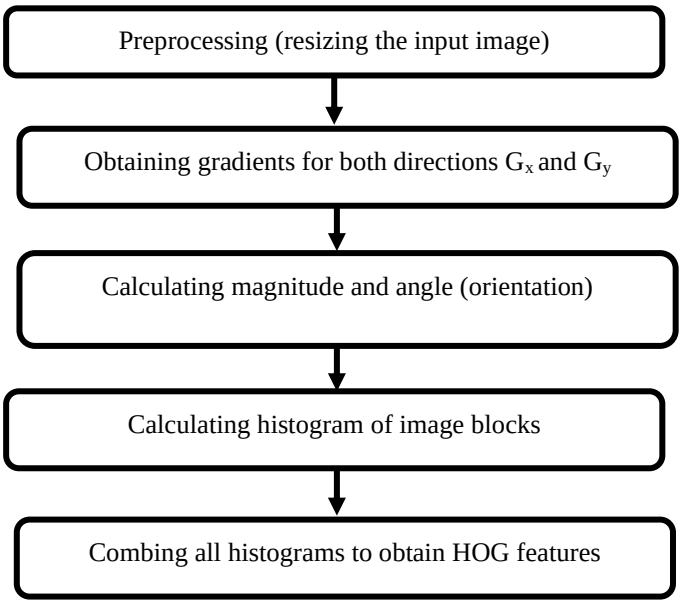

Figure 1: Process of HOG feature generation

1. Preprocessing : resizing the input image to simplify the calculations.
2. Obtaining the gradients for both directions G_x and G_y for each pixel in the image using Eqs. 1 and 2, respectively, by calculating the central differences of pixels in a 3x3 window:

$$G_x(r,c) = I(r, c+1) - I(r, c-1) \quad (1)$$
$$G_y(r,c) = I(r-1, c) - I(r+1, c) \quad (2)$$

Where I(r,c) is a pixel intensity in image I in row r and column c. Areas around the edges caused by image forgeries usually have higher differences.
3. Obtaining the magnitude and angle or orientation for each pixel using Eqs. 3 and 4, respectively:

$$\text{Magnitude}(\mu) = \sqrt{G_x{}^2 + G_y{}^2} \quad (3)$$
$$\text{Angle}(\Theta) = |tan^{-1}(G_y/G_x)| \quad (4)$$

4. Dividing the image into non-overlapping blocks of size (BxB) and generating a histogram using magnitudes and angles for each cell according to magnitudes and orientations obtained from step 3. The histogram is produced using N bins.
5.Combining all the normalized features obtained from all blocks to get HOG features for the whole image to be an input feature vector for a classifier. This classifier determines if the given image is authentic or not.
Figure 2 presents the sequence of steps implemented to obtain HOG features.

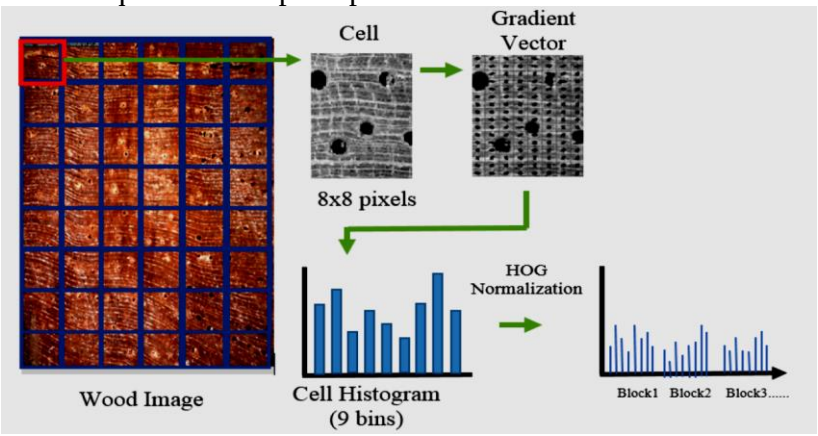

Figure 2: Steps Sequence to Obtain HOG Features [25]

4. The Suggested Methodology

Since edges are a natural product of image forgeries, collecting information about them is useful to detect these forgeries. As mentioned in Section 3, HOG computes the features using both the magnitude and the angle of the gradient; therefore, it is superior to other edge descriptors. It creates histograms for the areas of the image based on the gradient's magnitude and directions. Figure 3 shows the required steps to detect image alterations using the HOG descriptor. These steps can be summarized as follows:

1. Transforming an input image into YCbCr color space.
2. Collecting DWT coefficients for each channel (Y, Cb, and Cr).
3. Extracting HOG features for each sub-band (LH, HL, and HH) of each channel (Y, Cb, and Cr) according to the steps mentioned in Subsection 3.1.
4. Feeding extracted features from step 3 to a classifier to examine the authenticity of the image under investigation.

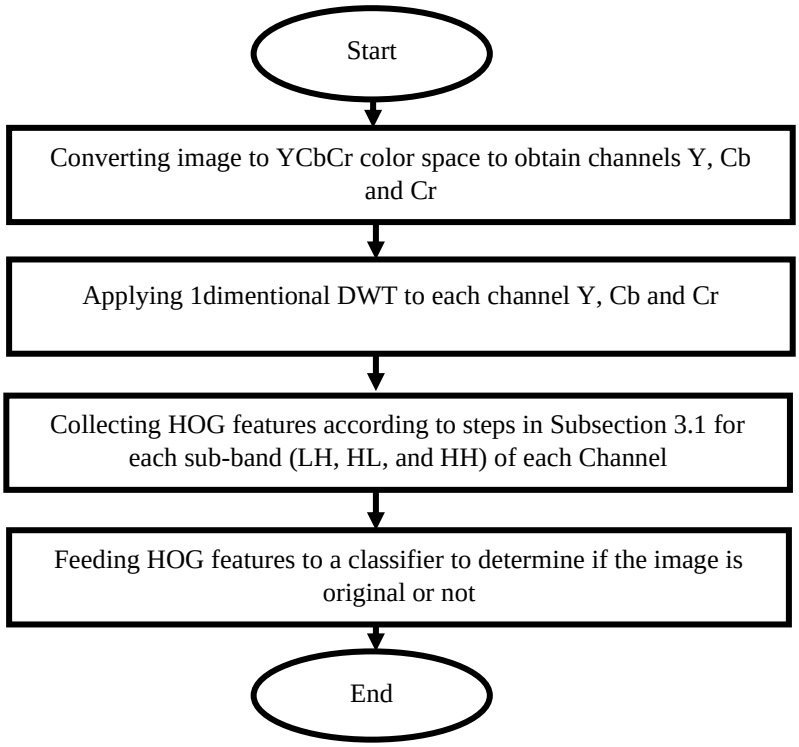

Figure 3: Steps of the Suggested Methodology

5. EXPERIMENTS

In this section, an experimental design and implementation are given. A description of the datasets used in the proposed study to detect image forgeries is given as well. Three experimental sets were conducted, and their results are presented in subsections 5.1, 5.2, and 5.3, respectively. The objective of the first experimental set was to investigate the efficiency of the proposed HOG features to detect image forgery. The objective of the second experimental set was to examine the impact of HOG block size on the classifier's accuracy. Finally, the objective of the third experimental set was to compare our proposed method with some proposed methods in Section 2. In all experimental sets, steps in Fig. 1 were implemented to collect HOG features.

Two freely available datasets, Casia v1.0 and Casia v2.0 [26], were used in the experiments to evaluate the performance of the proposed detection method. Casia v1.0 included 1721 images and was divided into two groups: 800 authentic images and 921 forged

images. These images were of sizes 384×256 and 256×384 and were all in JPG format. Casia v2 had two groups of images as well. The number of authentic images was 7942, while the number of forged images was 5124. The images in Casia v2.0 were in JPG, TIF, and BMP of sizes 240×160 to 900×600. A sample of utilized images in the proposed study from two datasets is shown in Figure 4, respectively.

(a) Original images from Casia v1.0

(b) Forged images from Casia v1.0

(c) Original images from Casia v2.0

(d) Forged images from Casia v2.0

Figure 4: Sample of used images from Casia v1.0 and Casia v2.0

Two evaluation metrics were used: 1) Accuracy Acc (the proportion of all correctly predicted forged images over all images), and 2) Area Under the Curve AUC of the Receiver Operating Characteristic ROC [27]. AUC, which serves as a summary of the ROC curve, is a measurement of a binary classifier's capacity to distinguish between classes. The ROC plots the false positive rate (FPR) against the true positive rate (TPR) to show how many fake images were correctly identified. The FPR also shows how many real images were correctly identified. The curve is made up of different threshold values. When AUC = 1, this means that the classifier model classified all authentic and forged images correctly, while when AUC = 0, no image is correctly classified. The classifier used was Multilayer Perceptron in Weka with default settings.

5.1 HOG Performance to Detect Forgeries:

Table 1 shows the results of the first experimental set. This set was to verify how well-extracted HOG features detect image forgery. This table shows the accuracy (acc) and area under the curve (AUC) for each DWT high-frequency sub-band: LH (horizontal), HL (vertical), and HH (diagonal) for Y, Cb, and Cr. The HOG features were extracted according to the steps mentioned in Section 3, with a block size of 8x8. From the table, it is shown that

the best results (bold font) of Acc = 91.45% and AUC = 0.96 were achieved for the Casia v1.0 dataset, while for Casia v2.0, Acc = 89.67% and AUC = 0.95 were achieved. Both best results were attained using extracted HOG features using the HH (diagonal) subband for Cb (Casia v1.0) and Cr (Casia v2.0) channels, respectively. These promising results prove the efficiency of using HOG features to detect image forgery.

Table 1: Performance of the proposed detection method

Channel	DWT sub-band	Casia v1.0		Casia v2.0	
		Acc 100%	AUC	Acc 100%	AUC
Y	LH	87.56	0.93	57.48	0.59
	HL	82.91	0.88	58.22	0.60
	HH	80.30	0.86	61.91	0.64
Cb	LH	85.29	0.91	80.75	0.88
	HL	80.88	0.88	83.70	0.90
	HH	**91.45**	**0.96**	88.43	0.95
Cr	LH	69.14	0.72	81.60	0.89
	HL	67.44	0.70	83.80	0.90
	HH	87.27	0.93	**89.67**	**0.95**

5.2 The Impact of HOG Block Size:

A second experimental set was conducted to show how HOG block size influences the accuracy and AUC of the classification model. Table 2 shows the accuracy (Acc) and AUC obtained using different block sizes while extracting HOG features. From the table, it can be observed that the highest accuracy and AUC for both datasets, Casia v1.0 and Casia v2.0, were obtained using block sizes of 8x8 pixels. Accuracy = 91.45% and AUC = 0.96 were fulfilled for the Casia v1.0 dataset, while for the Casia v2.0 dataset, accuracy = 89.67% and AUC = 0.95 were achieved. Also, it is worthy to notice from the table that increasing the block size from 8x8 to 16x16 and then to 32x32 caused a drop in accuracy and AUC for both datasets because the smaller the block size, the sharper magnitude changes can be captured whenever encountering edges. Thus, preparing data for any classification model is critical.

Table 2: Impact of HOG block size on Acc and AUC

Block size	Casia v1.0		Casia v2.0	
	Acc 100%	AUC	Acc 100%	AUC
8x8	**91.45**	**0.96**	**89.67**	**0.95**
16x16	75.01	0.80	80.22	0.80
32x32	69.72	0.74	68.59	0.76

This is also clearly shown in Figure 5, which plots FPR (x-axis) against TPR (y-axis) to get the AUC-ROC area under the curve of the receiver operating characteristic. This shows how good or bad the classification model is. From the figure, it can be noted that the best achieved AUC for both datasets was when using a block size of 8x8 (AUC = 0.96 for Casia v1.0 and 0.95 for Casia v2.0) to extract HOG features, while the worst achieved AUC was when using a block size of 32x32 (AUC = 0.74 for Casia v1.0 and 0.76 for Casia v2.0).

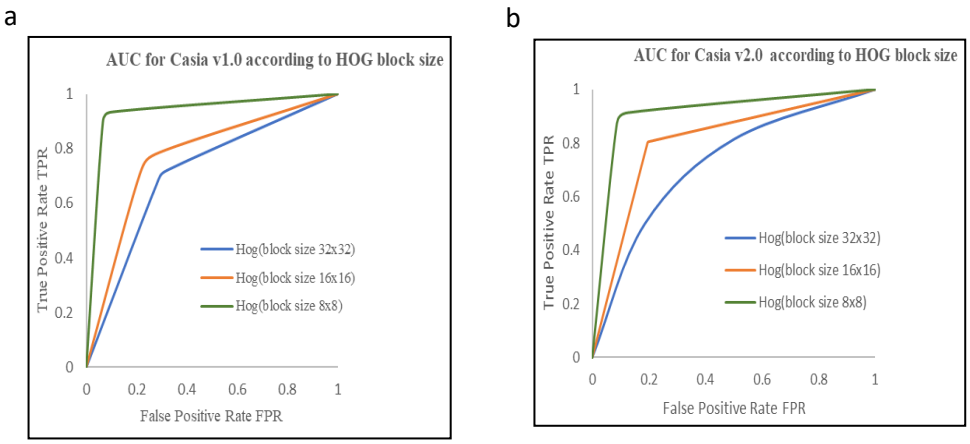

Figure 5: The influence of HOG block size on AUC (a) AUC for Casia v1.0; (b) AUC for Casia v2.0

5.3 Comparison with Some Previous Work

In this subsection, the results of the third experimental set are presented. An evaluation of the proposed method's performance in comparison with some previous work is given. The methods mentioned in [11] and [13] in Section 2 were chosen to be compared to our proposed method. Both methods were implemented according to their procedures. These two methods used a common local region descriptor called the co-occurrence matrix, which attracted many researchers. Table 3 presents the obtained results. From the table, it can be shown that the proposed detection method achieved the best performance on Casia v1.0 with Acc = 91.47% and AUC = 0.96 over both methods in [11] and [13]. Also, regarding Casia v2.0, the proposed method achieved the best AUC of 0.95.

Table 3: Performance of the proposed detection method with respect to some related work

Method	Casia v1.0		Casia v2.0	
	Acc 100%	AUC	Acc 100%	AUC
M. in [11]	66	0.65	91	0.91
M. in [13]	63.97	0.62	62.64	0.54
Proposed method	**91.45**	**0.96**	**89.67**	**0.95**

6. Conclusions

This research has shown that detection of image forgeries can be accomplished using HOG descriptors. This HOG descriptor was acquired for the DWT diagonal high-frequency sub-band of Cb and Cr channels in the YCbCr color space. Two datasets, Casia v1.0 and Casia v2.0, were used to evaluate the performance of the detection method. The proposed method offered promising results in terms of classification accuracy and AUC. The achieved accuracy for Casia v1.0 was 91.45% and the AUC was 0.96, while for Casia v2.0, the obtained accuracy was 89.67% and the AUC was 0.95 in comparison with some related work. These results were achieved when the HOG block size was 8x8 pixels. It has been shown in the research that the block size while extracting HOG features affected the classifier accuracy and AUC. The bigger the block size, the lower the accuracy and AUC. The next step in future work is to improve the method's accuracy. This could be done by combining features with HOG features such as Scale-Invariant Feature Transform (SIFT), where the image orientation has no effect on SIFT features. Also, HOG can be used to localize the forged region in the image.

References

[1] K. Hilal, and E. Abdullah, "Forensic Analysis of Images on Online Social Network: A Survey," *In: Ranganathan, G., Fernando, X., Piramuthu, S. (eds) Soft Computing for Security Applications. Advances in Intelligent Systems and Computing*, Springer, Singapore, vol. 1428, pp. 237–255, 2022. Available: https://doi.org/10.1007/978-981-19-3590-9_19.

[2] E. Talib, N. F. Hassan, and A. S. Jamil, "The Defensive Methods Against Deepfake: Review ,"*Iraqi Journal of Science*, vol. 64, no. 10, pp 5345–5357, 2023 https://doi.org/10.24996/ijs.2023.64.10.39.

[3] A. F. Sewan and M.S. Altaei, " Copy Move Forgery Detection Using Forensic Images," *Iraqi Journal of Science*, vol. 62, no. 9, pp. 3167-3181, 2021. Available: https://doi.org/10.24996/ijs.2021.62.9.31.

[4] G.K. Birajdar, and V.H. Mankar, "Digital Image Forgery Detection Using Passive Techniques: A Survey," *Digital Investigation: The International Journal of Digital Forensics & Incident Response*, vol. 10, no. 3, pp. 226-245, 2013. Available: https://doi.org/10.1016/j.diin.2013.04.007.

[5] H. M. Al-Dabbas, R. A. Azeez, and A. E Ali, "Digital Watermarking, Methodology, Techniques, and Attacks: A Review," *Iraqi Journal of Science*, vol 64, no. 8, pp. 4169–4186, 2023. Available: https://doi.org/10.24996/ijs.2023.64.8.37.

[6] N. Dalal, and B. Triggs, "Histograms of Oriented Gradients for Human Detection," *International Conference on Computer Vision & Pattern Recognition (CVPR '05)*, vol. 1, pp.886–893, 2005. Available: https://doi.org/10.1109/CVPR.2005.177.

[7] M. Zampoglou, S. Papadopoulos, and I. Kompatsiaris, "Large-scale Evaluation of Splicing Localization Algorithms for Images," *Multimedia Tools and Applications*, vol. 76, no. 4, pp. 4801-4834, 2017. Available: https://doi.org/10.1007/s11042-016-3795-2.

[8] Y.Q. Shi, G. Xuan, D. Zou, J. Gao, C. Yang, Z. Zhang, P. Chai, W. Chen, and C. Chen, "Image Steganalysis Based on Moments of Characteristic Functions using Wavelet Decomposition, Prediction Error Image, and Neural Network," *in Proc. IEEE International Conference on Multimedia and Expo*, 2005. Available: https://doi.org/10.1109/ICME.2005.1521412.

[9] J. Dong, W. Wang, T. Tan, and Y.Q. Shi, "Run- Length and Edge Statistics Based Approach for Image Splicing Detection. Digital Watermarking," *in Proc. 7th International workshop IWDW2008, LNCS* , vol. 5450, Springer, Berlin, Heidelberg, pp. 76- 87, 2009. Available: https://doi.org/10.1007/978-3-642-04438-0_7.

[10] J. Wang, Z. Li, C. Zhang, J. Chen, Z. Wu, L. Davis, and Y. Jiang, "Fighting Malicious Media Data: A Survey on Tampering Detection and Deepfake Detection", 2022. 10.48550/arXiv.2212.05667.

[11] W. Wang, J. Dong, and T. Tan, "Effective Image Splicing Detection Based on Image Chroma " , *in Proc. 16thIEEE International Conference on Image Processing (ICIP)*, pp. 1257-1260, 2009.

[12] A. A. Alahmadi, M. Hussain, H. Aboalsamh, G. Muhammad, and G. Bebis, "Splicing image forgery detection based on DCT and local binary pattern," *in 2013 IEEE Global Conference on Signal and Information Processing*. pp. 253-256, 2013. Available: https://doi.org/ 10.1109/GlobalSIP.2013.6736863.

[13] D. Cozzolino, D. Gragnaniello, and L. Verdoliva, "Image Forgery Detection Based on The Fusion of Machine Learning and Block-Matching Methods," *in Proc. IEEE International Conference on Image Processing (ICIP)*, pp. 5302-5306, 2014. Available: https://doi.org/10.48550/arXiv.1311.6934

[14] J.G., Han, T.H. Park, Y.H. Moon, and I.K. Eom, "Efficient Markov Feature Extraction Method for Image Splicing Detection Using Maximization and Threshold Expansion," *Journal of Electronic Imaging*, vol. 25, no. 2, p. 023031, 2016. Available: https://doi.org/10.1117/1.JEI.25.2.023031

[15] M. V. Hilal, P. Yannawar, and A. T. Gaikwad, "Image inconsistency detection using histogram of orientated gradient (hog)," *in 2017 1st International Conference on Intelligent Systems and Information Management (ICISIM). IEEE*, 2017, pp. 22–25. Available:

https://doi.org/ 10.1109/ICISIM.2017.8122141

[16] C. S. Prakash, A. Kumar, S. Maheshkar, and V. Maheshkar, "An integrated method of copy-move and splicing for image forgery detection," *Multimedia Tools and Applications*, vol. 77, no. 20, pp. 26 939–26 963, 2018. Available: https://doi.org/10.1007/s11042-018-5899-3

[17] M. H. Alkawaz, G. Sulong, T. Saba, and A. Rehman, "Detection of copy-move image forgery based on discrete cosine transform," *Neural Computing and Applications*, vol. 30, no. 1, pp. 183–192, 2018. Available: https://doi.org/10.1007/s00521-016-2663-3

[18] H. A. Jalab, T. Subramaniam, R. W. Ibrahim, H. Kahtan, N. F. M. Noor "New Texture Descriptor Based on Modified Fractional Entropy for Digital Image Splicing Forgery Detection," *Entropy*, vol. 21, no. 4, p. 371, 2019. Available: https://doi.org/10.3390/e21040371

[19] M. H. Siddiqi, Kh. Asghar, U. Draz, A. Ali, M. Alruwaili, Y. Alhwaiti, S. Alanazi and M. M. Kamruzzaman, "Image Splicing-Based Forgery Detection Using Discrete Wavelet Transform and Edge Weighted Local Binary Patterns," *Security and Communication Networks*, vol. 2021, p. 4270776, 2021. Available: https://doi.org/10.1155/2021/4270776

[20] K. Asghar, M. Saddique, M. Hussain, G. Bebis, Z. Habib, "Image Forgery Detection Using Noise and Edge Weighted Local Texture Features," *Advances in Electrical and Computer Engineering*, vol. 22, no. 1, pp. 57-69, 2022. Available https://doi.org/10.4316/AECE.2022.01007

[21] D.S. Sulaiman, M. S. M. Altaei," Image tampering detection using extreme learning machine" *AIP Conf. Proc.* , vol 2457, p. 040002, February 2023. Available https://doi.org/10.1063/5.0123415

[22] M. Hall, E. Frank, G. Holmes, B. Pfahringer, P. Reutemann, and I.H. Witten, "The WEKA Data Mining Software: An Update," *ACM SIGKDD Explorations Newsletter*, vol. 11, pp. 10-18, 2009.

[23] R. Ebrahimzadeh, and M. Jampour, "Efficient Handwritten Digit Recognition based on Histogram of Oriented Gradients and SVM," *International Journal of Computer Applications*, vol. 104, no. 9, pp. 10-13, 2014. Available: https://doi.org/10.5120/18229-9167

[24] C. Tomasi, "Histograms of Oriented Gradients,", 2017. Available: https://courses.cs.duke.edu/fall15/cps274/notes/hog.pdf.

[25] B. Sugiarto *et al*., "Wood identification based on histogram of oriented gradient (HOG) feature and support vector machine (SVM) classifier," *2017 2nd International conferences on Information Technology, Information Systems and Electrical Engineering (ICITISEE)*, Yogyakarta, Indonesia, pp. 337-341, 2017. Available: https://doi.org/ 10.1109/ICITISEE.2017.8285523

[26] L. Almawas, A. Alotaibi, and H. Kurdi, "Comparative Performance Study of Classification Models for Image-Splicing Detection," Procedia *Computer Science*, vol. 175, pp. 278-285, 2020. Available: https://doi.org/10.1016/j.procs.2020.07.041

[27] Ž. Đ. Vujović," Classification Model Evaluation Metrics," *(IJACSA) International Journal of Advanced Computer Science and Applications*, vol. 12, no. 6, 2021. Available: https://doi.org/ 10.14569/IJACSA.2021.0120670